Military Scenarios and Solutions from a Network Science Perspective

Ladan Gharai
ladan.gharai@baesystems.com

Kyle Guan
kyle.guan@baesystems.com

Reza Ghanadan
reza.ghanadan@baesystems.com

BAE Systems, 164 Totowa Rd,
Wayne, NJ 07474

Abstract—Network science has recently received a considerable amount of attention from the military and research communities. In this paper we analyze two military scenarios from a network science perspective. We discuss the pros and cons of problem solving for these scenarios using the current fragmented approach versus applying a unified view across three domains: social/cognitive, information, and communication. We perform a step by step evaluation of each scenario. At each stage we present and compare existing solutions with those provided by network science based approaches available through future advances in basic and applied network science research. Our goal is to highlight advantages and challenges in network science research by way of example.

Index Terms—Network science, social networks, communication networks, knowledge networks, collaboration and ontology.

I. INTRODUCTION

Our current life-style depends on networks in many different forms: transportation systems, power grids, telecommunication systems, financial networks, social networks, etc.; however, our understanding of these networks is still somewhat limited. This is especially true of communication and information networks. Although these networks have only developed in the last few decades, our society is heavily impacted by them, in many diverse aspects, such as our educational, financial and health systems. Despite this dependence, it is generally accepted that we are unable to accurately model these systems, predict their behaviors, secure them from adversaries or understand how they operate under extreme conditions and stress.

The field of network science, attempts to better understand different networking domains and their impacts and interrelations with each other. Currently, there is no real consensus about the boundaries of network science. In its 2005 report “Network Science” [1] the National Research Council (NRC) tentatively defined network science as “the study of network representations of physical, biological, and social phenomena leading to predictive models of these phenomena.” One of the key motivations for studying network science is the Army’s Network Centric Warfare (NCW) doctrine – where mission effectiveness is increased by a robustly networked force with improved information sharing and collaboration capabilities. This access to information and knowledge enhances the forces’ situational awareness and speed of command to fulfill the NCW vision.

As related to NCW, network science is often depicted as the intersection of social and cognitive, information, communication, and physical networks (Figure 1). Social/cognitive networks represent the human dimensions of networks: shared understanding, social network analysis (SNA), physiology, sociology, relationship development between communities and organizations, distributed planning, and decision making. Information and knowledge networks include concepts such as knowledge management, situational awareness, information fusion, and Web 2.0 concepts. Underlying all these networks are the communication and physical (wired or wireless) networks.

Figure 1: Network science, networking domains and research areas.
In this paper we present a close look at two typical military scenarios and outline the role of each network domain in these scenarios. This work was motivated by the case studies from battlefield operations presented in the NRC report [1], which demonstrate the complexity of integrating network science on the battlefield at the knowledge and social/cognitive levels. This study and introspection provided a better understanding of the challenges facing the field of network science.

The rest of the paper is organized as follows. In Section II, we analyze two military scenarios to show how the study of network science can improve mission planning and operation. In Section III, we address the challenges in applying network science, and we conclude our work in Section IV.

II. NETWORK SCIENCE ON THE FIELD

A. Scenario I: Sensor-Mission Assignment

![Figure 2: A military scenario involving social networks, information networks and communication networks.](image)

Intelligence, surveillance, and reconnaissance (ISR) operations involve the participation of different network domains. Figure 2 depicts a dynamic ISR sensor-mission assignment scenario [2] in a coalition context. Each network domain is marked in the figure. The social networks are formed by inter-related communities of interest (CoIs) and soldiers on the field. The knowledge network consists of knowledge and information databases accessed via the Global Information Grid (GIG) reach-back; sensor-networks and wireless connectivity represent communications networks.

The arrows in Figure 2 show the flow of information between components of each network domain. For example, data and/or information is exchanged between the GIG (effectively considered part of both the information and communication networks), the CoIs, soldiers in the mission theater, the information delivery modules of the sensor network, and the information fusion module of the communication network.

The various CoIs and coalition groups communicate and cooperate with each other to set and articulate mission goals and objectives. These must be translated into machine understandable form, so they can be parsed into a set of sensor-tasks. These tasks are then mapped to assets and sensors in the theater. Information obtained from these sensors is fused together with live intelligence from the mission theater and knowledge data bases, and delivered to the CoIs. Ideally, to increase mission success rate and flexibility, all exchanges of data and information between the different domains would happen iteratively in real-time during the life-time of the mission. That is an interactive process would dynamically feedback information garnered form raw field data to the CoIs. The CoIs then would discuss and adjust their goals based on this real-time update, followed by flowing down the new requirements to the communication networks, and finally repeating this process. With increased transparency and communication between these domains, we achieve higher mission success rates. To this end, at a minimum, the following challenges need to be addressed:

**A dynamic environment.** ISR in a coalition environment is challenging on a number of fronts. The coalition groups have different sizes and capabilities – ranging from well-trained and well-equipped national forces to small groups of individuals who possess knowledge of local geography and culture. In addition, coalition members may join and depart the coalition based on individual goals and capabilities. As such, this presents a difficult problem for conveying and translating the mission goals and objective developed by the CoIs, in concert with the social networks, into a technical format that can be mined by the information networks and mapped to the ISR assets. Addressing information transfer is especially important in an operational environment that is highly dynamic, where asset and sensor inventory can change due to any number of reasons. For example a previously engaged asset can become available, or conversely a key asset may experience technical failure, or become unavailable due to other reasons. So while the social networks (soldiers in the field) may be flexible, unless the system is engineered to
handle and react to such changes, the information from the social network cannot be absorbed by the rest of the system.

**Information exchange between network domains.** One of the main barriers to executing this scenario in real-time is the issue of how to implement the exchange of information between the domains as represented by the arrows in Figure 2. In [2], it is assumed that the CoI question of “is there suspicious activity on the MSR road?” is translated into a machine-parseable language, which can then be used by the sensor-task fitting module. It is relatively straightforward to write a module that can carry out the translation from a pre-formed set of phrases to the machine language of a particular set of sensors. The complexity of this problem is in supporting and providing a standardized and universal context and framework for the exchange. Due to the wide variety of data and types, state representation needs to be expressed in terms of more than a simple numerical representation (such as a mean and a covariance). To address these issues, ontological analysis conducted within the three domains of network science is needed. The analysis must help to derive data schemas that can effectively and flexibly capture the information pertinent to the operational context. These schemas will encode attribute values, pedigrees, and the relationships that can exist between attribute values. CoIs and other social groups involved will be provided with greater capability to cope with the different types of information presented.

**Security and information assurance.** Any information exchange raises the issue of security, and exchanging information between different network domains adds complexity. Securely disseminating mission critical tactical intelligence to the pertinent people in a timely manner is a critical factor to mission success. While information sharing across traditional organizational boundaries is becoming a necessity, it is important to mitigate the risk of unauthorized information disclosure. Managing risk of sensitive information leakage across multiple organizations with potentially conflicting objectives, policies, and cultures represents a great challenge. Trust management, developed based on a cross-discipline study of the notion of trust worthiness, can provide flexibility to accommodate these needs and be responsive to the dynamic coalition environment.

### B. Scenario II: Tactical and Operational Decision Making “Blue” vs. “Red”

In the second scenario, we consider the tactical and operational decision making of the “Blue” team against the adaptive adversary “Red” team [9]. As illustrated red team plans to set off an improvised explosive device (IED) vehicle in an urban area. The red team prepares the operations in a safe house where shipments of IED materials are received and bombs are assembled. The organization leader (also called red actor) of the red team instructs the time and location of the coming attack. The red team members at the safe house plan to deliver the IED to the target location. Based on prior knowledge of red activities, blue team is equipped with two unmanned aerial vehicles (UAV) to perform area surveillance. In addition, blue team has a signal intelligence (SIGINT) division (also called blue actor) that monitors cell phone communications to localize certain red actors.

The scenario starts when blue team receives information (presumably from an informant in red team) about the description of a suspected bomb materials delivery truck going to the safe house. Blue team first commands UAV-1 to locate and track the suspected bomb materials delivery truck. As the truck enters the area of the bomb factory, blue team initiates SIGINT to monitor cell phone calls. At this time, red leader informs the safe house about the arrival of the bomb materials delivery truck. Upon obtaining this information via cell phone interception, blue actor directs UAV-2 to the area to track the IED vehicle. Once the truck stops at the IED attack location, SIGINT intercepts another red cell phone call for red lookout agent to initiate the explosion. Acting on this newly obtained information, the blue team identifies the lookout location, captures the suspects, and subsequently locates the safe house.

A number of scenario excursions (what-ifs) can be developed in addition to the main success scenario. One of the excursions involved a cyber attack on the downlink used by UAVs to transmit images from their current field of view to the ground station UAV operators. As such, the UAV operator was obviously not able to control the UAVs thus causing a mission failure. In yet another similar excursion,
SIGINT detected the cyber attack and informed blue’s Cyber Cell Division which after certain time-period performed Anti-Jamming (AJ) to restore UAV downlinks. In this case, the UAV operators were again able to guide the UAVs, albeit with a delay caused by the cyber attack. The overall mission performance could be impacted.

How does an integrated view of networks and network science support decision making in this scenario and in the presence of a dynamic and adaptive adversary?

We note that from the social/cognitive perspective, blue team’s knowledge of the organization hierarchy, activity region, and communication pattern is crucial in intercepting the information exchanged within the red team and timely locating the attack location.

From the information network perspective, how to correlate and efficiently fuse and report the data plays a critical role in supporting decision making. As shown in the scenario and subsequent excursions, the types of information are multi-modal; they include images and video collected by UAVs, voice signals gathered by interception, and reports generated from human intelligence. Moreover, as the information is gathered from disparate sources, some of which are faulty by nature or vulnerable to adversary attack, security mechanisms need to be developed to detect faulty and malicious information sources and mitigate their impact in the decision fusion and making [7]. To accomplish this, knowledge about the social aspects of the red team can help evaluate the reliability of the information. For instance, prior knowledge of the red team’s hierarchy and activity pattern can correlate with an informant’s reports, to decide their trust worthiness. Last but not least, a reliable communication infrastructure with adaptive information flow provides a foundation for the decision process. As shown in the scenario excursions, timely anti-jamming can restore the downlink, thus ensuring the continuation of the mission.

III. CHALLENGES IN APPLYING NETWORK SCIENCE

In studying and applying concepts of network science to real-life military scenarios, we found that one of the main challenges the field faces is the cross-cutting aspects of networks science. In each of the network domains, key research challenges are well understood, and there exists a large body of research and experts. However no clear roadmap exists for understanding the impact and intersection of the domains. Figure 4 presents a cross-cutting matrix of research challenges and metrics in each of the domains and the two-by-two intersection of domains. For example, as shown in row one, column two of the figure, research challenges shared by communication and information networks include scalability, reliability of data storage and data retrieval, and data distribution in peer-to-peer systems.

Below we identify five overall areas of complexity in the cross-cutting aspects of network science. In addition to those cited in [1], we believe these complexities pose challenges in network science application and integration.

A. Ontology

Each of the three domains of network science has its own specialized parlance and ontology. Researchers and scientists from different domains interpret terms and language differently and according to their specific field. This can be a hindrance to the advancement of network science and must be addressed.

We illustrate this issue by reviewing the definitions of trust in each domain. In the social sciences, one of its widely used interpretations (in addition to numerous other definitions) is “the expectation of benevolent behaviors from others” [5] [6]. In knowledge networks it is frequently interpreted as reliability. This is more of an operational definition of trust and relates to information accuracy and reliability. Accuracy reflects the deviation of the information from truth, and reliability is confidence in the assessment of accuracy. In literature related to communication networks, trust is frequently reduced to a binary value of [0, 1] [7][8]; this value is either attributed to a node or to the connection between nodes.

To effectively conduct cross-cutting research between these networking domains, it is important to recognize the diversity and differences in ontology and work towards developing common concepts, terms, and models. For example, in the case of trust, how can a real value of trust between [0,1] be mapped to a definition of trust as understood in the social domain, and vice versa?

<table>
<thead>
<tr>
<th>Communication Networks</th>
<th>Information Networks</th>
<th>Social/Community Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metrics:</td>
<td>Metrics:</td>
<td>Metrics:</td>
</tr>
<tr>
<td>Latency, packet loss</td>
<td>Quality of service,</td>
<td>Consensus, information</td>
</tr>
<tr>
<td>BER, PER, throughput,</td>
<td>quality of information, access and reliability</td>
<td>assurance and accuracy</td>
</tr>
<tr>
<td>Energy, signal strength</td>
<td>inter-network and intra-network</td>
<td></td>
</tr>
<tr>
<td>Research Challenges:</td>
<td>Research Challenges:</td>
<td>Research Challenges:</td>
</tr>
<tr>
<td>Mobility, dynamic-connectivity,</td>
<td>Reliability, scalability, reliability, and security</td>
<td>Reliability of information, information fusion and sharing, inference, shared understanding</td>
</tr>
<tr>
<td>Activity pattern, trust</td>
<td>Storage and retrieval, peer-to-peer systems</td>
<td></td>
</tr>
</tbody>
</table>

Figure 4: Cross-cutting research challenges and metrics


**B. Tool and System Integration**

There are a number of different aspects to the issue of integrating tools and systems. There are technical and architectural challenges to integrating tools, systems, and technologies. Modeling and simulation tools operate in different domains, with different abstractions and time granularities. For example simulation in the social domain operates on time scales of days, months and even years. Simulations in the communication realm are useful in time increments of nano-seconds to second and maybe minutes.

How can simulations across these domains be conducted in a meaningful manner? How can models in different domains be abstracted in a meaningful and useful manner that will yield useful results?

In addition, there is the matter of intellectual property (IP) and licensing. IP must be addressed in a manner that benefits the IP holders, and encourages cross-collaboration. Addressing IP is important as it poses a road block to advances in network science. Many of the tools in each of these domains have been developed over the last decade or two; developing them from scratch again in a non-proprietary and open source form is almost akin to reinventing the wheel, and may not even be possible.

**C. Composition and Modeling**

The study of network science entails the study of large complex heterogeneous dynamic networks and networks of networks. One scientific method to better understanding and analyzing these systems is to apply the principle of separation of concern: view a system according to separate components as much as possible and minimize the interactions between those components.

In communication networks this concept has given us the layered protocol stack (some may argue this was an ad-hoc design). However recently this concept has been questioned and there has been an effort to systematically design network protocols as distributed solutions to some global optimization problems and use optimization decomposition, both horizontal and vertical, to holistically design protocol stacks [9]. This approach has gained traction in mobile ad-hoc and mesh networks, where all resources (bandwidth, power and connectivity) are very limited.

An interesting research question in network science is can we apply a cross-layer paradigm to create and understand large complex networks? Which method, or perhaps combination of approaches, will yield a better understanding of network science? This has implications on how we understand and define the relevant cross-cutting research challenges and metrics as the different domains relate to each other. What are the important metrics and variables at the intersection of the Venn diagram and how can we quantify and measure them?

**D. Collaboration**

A key ingredient to the success of network science is collaboration between researchers and scientists. Collaboration is needed to address the issues of ontology, tool integration and composition and modeling. Advances in science and technology have created uber-specialists in niche fields. Bringing these researchers together to explore problems and conduct collaborative research can be difficult; taking a systematic approach and providing incentives is crucial. A systematic approach entails:

- Utilizing high-end collaborative tools. Currently there exists a vast repertoire of collaborative tools. Making these tools available to researchers and encouraging their use can greatly impact collaboration between researchers.
- Holding joint cross-disciplinary workshops and conferences. This will both encourage joint publications and also bring researchers in contact with each other and will foster impromptu conversations and collaborations.
- Teaching and curriculum. This includes course and cross-disciplinary degrees, which prepares students and graduates to work and conduct research in cross-cutting areas.

In terms of incentives, the most basic incentive to conducting research in any area is providing support and funding. This can be in the form of scholarships for graduate students, support for research centers and funding of grants.

**E. Scalability**

Generally as the complexity of a network (measured in terms of number of users, protocols, applications, network elements, topological constraints, and functionality expectations) increases, the sheer volume of information that needs to be exchanged, stored, and processed in a global scale setting requires a highly scalable system to handle it. As such, scalability is a key design objective to avoid incurring prohibitive amounts of network traffic and turning the underlying communication network into a bottleneck. In other words, the trust enforcement mechanism and distributed decision making process need to provide the necessary flexibility, manageability, and performance as the disturbed network increases in size. Therefore we believe it is important to investigate the following two fundamental issues within all the domains of network science (social/cognitive, information, and communications):

- Identifying the structures and properties that allow a network to scale in terms of the measures of complexity;
- Characterizing how the network behavior changes as network scale changes. In particular, we investigate what rules and constraint models can assure the desired behavior across changes in scale.
IV. SUMMARY AND CONCLUSION

The US military is motivated to support fundamental and basic research in network science given the influence and potential impact on the Network-Centric Warfare doctrine. In this paper we presented two different military scenarios and discussed how the cross-cutting aspects of network science can aid in mission planning and success. In our study of these scenarios we identified some additional challenges to those listed in [1], such as addressing ontological differences, technical and licensing complexities in tool integration, options for composition and modeling, and scaling of large networks of networks.

In order to solve and address any of these challenges, however, a successful approach to cross-cutting collaboration between researchers and scientists from different domains and technical fields is crucial. Our recommendations for facilitating and encouraging collaboration are to first take a systematic approach and second provide incentives.

REFERENCES