Modeling Socio-Cultural Processes in Network Centric Environments

Eunice E. Santos[a], Eugene Santos Jr.[b], John Korah[a], Riya George[c], Qi Gu[b], Keumjoo Kim[b], Deqing Li[b], Jacob Russell[b], Suresh Subramanian[c]
[a]Institute of Defense and Security, University of Texas at El Paso, El Paso, TX, USA 79968
[b]Thayer School of Engineering, Dartmouth University, NH, USA 03755
[c]Department of Computer Science, University of Texas at El Paso, El Paso, TX, USA 79968

ABSTRACT

The major focus in the field of modeling & simulation for network centric environments has been on the physical layer while making simplifications for the human-in-the-loop. However, the human element has a big impact on the capabilities of network centric systems. Taking into account the socio-behavioral aspects of processes such as team building, group decision-making, etc. are critical to realistically modeling and analyzing system performance. Modeling socio-cultural processes is a challenge because of the complexity of the networks, dynamism in the physical and social layers, feedback loops and uncertainty in the modeling data. We propose an overarching framework to represent, model and analyze various socio-cultural processes within network centric environments. The key innovation in our methodology is to simultaneously model the dynamism in both the physical and social layers while providing functional mappings between them. We represent socio-cultural information such as friendships, professional relationships and temperament by leveraging the Culturally Infused Social Network (CISN) framework. The notion of intent is used to relate the underlying socio-cultural factors to observed behavior. We will model intent using Bayesian Knowledge Bases (BKBs), a probabilistic reasoning network, which can represent incomplete and uncertain socio-cultural information. We will leverage previous work on a network performance modeling framework called Network-Centric Operations Performance and Prediction (N-COPP) to incorporate dynamism in various aspects of the physical layer such as node mobility, transmission parameters, etc. We validate our framework by simulating a suitable scenario, incorporating relevant factors and providing analyses of the results.
Keywords: Network centric environments, modeling and simulation, socio-cultural modeling, complex networks

INTRODUCTION

Recent military operations such as Operation Iraqi Freedom (OIF)[1] have seen extensive use of information and communication systems for better situational awareness, better coordination, and faster response, bringing a little closer to fulfillment the promises of network centric environments. Network centric environments have enabled the military to reduce their reaction time and transformed modern military operations by devolving power to the edge and enabling local commanders to be more proactive in their support of mission goals. Each warfighter, who is or can be outfitted with advanced sensors and communications systems, is now a potential source of real time intelligence. This is necessary in an era where urban insurgency and unconventional warfare are the main threats faced by modern military forces. Although the effectiveness of networked forces has been studied, the emphasis has been on the technological aspects. Borrowing the terms of Network Centric Operations/Warfare (NCO/NCW)[2], most of the performance analysis has been on the physical layer consisting of the information and communication systems. However, this is only part of the story. Wars are won by soldiers from different services, backgrounds and training, working towards common goals. The social relationships formed by soldiers within their immediate groups such as a squad or extended group such as a brigade are critical for the successful completion of missions. By supporting communications between a wider set of warfighters, unrestricted by traditional command hierarchies, network centric environments have a deep impact on the formation and evolution of these relationships. Cognizant of the importance of social relationships, the military has been interested in applying social metrics such as cohesion and analyzing their impact on overall performance[3]. Traditional modeling methods for network centric environments model either the network/physical domain while making simplifying assumptions about the social domain or vice versa. However, changes in the network layer can have profound effects on how individuals collaborate with each other and how they form social relationships. Similarly, changes in those social relationships can alter how individuals work together in a team and ultimately how they communicate with each other. For example, it is more likely for an analyst to reach out to another analyst whom he/she knows and trusts rather than to a stranger. In warlike conditions, due to the extreme conditions of the environment, the characteristics of the physical networks change rapidly. Sensor and weapons nodes move at various velocities leading to change in transmission

Defense Transformation and Net-Centric Systems 2012, edited by Raja Suresh, Proc. of SPIE
Vol. 8405, 84050A · © 2012 SPIE · CCC code: 0277-786X/12/$18 · doi: 10.1117/12.921654

strengths, packet drop rate, and latency of the links. Social domains also change as individuals are assigned to new teams or allocated new tasks that require collaborations with other individuals. This in turn leads to formation of new relationships in the social domain. It is clear that any framework that seeks to model social processes has to model the relevant details of both the physical and social layer and how they evolve over time. Socio-cultural factors relevant to the social process being modeled should be represented in a realistic manner within the framework. However, such information is usually subjective and incomplete. There is also a high level of uncertainty when modeling the impact of these factors on individual and group behavior. In summary, the main challenges of modeling social processes in network centric environments are: 1) representing the interactions between the social and physical layers, 2) modeling the dynamism in both the physical and social layers, 3) incorporating relevant socio-cultural factors, and 4) dealing with the inevitable uncertainty and incompleteness of socio-cultural information.

We propose a novel framework for realistic modeling of social processes in network centric environments by representing the relevant details and dynamism in the physical and social layers. We will represent the physical layer by leveraging our previous work in NCO/NCW performance modeling, where we developed the Network Centric Operations Performance and Prediction (N-COPP) framework[4,5]. N-COPP has a flexible component based architecture that can incorporate multiple network sub-models, analytical tools and optimization methods. Using well-defined functional mappings between the components, it provides a modeling backbone to create and connect various segments of a network model. Therefore, sub-networks representing different assets such as sensors networks and weapons systems can be modeled independently and incorporated into N-COPP using its mathematical representation and functional mapping. In this work, we will expand the N-COPP methodology by incorporating social networks as one of the network structures in our framework. Social Network Analysis (SNA)[6,7] encompasses a broad range of techniques in computational social science to represent and analyze social processes. However, traditional SNA methods are limited in their utility as they do not truly represent the richness of available socio-cultural information. We will utilize Culturally Infused Social Networks (CISNs) to provide relevant cultural context in our models and generate more accurate analysis and explanations. CISN also provides the ability to deal with the inherent uncertainty and incompleteness of social information. With CISN, we will model the social layer in network centric systems, incorporate information from the physical layer and analyze social processes using various methods including classic SNA based algorithms. We will validate our framework by modeling group cohesion among warfighters during a real world scenario. We will also study how individual socio-cultural characteristics, group size, information sharing paradigms and events on the ground affect group cohesion. In the next section, we provide a brief background on some of the recent works in modeling and simulation of social aspects in network centric environment with a focus on military units. We will also provide a brief tutorial on the concept of group cohesion. This is followed by a detailed description of our new framework. The validation section describes the implementation details, experimental setup with details of a real world scenario and analysis of the results.

BACKGROUND

Researchers have used various modeling and simulation approached based on techniques such as multi-agent modeling[8] and complex adaptive[9] systems to understand various issues in military networks such as collaboration between warfighters, impact of technology on situational awareness and decision making and overall system performance. We provide a brief description of previous work in modeling network centric environment, with focus on Network Centric Operations/Warfare (NCO/NCW). Most research efforts in network centric environments have focused on modeling the communication and sensor technology. Lu[10] formulated a model for developing the network infrastructure to support NCO communications, but like many approaches, they leave out the human and social factors. The same is true for Walker *et al*[11], which applies Social Network Analysis (SNA) techniques to analyze a standard NATO approach to NCO, but again focuses on the physical network and command hierarchy, and also does not address the human factor. Theories of social network analysis have been explored much longer than NCO, and while useful, cannot provide a complete solution for modeling or analyzing these systems. Wong-Jiru *et al*[12] developed a multi-layer model of the NCO approach, with layers for people, applications, processes, a physical network, etc., to support a deeper graph-theoretical analysis of NCO components and networks. However, the modeling of the human factor was very simplified, as is the case with many SNA-centric approaches to analyzing or simulating NCO, and did not reflect in the analysis how uniquely human factors such as culture, friendship, and trust affect the actions of human agents in a complex military network. Schneider *et al*[13] , building on work by Marinier *et al*[14], present an approach for modeling human behavior and emotion, in the context of NCO, but do not attempt to combine this in a unified way with other aspects like the military hierarchy or network communications. Though challenging, the importance of modeling the human factor in NCO has not gone unnoticed. West *et al*[15] and Gharai *et al*[16] describe the importance of including the human factor in a complete model of the NCO approach. As an integral part of any NCO system, and probably one of the most complex, the human agent must be accurately modeled in any realistic simulation, which requires a representation of human characteristics, relationships, and decision-making processes. In summary, current state of the art in modeling and simulation of network centric environments focus on certain aspects of the problem while making simplifications in the representation of technological and social factors. There is a need for a generic modeling framework for analyzing the various social processes in this domain that truly models the complexity of individual and group behaviors by incorporating all relevant factors in both the physical and social layers.

Group cohesion in military units measures the dynamic social behavior among the military groups and is also one of the most widely studied social metrics. In order to measure the performance of a group, it is necessary to understand the social dynamics among the group members and Mullen *et al*[3] shows that evaluating cohesion among groups is a good indicator for performance. Many definitions of cohesion are available and one of the earliest by Festinger[17] broadly defines cohesion as "the resultant of all the forces acting on all the members to remain in the group". On the other hand, Gross *et al*[18] argues that cohesion should be measured as the resistance of the group against disruptive forces. In military contexts, cohesion can be defined as "the bonding together of members of an organization/unit in such a way as to sustain their will and commitment to each other, their unit, and the mission"[19]. Even when a common definition for cohesion is agreed upon, formulating a method to measure cohesion remains a challenge. This is because many factors such as shared goals, motivations, interpersonal relationships, teamwork, etc. have to be taken into account in a realistic representation of cohesion. The most common classification divides cohesion measures into two types: task cohesion and social cohesion. MacCoun[20] refers to task cohesion as "the shared commitment among members to achieving a goal that requires the collective efforts of the group" and social cohesion as "the nature and quality of the emotional bonds of friendship, liking, caring, and closeness among group members". It can be concluded that a group with higher task cohesion will be more committed towards achieving a goal than a group with lower task cohesion. Similarly a group with high social cohesion will have team members who prefer to spend time with each other and share a higher emotional bond. MacCoun[20] also suggests that task cohesion has a greater impact on performance than social cohesion. Social cohesion can also have unfavorable consequences. Greater social cohesion can lead to excessive socializing and groupthink, thereby affecting rational decision-making which is not desirable in a military situation. Janis[21] suggests that a moderate level of social cohesion is desired for optimal performance. Some of the factors that influence social and task cohesion in military units are: group membership, quality of leadership, and group size.

MODELING FRAMEWORK

In this paper, we propose a computational framework to model and analyze social processes in network centric environments by simultaneously representing the physical and social layers. We will leverage previous modeling, specifically in modeling the NCO/NCW network layer using the Network Centric Operations Performance and Prediction (N-COPP) framework[22] and modeling the social layer using Culturally Infused Social Networks (CISN)[23]. The key idea behind the framework is that social processes have two components: social interaction and socio-cultural factors. Interaction is facilitated by actual physical meetings and communication technologies. However, two individuals who interact frequently may not form a social relationship if they are from different strata of society, have different values or follow different social norms. In short, commonality of the socio-cultural makeup of the interacting individuals or groups has an impact on the formation of social ties or spread of influence. In keeping with this central principle our framework, shown in Figure 1, models social interaction in terms of the interaction and ideology networks. Since the physical layer facilitates communication between individuals in network centric systems, the various network structures of the physical layers are used to construct the overall interaction network. The ideology network connects individuals based on the similarities in their personalities and beliefs. Culturally Infused Social Network (CISN) is generated by combining the interaction and ideology networks. In the following sections we describe in detail the components of our framework that deal with modeling the physical layer, modeling the social layer and analyzing the social process.

Modeling the Physical Layer

Modeling the physical layer aspects of network centric systems, especially in NCO/NCW, presents many challenges. They are complex networks consisting of multiple sub-networks, each potentially using different technologies and operating under different standards. The nodes may have different functionalities and divergent mobility characteristics, and operate under varying conditions. Moreover, they operate within rapidly changing and extreme environments. Reliability and performance of the underlying communication, information, and decision systems are critical to successful completion of missions. The N-COPP framework was designed to meet the performance modeling challenges of heterogeneity, dynamism, and complexity of the physical layer in a network centric environment. N-COPP has a component-based architecture with the following components: 1) Network Representation Component (NRC): embodies the graphical representations in the form $G(V,E)$, of the various networks and sub-networks in the system, where V and E represent the nodes and edges, respectively. The graph nodes represent the entities such as sensors, weapon systems, fusion nodes, etc. The edges represent the connection properties between the nodes such as link speed, bandwidth and connectivity. The graph representations in NRC are used by other components for analysis and prediction. 2) Performance Measures Component (PMC): contains functional mappings to represent future states of the representations in NRC. The functional mappings can be implemented using prediction algorithms or simulations. *NRC+PMC* components model the dynamic state of the physical layer. 3) Performance Tools Suite Component (PTSC): contains algorithms and methodologies for analyzing the network characteristics and performance. 4) Sub-component Interaction Component (SIC): contains methodologies for quantitatively assessing the network and providing suggestions to optimize network performance. The flexible architecture of N-COPP, where each component deals with a specific aspect of network modeling and analysis, is crucial for plug-n-play property. More details on the framework and how it has been applied can be found in Santos *et al*[4,5].

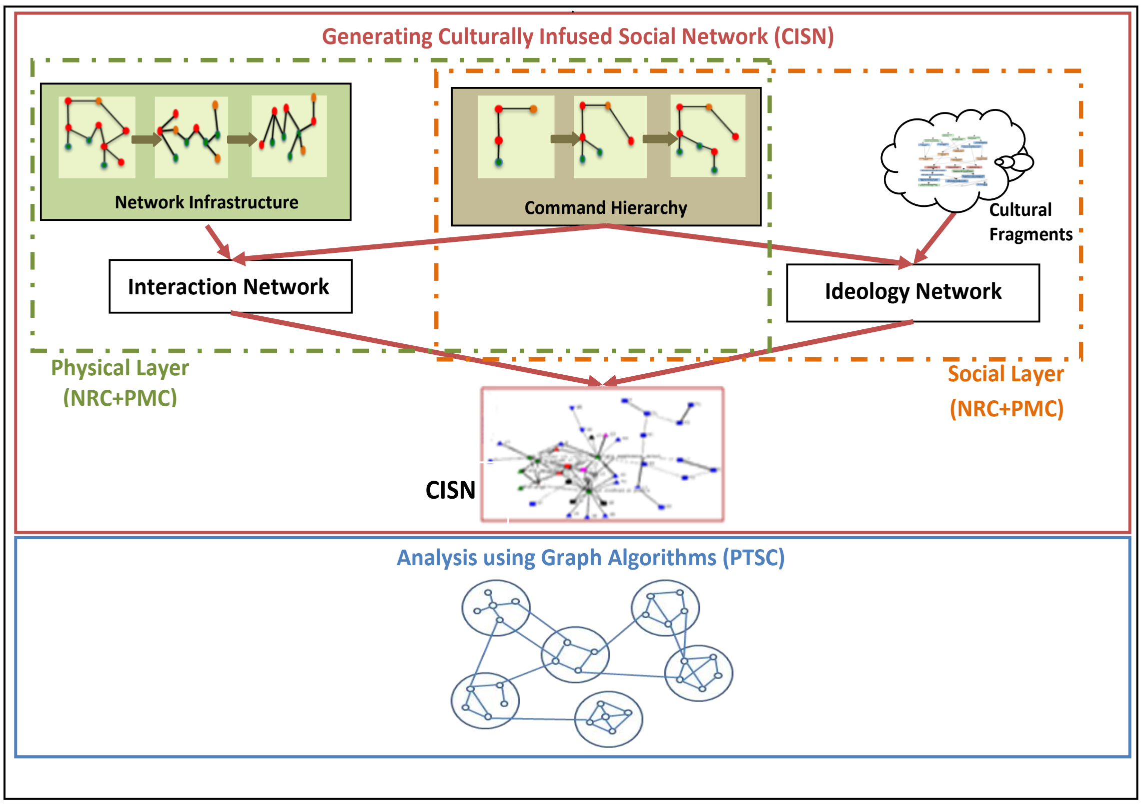


Figure 1. Framework for Modeling Social Processes in Network Centric Environments

Modeling the Social Layer

In order to capture the socio-behavioral aspects of processes in network centric environments, we leverage the Culturally Infused Social Networks (CISN)[22,23] , shown in Figure 2, and extend traditional social networks formed in network centric environments by incorporating cultural factors. CISN is a generic modeling framework that provides a cultural context that is lacking in traditional approaches to social network analysis. Culture is key to understanding individual and group behavior. However, modeling culture is a challenge due to the inherent uncertainty and subjectivity of social information. Moreover, connecting underlying cultural factors to emergent behavior of individuals and groups is difficult. In real world scenarios, the social systems are typically multi-scale, and behaviors at various scales have to be included in the model. The notion of intent[24], which models individual, group or organizational behavior as a set of beliefs, goals and actions, is used to tie underlying cultural factors to complex behavior. Intent is represented using a probabilistic network framework called Bayesian Knowledge Bases (BKBs)[25]. A BKB (example is given in Figure 3) is a directed graph consisting of two types of nodes: I-nodes (boxes) and S-nodes (circles), which represent probabilistic if-then rules. Each I-node represents a single instantiation of a random variable (*rv*). Each S-node is connected to a single I-node. Zero or more I-nodes may be connected to an S-node. The S-node denotes the conditional probability value for the rule that connects the incoming I-nodes to the outgoing I-nodes. The behavior rules formed with socio-cultural information using the intent model are represented in BKBs. The intent model represents an entity's behavior in terms of the following variables:

a) Beliefs: include the information and perceptions that the entity has towards the environment and other entities.

b) Goals: are the desired end-states that the entity would like to achieve.

c) Actions: are the available options that the entities towards achieving the goals

d) Axioms: consist of self-referential perceptions of the entity.

The intent model also explicitly represents the causal chain between the beliefs, goals, actions and axioms, and help to provide explanations for observable behavior. The intent model is implemented using BKBs to explicitly represent the uncertainty and incompleteness of information using conditional probability measures while supporting reasoning algorithms that can be used to provide analysis. The intent model also specifies rules for interconnecting the I-nodes representing the beliefs, goals, actions and axioms. Axioms I-nodes can have beliefs as inputs and serve as inputs to other axioms and goals. Beliefs and goals may form inputs to actions. Actions can also lead to other actions. In addition to axioms, beliefs also form inputs to goals. Goals can lead to other goals. In Figure 3, the I-nodes representing beliefs, goals and actions are tagged with the strings (B), (G) and (A) respectively. Various strands of socio-cultural information, in the form of entity intent, are represented by BKBs in the form of cultural fragments. Cultural fragments relevant to an entity can be fused together using the Bayesian fusion algorithm[26], to form a single large BKB. This is critical for modeling dynamism as fragments, representing real time changes, can be added during a simulation.

By inferencing the intent of each group member, we are able to detect the similarities and differences between individuals with respect to personal likes and dislikes. An ideology network is built to capture such intent proximity inside a group of people, each represented by a node. A weighted link between two nodes indicates the similarity of two people's intent and ideology, where the weight is calculated based on the probability that they will pursue similar goals or actions. It is expected that people with similar ideologies will be more likely to collaborate, given the opportunity. Thus, ideology can be used to assess the desire or potential for collaboration. The effectiveness of communication between people is restricted by the potential for physical interaction. If two like-minded people never have the chance to talk to one another, their ideological similarities will make little difference to the probability that they will collaborate. Thus, in order to reflect the complexity in social influence, it is crucial to combine the ideology network and physical network. The CISN computational framework has been used for modeling such complex simulations due to its component-based architecture. CISN leverages a probabilistic reasoning framework to represent various socio-cultural factors and relationships with inherent uncertainty and incompleteness. Different components of the framework deal with various aspects of social systems, including physical interactions, social influences, and perceptions. The CISN in this work consists of two components: the ideology network and the physical network, and the weight w for edge e in CISN is calculated as: $w = w_i r^{w_p}$ where w_i and w_p are the weights of the corresponding edges in the ideology network and physical network respectively. r is a constant indicating the strength of influence of the physical network when calculating the edge weights for the CISN.

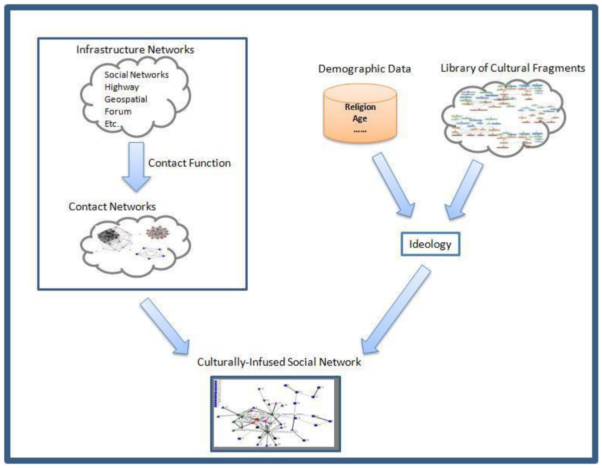


Figure 2. Culturally Infused Social Network Analysis[23]

Analysis

The generated CISN can be analyzed using various techniques including traditional social network analysis. The analytical component of the framework implements these analysis algorithms. The CISNs generated for real world military networks are typically very large ranging from tens of thousands to hundreds of thousands of nodes. The networks may also be very dense. Due to the dynamic nature of the underlying physical and social layers, the structure and characteristics may change rapidly. These factors can raise substantially the time required to provide analysis. Parallel and distributed algorithms help to deal with large, dense and dynamic graphs by providing analysis in a time-bounded manner. The Anytime-Anywhere framework by Santos *et al*[6,7,27] provides a reliable parallel and distributed architecture to implement graph analysis algorithms for social networks. Anytime algorithms are interruptible algorithms that generate initial estimations quickly, and then results of increasing quality over time. Anywhere algorithms provide the ability to deal with changes in the networks by reusing previous results to generate the new results, saving time and resources. The Anytime-Anywhere framework has been validated by designing algorithms to calculate shortest paths[6], centrality[7] and maximum cliques[27] with various network size *s* and types of dynamism. In this paper, we will leverage some of this previous work to validate our framework, measure group cohesion by identifying *k*-cliques, and study the changes in group cohesion in a network centric system due to a changing environment. Parallel and distributed algorithms for analyzing social processes in network centric environments will be a focus of future work.

VALIDATION

Cohesion is one of the social metrics that is both relevant to the performance of a network centric environment and is affected by changes in the physical and social layers. We will validate our framework by using it to model changes in cohesion in a real world scenario and provide explanations for the changes. Cohesion within a group can change based on the support for a proposed plan of action within its members. Actions based on consensus will improve group cohesion. In military units, where the consensus process is rare or absent and soldiers are expected to follow orders, true support for the commander's plan of action is harder to gauge. We will use the notion of intent, described in an earlier section, to take the underlying beliefs, motivations and goals and determine plausible actions of each individual soldier, and determine how aligned his/her intent is with that of the commander. A soldier's decision-making process, which is a part of his/her intent, is dependent on the available information. We will simulate two intelligence sources in the scenario that provide either concurrent or contradictory information to the soldier and analyze its effect on cohesion. In order to do this, the scenario should be detailed with information about the events, makeup of the military units and relevant socio-cultural characteristics of the individuals. In this section we will describe the scenario, the implementation details of the framework, and the details of the cohesion metric.

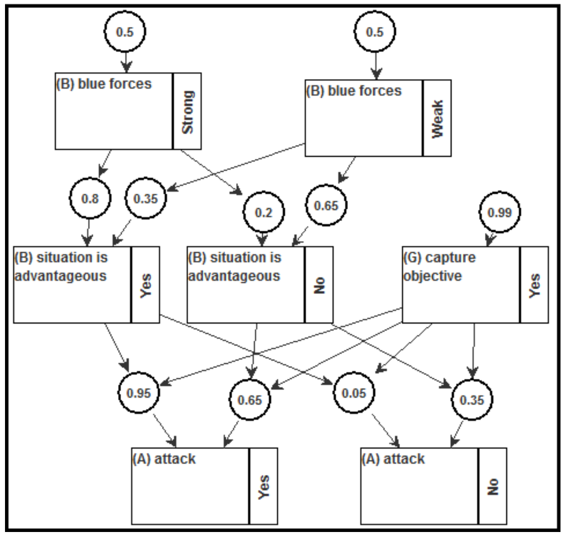


Figure 3. Example of BKB

Scenario

We used open source information about unit tactics, communication equipment and training manuals to gather information about suitable unit operations that can be used to construct the scenario. Since NCO/NCW is relatively new, case studies and analyses of tactics adopted by networked forces are scarce. We focused on recent military engagements such as Operation Iraqi Freedom (OIF), where NCO/NCW techniques were employed. The events in our scenario were generated using related case studies[1] which describe actual battle field events where units from infantry, armored and artillery units had to work in unison against Iraqi forces. The case studies helped to build a fictional set of events with the goal being to analyze how the soldier's state of mind changes over time and how that in turn affects group cohesion. We will demonstrate that our framework is capable of capturing group cohesion using soldiers' intent, and provide explanatory analysis. We also assign relevant socio-cultural traits to soldiers. This will help to generate a diverse population and capture interesting group behaviors. Table 1 lists the actions and events relevant to the scenario where the objective of the blue forces to capture a bridge over a river Euphrates and proceed towards the capital of red forces. The soldiers in the blue force have access to two intelligence resources/units, labeled Intel A and Intel B. We will consider two sub-scenario where the information they provide are the same or different. As explained earlier we seek to demonstrate how the intent of the soldiers changes with the events in the scenario and how aligned their intents are to what actually happens. The soldier's view is affected by information coming in from the intelligence units. His/her view is also shaped by personal experiences and training. We are more interested in those events or concerns which have the potential of creating divisions in the unit and reduce confidence in the commander. Such concerns/events include presence of overwhelming opposition forces, possibility of chemical weapons, losing contact with certain components of the unit, etc.

Table 1 Description of Time Steps in Scenario

Time Step	**Event**	**Sub-scenario 1.1 (intelligence units give same info)**	**Sub-scenario 1.2 (intelligence units give contradictory info)**
1.	Blue forces are getting ready to engage the red forces defending the bridge.	Intelligence indicates weak red forces on the west side of the bridge.	Intel A: Weak forces on the west side of the bridge. Intel B: Strong forces on the west side of the bridge.
Outcome: Blue forces move forward and engage the weaker red forces.			
2.	Blue forces move forward and engage red forces	Reports of WMD being deployed by red forces to stop blue forces	Intel A: WMD being deployed by red forces Intel B: No reports of WMD

Outcome: Red forces engaged. No WMD found. Blue forces are getting ready to cross bridge.			
3.	Blue forces move to capture bridge	Intelligence units provide reports on explosives on bridge which may result in heavy casualties.	Intel A: Explosives on bridge Intel B: No explosives on bridge
Outcome: Explosives found on the bridge. Some of the explosives could not be defused in time leading to casualties.			
4.	More fighting	Intelligence unit provide info that casualty rate is increasing.	Intel A: Casualty rate is increasing Intel B: Casualty rate not very high
Outcome: Casualty rate is indeed high.			
5	Blue forces push forward.	Intelligence unit provides info that blue forces are running low on ammunition and supplies	Intel A: Low on ammunition and supplies Intel B: Enough ammunition and supplies to sustain the attack
Outcome: Units running low on ammunition and supplies.			
6.	Blue forces enter enemy stronghold.	Intelligence unit provide info that large red forces are lying in wait for ambush	Intel A: Red forces lying in wait for ambush Intel B: No red forces in area
Outcome: Strong red forces in the area			

Implementation

In order to validate the framework with the scenario described in the previous section, we will use open source information and synthetic data to populate the social and physical layer sub-models in the framework. We will now describe in detail the creation of the interaction and ideology networks for military units of various sizes and show how CISNs are generated. We will also describe how social science literature was used to design the group cohesion metric that we use to analyze the scenario.

Generation of Simulated Military Unit

Since there is limited data available on the makeup of real world units, we attempted to generate a simulated military unit that would be representative of a real one with regards to both the hierarchical structure, and the socio-cultural characteristics of individual soldiers (e.g. age, experience level, marital status, risk aversion, etc.). The structure of the unit is in keeping with US military hierarchy, starting with a brigade-level unit. This is composed of companies, and the hierarchy continues with platoons and squads. Each unit has a commander, staff members, and the appropriate subordinate units. We study cohesion for various group sizes by varying the number of platoons generated within the brigade. As the soldiers in various positions within the hierarchy are generated, their personality traits are also created. We used a random generator to introduce an element of randomness to the process, but certain things like age, time in service, marriage status, etc., are generated within constraints based on the position that soldier is in.

Physical Layer

Due to the lack of real-world data on interactions between soldiers in network centric environments, we generated the data using a detailed simulation of the communication links. For the sake of reproducibility, we used an off-the shelf Omnet++[1] 4.1b discrete event simulator along with the MiXiM[2] wireless framework. We generated a communication network that followed the command hierarchy generated in the previous section. We chose random initial locations for each non-leaf node within a 500x500 unit square and the leaf nodes were then randomly placed within a 50x50 unit square, centered on their parent node. The nodes communicate with each other by sending data packets. Each packet is generated with a destination node (which may not be connected directly to it) and then sent over a random connection until it reaches the destination or gets dropped. The strength of the communication link varies according to the distance between the nodes and the velocity of the nodes. A packet that is transmitted across a link, gets dropped when the signal strength drops below a certain threshold. On an average, *n mod 8* packets (where n is the number of nodes) get transmitted at a time in the simulation, so as to achieve a relatively uniform distribution of packets for any size network.

---

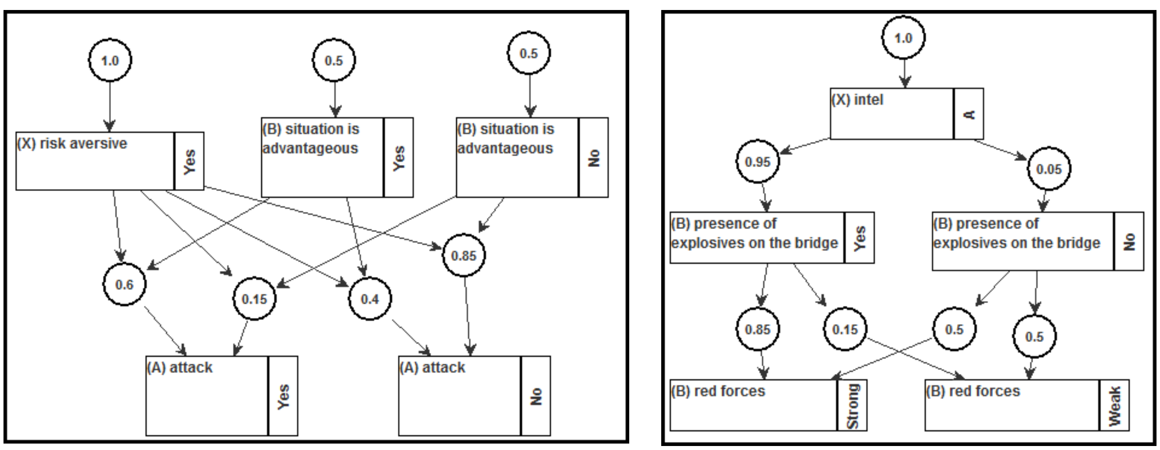
[1] http://www.omnetpp.org/
[2] http://mixim.sourceforge.net/

The communication network is simulated and interaction network generated for each step of the scenario. The weights of the edges in the resultant ideology are measured in terms of the data sent across the edges and are calculated using the formula: $\frac{n_s}{n_s+n_d}$ where n_s is the total number of packets successfully transmitted and n_d is the total number of packets dropped. If no packets were ever sent along an edge, then the edge gets a weight of 0.

Social Layer

However, merely modeling communications in the field is not sufficient for modeling cohesion. We need to take into account the individual characteristics that soldiers possess as these have a great impact on their decision-making and performance in the battlefield. Incorporating the cultural information along with the communication network helps to give a better understanding of the intent of the soldiers in the network. Bayesian Knowledge Bases (BKBs) are used to represent this information in the form of cultural fragments. For the simulation, we built two types of fragments: a) Persistent Fragments: represent the cultural traits of the soldiers and remain constant throughout the simulation. In our simulation we used three persistent fragments representing information about experience, risk aversion, and marital status. An example of a persistent fragment representing a highly risk-averse soldier is given in Figure 4(a), and b) Event Fragments: represent the dynamic information about an event and information obtained from Intel A and Intel B. These fragments change during each time step in the scenario. An example of an event fragment providing information from Intel A is given in Figure 4(b).

Although each soldier in the simulation gets information from both Intel A and Intel B, each also has a higher initial trust in only one of the intelligence sources. In the simulation, each soldier is initially modeled by fusing all the relevant individual persistent fragments. In order to generate a diverse population, persistent fragments are fused with a random reliability value. For each time step of the scenario, new information provided by both of the intelligence units (which can be either correct or wrong) is added by fusing corresponding event fragments to the soldiers' BKB. Depending on the turnout of each event and how accurate the intelligence units are in relaying information, the trust that the soldier has in the intelligence unit will change. The target random variable (*rv)* used for generating the ideology network in this simulation is "(A) attack". For every time step, the ideology network representing how similar the soldiers are in their inclination to attack is generated. The corresponding CISNs are generated by combining the ideology network with the physical network.



(a) (b)

Figure 4. Examples of Cultural Fragments a) Persistent Fragment b) Event Fragment

Measuring Cohesion

The CISN framework captures the essence of the physical and social layers in the network centric system and allows for the application of graph theoretic methods to analyze the dynamic social behaviors occurring both inter-group and intra-group. In this paper, we focus on group cohesion. We measure this through maximum clique enumeration in the CISN network and evaluate how cohesion changes as the situation evolves over time. We first build a power graph based on the original graph by calculating an all-pair shortest-path matrix for the original, then removing entries greater than a threshold *k*. Thus, nodes in this power graph are only connected if the distance between them in the original graph is no greater than k. We then calculate the maximal cliques of the power graph, which are equivalent to the k-cliques of the original graph. The algorithm for shortest-path calculation is based on the Distance Vector Routing (DVR) algorithm [28]. Its formula is as follows: $D_x(Y,Z) = c(X,Z) + min_w\left(D_z(Y,w)\right)$ where $D_x(Y,Z)$ is the shortest path distance from X to Y via X's direct neighbor Z, $C(X,Z)$ is the distance between X and Z, and min_w is taken over all of Z's direct neighbors. The algorithm for maximal clique enumeration is based on Zhang's algorithm[29], which calculates cliques in increasing order of clique size, starting with each connected pair of nodes (2-cliques). If the algorithm is able to find a neighbor common to all the nodes in the current clique of size n, it is added to form a clique of size $n+1$. The process is repeated for the addition of each common neighbor until there are no more possible nodes to add, and the maximal clique is generated. After completing stage n, all maximal cliques up to size n have been calculated and can be used for further analysis.

We will leverage previous work[30,31] in social science that used the proportion of mutual pairs to the total number of possible pairs in a group as an indicator of group cohesion. A larger proportion suggests a higher level of social identification within the group. Similar statements can be found in Reffay *et al*[32] that if every member of a group belongs to at least one clique, and every clique has a large number of members, then the group is considered very cohesive. We designed a metric to dynamically measure the group cohesiveness based on the maximum cliques generated from the CISN. Given a set of maximum cliques $C = \{C_1, C_2, \dots . C_m\}$, the overall group cohesion is calculated as below:

<u>Algorithm 1</u>

Set cohesion = 0;
for node n_i, i = 1: n

$$\text{cohesion} = \text{cohesion} + \max_{n_i \epsilon C_j}\left|C_j\right|$$

end

$$\text{cohesion} = \frac{\text{cohesion}}{n^2}$$

return cohesion

The cohesion ranges from [0,1], where 0 indicates that every node is isolated from all others, and 1 is achieved when all nodes are connected to each other. The underlying idea is that the more overlap we find between cliques, the higher cohesion we should expect.

Experimental Setup

The primary goal in this section is to validate the ability of our framework to combine the characteristics of the physical and social layers and provide analysis of the dynamic social processes in network centric systems. The social dynamics between the warfighters in the systems are affected by unfolding events, situational awareness provided by intelligence units and individual behavioral characteristics. Our framework allows for realistically representing these different factors and analyzing the emergent group dynamics. The experimental validation consists of two sub-scenarios 1.1 and 1.2, which were simulated on two types of physical layers, termed physical-A and physical-B. In physical-A, the nodes communicate with their immediate neighbors in the command hierarchy. This represents the traditional way of looking at interactions that are guided strictly by the command structure in the military units. On the other hand, physical-B has nodes that can communicate with each other irrespective of their position in the hierarchy. This represents the modern NCO paradigm where nodes use communication and information technology to collaborate leading to quicker and more effective operations. For each network size, we generated the CISNs with physical-A and physical-B for each event in sub-scenarios 1.1 and 1.2. Since the interactions in the physical network are probabilistic in nature, we ran each simulation three times and took the average of the generated cohesion values.

We will utilize the scenario to validate some key facts about group cohesion. It is known that as the group size increases the general liking of the members towards the group decreases[33]. Therefore group cohesion generally decreases with group size. In the first experiment, we will test this hypothesis by analyzing the change in cohesion in a CISN with sizes ranging from 127 to 727 nodes. For brevity, we will provide results of the CISN generated with physical-A. Next we look at the role of information and its effect on cohesion. As stated earlier in the context of task cohesion[20], cohesion should increase when group members support a particular course of action or are in agreement on a particular strategy. However, an individual's decisions are based on, among other things, the information that is presented to him. In order to test the importance of information on group cohesion, we analyze the change in cohesion for sub-scenario 1.1 and sub-scenario 1.2. Recall that in sub-scenario 1.1 all nodes get the same Intel information which is always correct whereas in sub-scenario 1.2 the information provided by Intel A and Intel B are different, and some nodes trust Intel A more than Intel B and other nodes trust Intel B more than Intel A. For the final set of results, we will compare the cohesion values for the CISN generated with physical-A and physical-B layers. Since physical-B supports wider interaction, it is expected to have higher cohesion values. We provide detailed analysis and explanations of the results in the next section.

Results and Analysis

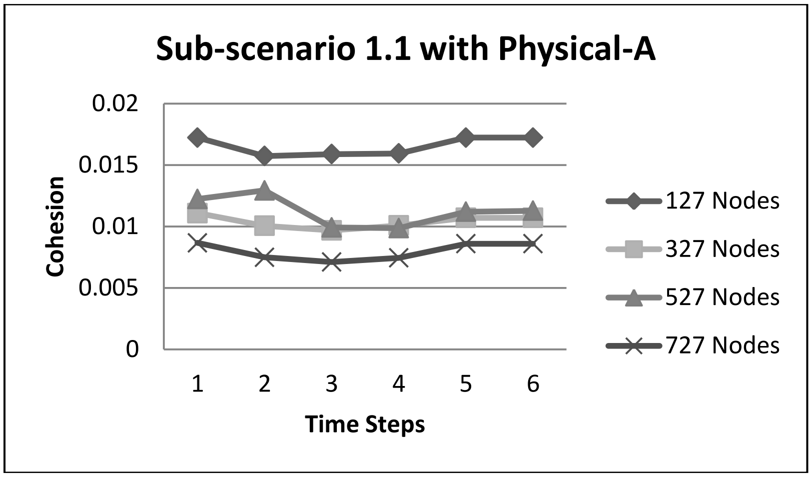


Figure 5. Changes in Cohesion in Sub-scenario 1.1 simulated with Physical-A

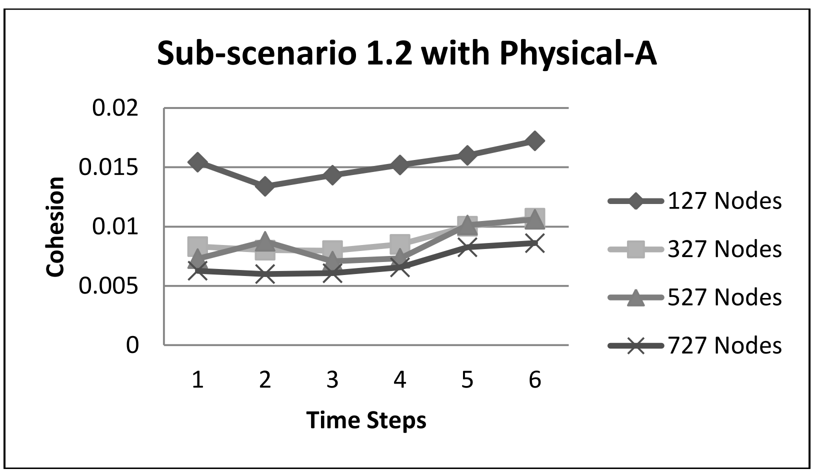


Figure 6. Changes in Cohesion in Sub-scenario 1.2 simulated with Physical-A

Figure 5 and Figure 6 shows the cohesion values for sub-scenarios 1.1 and 1.2 respectively, when simulated with physical-A. From the results, it is clear that the average cohesion of the group in both sub-scenarios decreases when the size of the group grows. This is due to the fact that larger group can result in feelings of isolation, which makes the group more likely to be divided into isolated parts. This is also consistent with existing literature on cohesion[3]. Additionally, when the size is greater than 327, the cohesion does not decline much. This finding indicates that intra-group cohesion becomes less sensitive to the size of group when the size is larger than a threshold. When we compare the cohesion patterns in Figure 5 and Figure 6, we see that there is a subtle but clear increase in cohesion in sub-scenario 1.2 while the cohesion in sub-scenario 1.1 fluctuates around an average value. In sub-scenario 1.2, each node has a higher trust in either Intel A or Intel B. Depending on the outcome of each time step and how accurate the information was, each node upgrades or degrades its trust in the intelligence sources. Since Intel A is always correct and Intel B is always wrong, all the nodes gradually trust Intel A more than Intel B. Since information has an impact on the node's motivation to fight, which is the primary decision variable in our scenario, the group cohesion will increase as all nodes come to trust the same source of information.

Next, we compare the cohesion values for network centric systems simulated using different physical layers: physical-A and physical-B as shown in Figure 7 and Figure 8, respectively. Since physical-B improves information sharing and encourages communication between nodes in the network centric environment, it is natural to believe that the cohesion would be enhanced. We compare the cohesion between physical-A and physical-B under both scenarios and see that the cohesion is always higher in physical-B. This supports our hypothesis. Next, we make a closer analysis by looking at the change in cohesion as the scenario progresses. Again, referring to Figure 7 and Figure 8, physical-B shows a more fluctuant cohesion trend than physical-A. One possible explanation is that physical-B enhances the connection bond between soldiers in the group such that any disagreement or conflicting opinion caused by the influence of new events is spread more quickly and more broadly which may increase the probability of undermining group cooperation. In fact, it is difficult not to be aware of ideological differences in an efficient information sharing system.

CONCLUSION

Technological progress in sensor, communications and information technologies has provided warfighters the ability to collaborate and share information in real time. This allows for individuals from various units to work in tandem to achieve self-synchronization and respond quickly to emerging threats. Social relationships between warfighters have always been critical for successful completion of mission goals. Traditionally, relationships developed between soldiers within the immediate squad and with individuals in the parent organization. In network centric environments, there are more opportunities for soldiers to collaborate with individuals who are at best acquaintances. The relationships are initiated and fostered remotely through telecommunication channels and are often formed in the heat of the battle. In such circumstances it has become important to model and analyze the evolution of social processes involved in team formation, trust formation, etc. In this paper, we introduced a novel framework for modeling social processes in network centric environments that incorporates relevant factors and dynamism in both physical and social layers. Our framework maps the complexity of both these layers into Culturally Infused Social Networks (CISNs) which allows for the adoption of SNA tools for analyses. We validate our framework by modeling the evolution of group cohesion of military units of various sizes and show how cohesion is influenced by group size, individual socio-cultural characteristics, situational information, and communication characteristics.

Social networks for real world network centric environments typically range from the tens of thousands to hundreds of thousands. In order to analyze such large networks, we will look into parallel and distributed methods such as anytime-anywhere social network analysis framework[6,7] to provide time-bounded analysis of the social processes. We will design algorithms that will deal with dynamism in a computationally efficient manner. Further work in cohesion will involve using future conditions in the physical and social layers to predict future values of the cohesion metric.

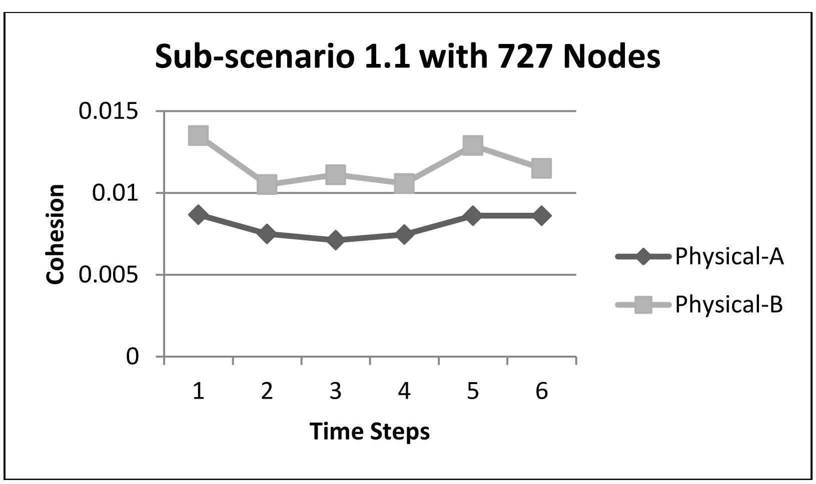


Figure 7. Comparisons of Cohesion in Sub-scenario 1.1 with Different Physical layers (727 Nodes)

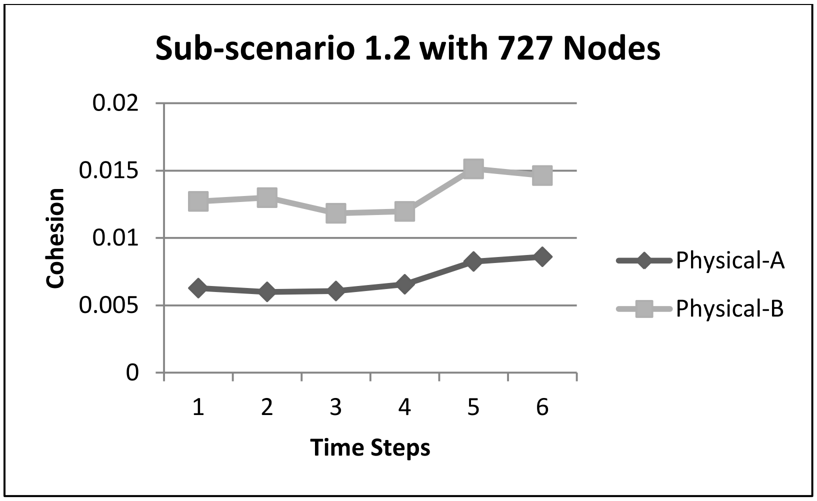


Figure 8. Comparisons of Cohesion in Sub-scenario 1.2 with Different Physical layers (727 Nodes)

ACKNOWLEDGEMENT

This work was supported in part by Army Research Laboratories, Defense Threat Reduction Agency, and Air Force Office of Scientific Research. We also acknowledge the support provided by Dr F. Alex Kilpatrick and Morgan Pittkin towards implementing the command hierarchy network and graph analysis algorithms respectively.

REFERENCES

[1] Tisserand III, J.B., "Network Centric Warfare Case Study U.S. V Corps and Third Infantry Division during Operation Iraqi Freedom Combat Operations Volume III: Network Centric Warfare Insights" (2006).

[2] Alberts, D.S., Garstka, J.J., and Stein, F.P., [Network Centric Warfare: Developing and Leveraging Information Superiority], CCRP Publication Series (1999).

[3] Mullen, B., and Copper, C., "The relation between group cohesiveness and performance: An integration," Psychological Bulletin 115(2), 210-227 (1994).

[4] Santos, E.E., "A framework for assessing and predicting network loads and performance for network-centric operations and warfare," in Proceedings of SPIE 6578, 65780T (2007).

[5] Santos, E.E., Ojha, A., and Korah, J., "Modeling situational awareness in network centric systems," in Proceedings of SPIE, 73500J (2009).

[6] Santos, E.E., Pan, L., Arendt, D., Xia, H., and Pittkin, M., "An Anytime Anywhere Approach for Computing All Pairs Shortest Paths for Social Network Analysis," in Integrated Design and Process Technology (2006).

[7] Santos, E.E., Pan, L., Arendt, D., and Pittkin, M., "An Effective Anytime Anywhere Parallel Approach for Centrality Measurements in Social Network Analysis," in Proceedings of IEEE International Conference on Systems, Man and Cybernetics, 4693 - 4698 (2006).

[8] Cila, I., and Mala, M., "A multi-agent architecture for modelling and simulation of small military unit combat in asymmetric warfare," Expert Systems with Applications 37(2), 1331–1343 (2010).

[9] Masato, D., Norman, T.J., Poltrock, S., Bowyer, H., and Waggett, P., "Adaptive Military Behaviour in a Collaborative Simulation," in Proceedings of the SISO European Simulation Interoperability Workshop (EURO-SIW) (2008).

[10] Lu, N.H., "Network Design Methodology for Network-Centric Operations," in IEEE Sensors Applications Symposium 2007 (SAS '07), 1-5 (2007).

[11] Walker, G., Stanton, N.A., Salmon, P., Jenkins, D., Revell, K., and Rafferty, L., "Measuring Dimensions of Command and Control Using Social Network Analysis: Extending the NATO SAS-050 Model," The International C2 Journal 3(2), 1-46 (2009).

[12] Wong-Jiru, A., Colombi, J., Suzuki, L., and Mills, R., "Graph Theoretical Analysis of Network Centric Operations Using Multi-Layer Models," in 5th Annual Conference on Systems Engineering Research (2007).

[13] Schneider, B., Schwarz, G., and Kunde, D., "The Architecture HuFaNCO - Modeling Imperfect Human Information Processing with Special Reference to Network Centric Operations," in Proceedings of the 18th Conference on Behavior Representation in Modeling and Simulation(April), 23-30 (2009).

[14] Marinier III, R.P., Laird, J.E., and Lewis, R.L., "A Computational Unification of Cognitive Behavior and Emotion," Cognitive Systems Research 10(1), 48-69 (2009).

[15] West, B.J., Bowman, E.K., and Rivera, B., "The Human Dimension of Networks," in 13th International Command and Control Research and Technology Symposia (ICCRTS 2008) (2008).

[16] Gharai, L., Guan, K., and Ghanadan, R., "Military Scenarios and Solutions from a Network Science Perspective," in IEEE Military Communications Conference (MILCOM 2009), 1-6 (2009).

[17] Festinger, L., Schachter, S., and Back, K., [Social pressure in informal groups.], Harper & Row, New York (1950).

[18] Gross, N., and Martin, W.E., "On Group Cohesiveness," American Journal of Sociology 57(6), 546-564 (1952).

[19] Henderson, D., [Cohesion : The human element in combat], National Defense University Press, Washington, DC, 4 (1985).

[20] MacCoun, R.J., [Sexual orientation and military cohesion: A critical review of the evidence.], in Out in force: Sexual orientation and the military, G. Herek, J. Jobe, and R. Carney, Eds., University of Chicago Press., Chicago, 157-176 (1996).

[21] Janis, I.L., [Groupthink: Psychological Studies of Policy Decisions and Fiascoes], 2nd ed., Houghton Mifflin, Boston (1983).

[22] Santos, E.E., Santos Jr., E., Wilkinson, J.T., Korah, J., Kim, K., Li, D., and Yu, F., "Modeling Complex Social Scenarios Using Culturally Infused Social Networks," in Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics, 3009-3016 (2011).

[23] Santos, E.E., Santos Jr., E., Pan, L., and Wilkinson, J.T., "Culturally Infused Social Network Analysis," in Proceedings of the International Conference on Artificial Intelligence (IC-AI), 449-455 (2008).

[24] Santos Jr., E., and Zhao, Q., [Adversarial Models for Opponent Intent Inferencing], in Adversarial Reasoning: Computational Approaches to Reading the Opponents Mind, A. Kott and W. McEneaney, Eds., Chapman & Hall/CRC, Boca Raton, 1-22 (2006).

[25] Santos Jr., E., and Santos, E.S., "A Framework for Building Knowledge-Bases Under Uncertainty," Journal of Experimental & Theoretical Artificial Intelligence 11(2), 265-286 (1999).

[26] Santos Jr., E., Wilkinson, J.T., and Santos, E.E., "Bayesian Knowledge Fusion," in Proceedings of the 22nd International FLAIRS Conference, 559-564 (2009).

[27] Pan, L., and Santos, E.E., "An anytime-anywhere approach for maximal clique enumeration in social network analysis," in IEEE International Conference on Systems, Man and Cybernetics, 3529-3535 (2008).

[28] Kurose, J.F., and Ross, K.W., [Computer Networking, A Top-Down Approach Featuring The Internet], Addison Wesley Longman (2001).

[29] Zhang, Y., Abu-Khzam, F., and Baldwin, N., "Genome-scale computational approaches to memory-intensive applications in systems biology," in Proceedings of 2005 ACM/IEEE conference on Supercomputing (2005).

[30] Cartwright, D., [The nature of group cohesiveness], in Group dynamics: Research and theory, 91-109 (1968).

[31] Northway, M.L., and Weld, L., [Sociometric testing: A guide for teachers] (1957).

[32] Reffay, C., and Chanier, T., "How social network analysis can help to measure cohesion in collaborative distance-learning," in Proceedings of the International Conference on Computer Support for Collaborative Learning, B. Wasson, S. Ludvigsen, and U. Hoppe, Eds., 343-352 (2003).

[33] Indik, B.P., "Operational size and member participation: Some empirical tests of alternative explanations.," Human Relations 18, 339-350 (1965).