2014

A Bayesian Abduction Model For Sensemaking

Paul W. Munya
North Carolina Agricultural and Technical State University

A Bayesian Abduction Model for Sensemaking

Paul W Munya

North Carolina A&T State University

A dissertation submitted to the graduate faculty

In partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Department: Industrial & Systems Engineering

Major: Human Machine Systems Engineering

Major Professor: Dr. Celestine A. Ntuen

Greensboro, North Carolina

2014

The Graduate School
North Carolina Agricultural and Technical State University
This is to certify that the Doctoral Dissertation of

Paul W Munya

has met the dissertation requirements of
North Carolina Agricultural and Technical State University

Greensboro, North Carolina
2014

Approved by:

Dr. Celestine Ntuen Major Professor	Dr. Eui H. Park Committee Member
Dr. Jung Hee Kim Committee Member	Dr. Daniel Mountjoy Committee Member
Dr. Tonya L Smith-Jackson Department Chair	Dr. Janis Oldham Committee Member

Dr. Sanjiv Sarin
Dean, The Graduate School

Biographical Sketch

Paul W. Munya obtained his Bachelors of Science in Electrical & Electronics Engineering degree from the Jomo Kenyatta University of Agriculture and Technology in Nairobi, Kenya in 1999.He received his Masters of Engineering degree in Industrial & Systems Engineering from Iowa State University in 2002. In the fall of 2004, he joined the doctoral program in Industrial & Systems Engineering at North Carolina Agricultural &Technical State University in Greensboro, North Carolina.

He has been the recipient of numerous honors and awards include a Southern Regional Education Board (SREB) Alliance for Graduate Education and the Professoriate (AGEP) scholar award, a North Carolina Alliance to Create Opportunity through Education NC OP-TED award and a Sloan Doctoral Scholarship awarded by the National Action Council for Minorities in Engineering (NACME). He has presented his research at international conference meetings and workshops including the International Command and Control Research and Technology Symposium (ICCRTS), Institute of Industrial Engineers (IIE) Annual conference, Human Interaction with Complex Systems (HICS) Symposiums and the Human-Computer Interaction (HCI) International Conference

While pursuing his degree, he works for the United States Army Research Laboratory as a Human Systems Integration Engineer stationed at the Tank Automotive Command (TACOM) headquarters in Warren, Michigan. Before his current assignment, he worked as a Senior Specialty Engineer for Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) at BAE Systems, a Department of Defense contractor.

Dedication

To the Almighty God,

For the abundant blessings; friends, family, mentors

And good people from all walks of life

That I have met along this journey

So far away from home

&

To my family

For the motivation to get up every morning

And new dreams to pursue every day

Acknowledgements

I would like to express my gratitude and many thanks to my advisor Dr. Celestine Ntuen for supporting me over the years, personally and professionally and showing extraordinary patience to make sure I got this done. For that, I'm forever grateful. I would also like to thank Dr. Eui Park, my committee member, graduate advisor and mentor for the tremendous support that I have received as a doctoral student since my enrollment to date. I express my gratitude to my committee members Dr. Jung Hee Kim for her constant encouragement and for always making time to listen to me and to Dr. Daniel Mountjoy for taking time to review and offering helpful suggestions.

The staff and faculty of the Industrial & Systems Engineering department have been a wonderful family to me. They have created a great environment of mentorship and instruction for students to excel professionally and for that they are truly exception. I express my sincere thanks to all of them starting with Chair, Dr. Tonya L. Smith-Jackson and extending to all the faculty and staff. A special recognition is given to Mrs. Elizabeth Brooks who has received probably a million phone calls and emails from me and patiently responded to each of them with the same courtesy and professionalism. She is truly a wonderful person. Special thank you as well to Dr. Salil Desai who has always found time to talk to me not only professionally but as a friend.

At ARL, I would like to thank my supervisor, Ms. Belinda Lutas-Spencer, for giving me all the accommodation I needed to work on this. She is a true blessing from God. To my friends Ben, Femi and Emeka, thank you for the encouragement over the years. Lastly I would like to thank my parents Syphrosa and Christopher Munya for their prayers and encouragement and for always believing in me, even from tens of thousands of miles away.

Table of Contents

List of Figures

List of Tables

Abstract

This research develops a Bayesian Abduction Model for Sensemaking Support (BAMSS) for information fusion in sensemaking tasks. Two methods are investigated. The first is the classical Bayesian information fusion with belief updating (using Bayesian clustering algorithm) and abductive inference. The second method uses a Genetic Algorithm (BAMSS-GA) to search for the k-best most probable explanation (MPE) in the network. Using various data from recent Iraq and Afghanistan conflicts, experimental simulations were conducted to compare the methods using posterior probability values which can be used to give insightful information for prospective sensemaking. The inference results demonstrate the utility of BAMSS as a computational model for sensemaking. The major results obtained are: (1) The inference results from BAMSS-GA gave average posterior probabilities that were 10^3 better than those produced by BAMSS; (2) BAMSS-GA gave more consistent posterior probabilities as measured by variances; and (3) BAMSS was able to give an MPE while BAMSS-GA was able to identify the optimal values for kMPEs. In the experiments, out of 20 MPEs generated by BAMSS, BAMSS-GA was able to identify 7 plausible network solutions resulting in less amount of information needed for sensemaking and reducing the inference search space by 7/20 (35%). The results reveal that GA can be used successfully in Bayesian information fusion as a search technique to identify those significant posterior probabilities useful for sensemaking. BAMSS-GA was also more robust in overcoming the problem of bounded search that is a constraint to Bayesian clustering and inference state space in BAMSS.

CHAPTER 1

Introduction

1.1 Background

In the last decade, asymmetric warfare has evolved into complex multifaceted conflicts in all the major trouble spots around the world. The conflicts have involved conventional armies of nation states against a proliferation of non-state actors that carry out sustained insurgencies against the superior armed forces. The end states of these insurgencies, the motivations, and tactics vary from one insurgency to another, introducing a level of complexity into the battlespace that requires military strategists to adopt new ways of thinking to cope with the complexities. Often, these insurgencies are nested in complex conflicts involving third and fourth forces (Metz, 2003) the insurgents themselves, and the regime.

Consider the most recent military conflicts in Iraq and Afghanistan. The adversary environment is known to be complex, "wicked" and completely asymmetric - the adversaries are barely known, and their tactics keep changing against the coalition forces. The conventional forces have superior weaponry, resources and manpower enabling their domination in ground and air maneuvers, while the adversaries have the advantage of superior terrain knowledge, no time constraints, and support from the local population making them dominant in guerilla maneuvers. The deliberate Military Decision Making Processes (MDMP) with all their linearity assumptions collapse immediately when they come in contact with asymmetric information environments. Generating courses of action must be progressive and opportunistic - the usual analytical models of judgment and choice that fit force-on-force tactics must be recalibrated to fight unknown enemies.

Traditionally, this kind of problem has been addressed using Boyd's (1987) *Observe, Orient, Decide, and Act* (OODA) model which cognitively aligns the battle staff's intuitive estimates through a linear space of "Observing" the data, "Orienting," "Deciding," and "Acting." Usually mentioned anecdotally is the sensemaking aspect of the Orient stage in the OODA (Breton & Rousseau, 2005). It is believed here that by improving the sensemaking aspect of the OODA with analytical models, the commander's decision making could be improved (Munya, Trevino, & Ntuen, 2005).

A commander must draw inferences from uncertain data, identify appropriate sequences of objectives and optimally assign resources to ensure their attainment (Thoms, 2003). In recent decades, information has been obtained by employing sensors, data fusion and communication systems that support inferential reduction of uncertainty in battlespaces. In the context of asymmetric warfare, the ability of the commander to swiftly decide to counter the enemy's insurgent behavior puts more mental load on the staff and the commander owing to the quantity of information to be processed. Making sense of dynamic, multivariate information to establish a reasonable, justifiable belief about the adversary's intent has become a hard, cognitive, analytical problem (Ntuen, 2009).

As noted by Van Creveld (1985), there are four contextual processing regimes which influence the commander's decisions - the organizational, operational, informational and inferential components. Organizationally, the commander must deal with the stratified hierarchical nature of the military structure at the strategic, operational, and tactical levels. Operationally, he must have a complete understanding of the entire theater of war and the spectra of mapping one's forces to counter the enemy's plans. From an information perspective, the commander must align the battle staff to develop the best Courses of Action (COA) estimates

using the varied information available. Additionally, in making decisions, the commander must be able to deal with the current situations in the field and make probabilistic inferences about the future of the battlefield and the adversaries (Thoms, 2003).

Given the four macro-regimes of the command space, the ability of the battle staff to develop a reasonable, but plausible rough estimate of the battle COA depends in part on their sensemaking ability under the flux of battlespace information from the many information generating mechanisms including humans and technology. The commander's battle staffs, though aided by technology, still rely on their intuition to understand the evolving situation. This sensemaking process begins when both the commander and the staff assess the battle situation by extrapolating their apriori knowledge onto the existing information space to understand the ground realities.

1.2 Sensemaking

Much of the epistemological discussions of sensemaking especially the adoption of the sensemaking construct and its impact on research paradigms, theory, and methodology, has occurred in the social and management circles (Weick, 1995) which have yielded most of the definitions of sensemaking. Weick defines sensemaking as a process involving identity, retrospect, enactment, social contact, ongoing events, cues and plausibility (1995). Huber (1991) introduces the concept of "active agents" capable of constructing sensible and sensable events.

From information fusion discipline, sensemaking involves putting stimuli into some kind of framework (Starbuck & Milliken, 1988).When people put stimuli into frameworks, this enables them to "comprehend, understand, explain, attribute, extrapolate and predict." Sensemaking is also viewed as a thinking process that uses retrospective accounts to explain surprises (Louis, 1980).Thomas, Clark and Gioa describe sensemaking as the "reciprocal

interaction of information seeking, meaning ascription and action" (1993, p.240). Sackman (1991) talks about sensemaking mechanisms that organizational members use to attribute meaning to events, mechanisms that include the standards and rules for perceiving, interpreting, believing and acting that are typically used in a given cultural setting (p.33). Feldman and March (1988) define sensemaking as an interpretive process that is necessary for "organizational members to understand and to share understandings about such features of the organization as what it is about, what it does well and poorly, what the problems it faces are and how it should resolve them." Ring and Rands (1989) define sensemaking as a "process in which individuals develop cognitive maps of their environments" (p.342). In military circles, sensemaking is defined as a multidimensional process of developing an operational understanding and awareness within a complex and evolving task domain (Leedom, 2004).

These definitions point to sensemaking as a concept, a process or even a structural framework. Conceptually, sensemaking is presented in terms of principles and theories (Ntuen, 2006). By general definition, a principle refers to an assumption, a basic truth, or law that must hold for an entity to be accepted as such in the field of research. As a process, sensemaking is defined in terms of situated (contextual) actions, informational or symbolic level of processing, and cognitive information processing that is mainly tacit knowledge explication. As a structural framework, sensemaking can be viewed as an ontological link of information from individuals or organizations for the purpose of discovering intrinsic values for decision making.

Ntuen, Park, and Kim (2013) note that information is the heart of the sensemaking process. In cases where the required information may be completely missing, the sensemaking process starts with making guesses using retrospective knowledge. The information may be incomplete, in which case the sense-maker becomes an intuitive statistician, mentally estimating

and connecting dots. Finally, information may be overwhelmingly too much. For example, in military command and control centers, there is a multitude of sensor devices generating information in real-time.

Relevant to knowledge management, Ntuen, Park, and Kim (2013) further observed three major characteristics of sensemaking:

(a). Sensemaking is an aspect of information foraging: Pirolli and Card (1999) define the Information Foraging Theory as an approach to understanding how strategies and technologies for information seeking, gathering, and consumption are adapted to the flux of information in the environment. The theory assumes that people, when possible, will modify their strategies or the structure of the environment to maximize absorption of valuable information. Pirolli and Card (2005) note that foraging tasks consist of information gathering, representation of the information in a schema that aids analyses, the development of insight through the manipulation of this representation, and the creation of some knowledge product or direct action based on the insight.

(b). Sensemaking is an information fusion tool: Sensemaking is viewed as a thinking process that uses retrospective accounts to explain surprises (Louis, 1980, p.241), and uses new information to update prospective states of a situation. Previously, Munya and Ntuen (2007) have used this axiom to develop an Information Fusion Model using Bayesian Information Updating.

(c). Sensemaking supports situation understanding: The overarching goal of sensemaking as noted by Starbuck and Miliken (1988) is information interpretation through the process whereby stimuli is placed into some kind of framework as a consequence of which, the situation is understood. Comprehending the situation supports better judgments, decisions and

actions. Klein (2006) describes sensemaking as the set of processes involved in trying to improve an individual's understanding of a situation, often in response to surprise. Malhotra (2001) notes that by understanding a situation, we can conceptually link available information and the expected result or the anticipation of task outcomes. It helps us understand the gap between performance expectations based on information in context (Malhotra, 2001; pp. 120).

1.3 Challenges in Fusing Information from Asymmetric Battlespace to Support Sensemaking

In the asymmetric battlespace environments, the deliberate MDMP with all their linearity assumptions are generally deemed inadequate. COA generated must be progressive and opportunistic rather than contextual and analytical. While contextual and analytical models of judgment and choice fit force-on-force tactics, they are much less adaptable to asymmetric battlespaces. Sensemaking for asymmetric battlespace information management has been advocated by Bodnar (2005); Leedom (2004, 2005); Leedom and Eggleston (2005); Ntuen (2006, 2008); Klein (2006), and Good et al., (2004). Even among these researchers', there is a consensus that sensemaking is anecdotal and prescriptive because it is governed by expert judgment and experience.

There are also many problems and gaps in the literature with respect to developing analytical models to capture sensemaking. These gaps are enumerated and described below:

(a). Asymmetric information is generally characterized with equivocation, different types of uncertainties, ambiguities and surprises, emerging and evolving information, and complexities, among others.

(b). There is a problem of scale related to information complexity in military command and control (C2) organizations. For example, there are challenges in applying closed-form

mathematical models such as Bayesian Models to a battlespace system even at the brigade and lower levels mostly due to the information-handling costs.

(c). Most analytical models lack the robustness to deal with sensemaking problems arising from non-crisp information.

(d) Lack of cognitive architectures that support the ability to fuse core knowledge and use such knowledge in performing meta-reasoning with the available information in novel situations. Core knowledge, serves as apriori information to a decision maker and is a key sensemaking input.

Given the above challenges, some critical issues giving impetus to this research can be identified for the analytical modeling of the sensemaking process as:

- Development of a framework that can computationally represent sensemaking with all its tacit dimensions of knowledge as a model of human cognition.
- A reasoning construct supported by Bayes Theorem that can support the sensemaking process. Bayesian Networks are propositional in nature and have inherent limitations in their expressive powers.
- Development of an architecture that can sufficiently combine and represent the expressive nature of Bayesian Networks with the ability to handle multiple types of uncertain information while increasing information entropy.

1.4 Research Goals and Objectives

This research aims to develop a Bayesian Abduction Model for Sensemaking Support (BAMSS). The application domain is for the analysis of military Courses of Action. The research objectives are broadly defined as:

1. To develop a sensemaking analytical model to support military commanders in integrating information from various sources in asymmetric battlespace. The modeling

process is centered on using a Bayesian Network to represent causal relationships among the decision variables and perform abduction reasoning to get the most explainable causes.

2. To validate a prototype BAMSS using case situations from asymmetric warfare.
3. To improve and optimize the BAMSS output by using a genetic algorithm to seed the relevant Bayesian data.

1.5 Intellectual and Broader Impact Contribution

The research demonstrates the development of a sensemaking analytical model using a Bayesian Network. Bayesian Networks are used as knowledge representation and analysis tools. A Bayesian Network was chosen because of its robustness to make abduction inference - typical of sensemaking in that it looks for the most probable cause-effect relations within the information. It is believed that Bayesian algorithms will enable real-time information fusion, thus easing the process of sensemaking, especially, testing multiple competing hypotheses from a domain-specific large database. We also demonstrate that the model is robust and scalable and can be applied to many different situations that require information fusion.

1.6 Chapter Summary and Thesis Overview

Chapter 1 introduces the research topic, the problem statement, the research goals and objectives, the challenges encountered in the research and the general contribution to the scientific body of knowledge. Chapter 2 discusses the contextual framework of sensemaking analytics. Chapter 3 presents the Bayesian formalism as a mathematical model for knowledge representation in a sensemaking context. A discussion of abductive inference for BAMSS is also presented. Chapter 4 presents the BAMSS information and functional architecture, the

computational platform requirements (software and hardware), sample computational algorithms, and sample case vignettes. Chapter 5 extends the discussion of the BAMSS model by incorporating a Genetic Algorithm to improve and optimize the output. Chapter 6 presents the research summary, observations, conclusions, and recommendations for further research.

CHAPTER 2

Sensemaking Analytics

2.1 Contextual Framing

Analytical models of sensemaking focus mainly on the micro cognitive aspects of sensemaking at the individual level. The underlying theme is to isolate and represent aspects of cognition that humans rely on to understand events in uncertain environments. The dominant rubric in the development of these models has been to fashion them like linear decision support systems whose output is almost always linear. Such systems take the black box approach to the problem of sensemaking assuming that any number of inputs to the system can be processed by some algorithm to produce the right output. This works well if we are to assume a deterministic situation. The reality is that sensemaking is used for situations that are dynamic and complex with nonlinear behaviors.

Models for sensemaking analytics should consider uncertainty, contradiction, ambiguity, time-based behaviors, and indeterminacy which extend beyond the deterministic models. Anecdotally, the Think Loop Model (Bodnar, 2005) exemplifies these sensemaking characteristics by breaking down the analytical process into a nested series of "think loops" which indicate how analysts combine "bottom-up" data with "top-down" data to derive useful information. Leedom and Eggleston (2005) described a working simulation model of human sensemaking and decision-making within a future joint or coalition military Command, Control, Intelligence, Surveillance, and Reconnaissance (C2ISR) system. Their sensemaking framework uniquely integrated two areas of modeling; i) explicit representation of the knowledge framework (abstraction hierarchy) required for decomposing command intent into actionable knowledge within each of the Political, Military, Economic, Social, Information and

Infrastructure (PMESII) dimensions of the battlespace and ii) explicit representation of the staff work flow and patterns of collaboration within the various centers, working groups, cells, and teams that build this knowledge framework.

Other analytic models of sensemaking examine the cognitive and external resource cost of sensemaking (e.g. by Russell, Stefik, Pirolli, & Card, 1993), the effects of tools on the behavior of people doing rapid large-volume data assessment (Russell, Slaney, Qu, & Houston, 2005), rapid understanding of large document collection (Russell &Slaney, 2004) and visual sensemaking (Chi & Card, 1999; Card, 2004; Russell, 2003). The next section examines different approaches to qualitative models of sensemaking.

2.2 Qualitative Models of Sensemaking

Several qualitative models have been proposed for sensemaking analyses. However, a unifying paradigm for sensemaking is currently lacking. Additionally, there is no general consensus as to how the sensemaking process might be operationally defined, analytically modeled, empirically tested, and critically assessed in terms of key constructs and variables, process interactions and obstacles, performance dimensions and metrics, and objective criteria for assessing the adequacy or sufficiency of outcome (Leedom, 2004).These models have been tailored to suit different domains ranging from Mission Command situations to business decision- making .

The OODA model was developed by Boyd and is commonly applied to military command and control decision-making situations. In the OODA model, the *Orient* phase attempts to capture the cognitive processes involved in sensemaking. A modified version of the model, the Cognitive-OODA (Breton & Rousseau, 2005), was developed in response to the military adoption of the Effects Based Operations (EBO) which emphasizes analytical rather

than conventional tactics. Endsley's Model of Situation Awareness (1995) closely mirrors the sensemaking process mostly at the level II Situation Awareness (SA). At level II SA, sensemaking represents the comprehension of information (transformation of information to knowledge).

Wiig (2002) describes sensemaking as a continuous integration of evolving situation-handling activities that are based on cognitive constructs. The model assumes that an individual's sensemaking process is based on four types of mental models: the Situation Recognition Model, the Decision-Making and Problem Solving Model, the Execution Method Model and the Governance Approach Models. In Shattuck and Millers' Dynamic Model of Situated Cognition (2004), sensemaking is viewed as a sequence of situated acts. Situated action models emphasize the emergent, contingent nature of human activity, and the way it grows directly out of the particularities of a given situation. A central tenet of the situated action approach is that the structuring of activity is not something that precedes it but only grows directly from the immediacy of the situation (Lave &Wenger, 1991).

Klein's (2004) Data/Frame Analytical Model focuses on the micro-cognitive aspects of individual sensemaking. Framing indicates how we structure problems into a particular set of beliefs and perspectives that constrain data collection and analysis. The Plan as You Execute (PAYE) model (Ntuen, 2006), was developed as a hybrid model incorporating a variety of the cognitive models discussed above. The model architecture is dependent on schema-based knowledge representation about the world, a question answering (Q-A) sensemaking query system, reflexive and reflective cognition models and the dynamic cognitive scripts or meta-cognition knowledge elements.

The non-linearity and complexity of the asymmetric battlespace has been analyzed using Complex Adaptive Systems Theory. Kilcullen (2004) defines the asymmetric battlespace as an open and complex adaptive system characterized by the non-linear interaction of its subordinate elements. Comprised of many dynamically interacting subcomponents, complex adaptive systems exhibit coherent behavior despite their highly dispersed and decentralized control structure (Kilcullen, 2004).

The complexity of asymmetric warfare has also been researched by a number of researchers (Ryan, 2008; Bar-Yam, 2004; Kilcullen, 2004). Ryan uses the Law of Multiscale Variety (Bar-Yam, 2004) to discuss two complex systems ideas (multiscale variety and adaptation) that underpin our understanding of asymmetric warfare. For a system with *N* parts that must be coordinated to respond to the external contexts, the scale of the response is given by the number of parts that participate in the coordinated response. Second, we assume that under (complete) coordination, the variety of the coordinated parts equals the variety of a single part. The induced sensemaking process is interpreted to operate on the same axiom of Law of Multiscale Variety—where information is subject to serious uncertainties and equally *N*-order entropy. The generalized Law of Multiscale Variety states that at every scale, the variety necessary to meet the tasks, at that scale, must be larger for the system than the task requirements.

The Cynefin Model (Kurtz & Snowden, 2003) emphasizes the effect of problem type and environment on the sensemaking and decision-making capabilities. The novelty of this model lies in its approach to problem-solving in a realm that encompasses all problematic situations. Combining Ryan's concept of multiscale variety and adaptation with this model of sensemaking, we argue that the context of MDMP in asymmetric battlespace spans both the *knowable space*

and the *complex space*. In the *knowable space*, also called *complicated order* or *Realm of Scientific Inquiry*, cause and effect relationships are generally understood, but for any specific decision it is imperative to gather and analyze further data to predict the consequences of a COA without any uncertainty. Snowden characterizes decision making in this space as {SENSE, ANALYZE and RESPOND}. Decision analysis and support require accurate fitting and use of models to forecast the consequences of actions with appropriate levels of uncertainty (French, 2013)

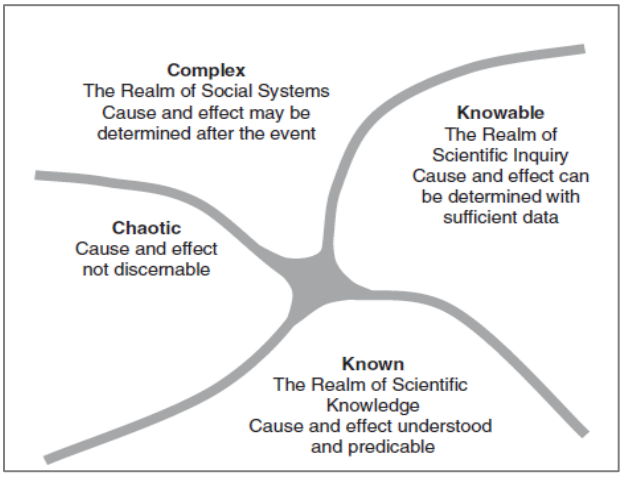

Figure 1. Cynefin Model. Adapted from Kurtz and Snowden, 2003.

In the *complex space*, also called the *complex unorder* or the *Realm of Social Systems*, decision-making situations involve many interacting causes and effects. Knowledge in this space is at best qualitative: there are too many potential interactions to disentangle particular causes and effects. There are no precise quantitative models to predict system behaviors as seen in *known* and *knowable spaces*. Decision-making is more focused on exploring judgment and issues and on developing broad strategies that are sufficiently flexible to accommodate evolving situations. Snowden suggests that in these circumstances, decision making is more of the form {PROBE, SENSE and RESPOND} (French, 2013). Analysis begins with informal qualitative

models. If quantitative models are used, then they are simple, perhaps linear multi-attribute value models (Belton & Stewart, 2002).

Bodnar (2005) developed a Think Loop Model (TLM) for sensemaking analysis that breaks the analytical process down into a nested series of "think loops" which indicate how analysts combine "bottom-up" data-driven steps with "top-down" hypotheses-driven steps to be able to forage through new data, and then synthesize that data into evidence-based schemas and theories. The TLM process considers many back loops within a sensemaking component cycle by using one set of activities that cycle around finding information and another that cycle around making sense of the information, with multiple interactions between them. Additionally, the upward processes fall into a single overall scheme for data-driven analysis while the downward arrows fall into a single overall scheme for hypotheses-driven analysis.

Russell, et al., (1993) developed the Sensemaking Thinking Loop (STL) as a continuous evolving state of reasoning about a problem context. The STL has three main processes, namely, search for representation, instantiating representation, and shifting representation, respectively. Searching for representations is designed to capture salient features of the data in a way that supports the use of the instantiated representation. Instantiating a representation identifies information of interest and encodes it in a representation that emerges from the generation loop. The instantiated schemas called *encodons* are created in the data coverage loop. Shift representation is designed to cope with contextual information changes and entails forcing a change in the representation via a bottom-up or data-driven process.

A diversity of efforts exists within the sensemaking community of practice. Therefore, Buckingham-Shum and Selvin (1999) note that, "there are not only gaps in the languages, frames of reference, and belief systems that people in the different communities of practice have, but

also gaps between their respective sensemaking efforts - their concepts in the representational situation. In many cases, different communities have mutually unintelligible sensemaking efforts, leading to mutually unintelligible representational effort."

2.3 Sensemaking Analytics Tools

The major difference between a Sensemaking Support System (S3) and a Decision Support System (DSS) is that S3 supports sensemaking activities, while DSS supports decision making activities. DSS has matured in its constructs and theories, and is usually designed to help an agent choose from the multiple options. S3s are relatively nascent and universally lack acceptable theoretical frameworks and constructs. An S3 will usually target problems in information foraging, diagnosis, information fusion, and help the sense-maker understand the specific problem situation.

The S3 is a product developed by Ntuen, Park, and Kim (2013) as a tool for information fusion during sensemaking within a military domain. S3 provides the backbone for developing a collaborative decision support system since it is designed for multiple users engaged in collaborative sensemaking. The tasks are defined at different strata of operational doctrines. The user can use maps, whiteboards, annotations, and graphics to illustrate facts or clarify arguments. The display model is implemented using the stages of the cognitive abstraction hierarchy which maps the requirements of sensemaking stages (Figure 2). S3 enables the users to develop and frame the hypotheses, analyze the hypotheses in the experimental domain, and provide cases for simulation experiments. The visualization and sensemaking support module in S3 provides a user interface and visualization support.

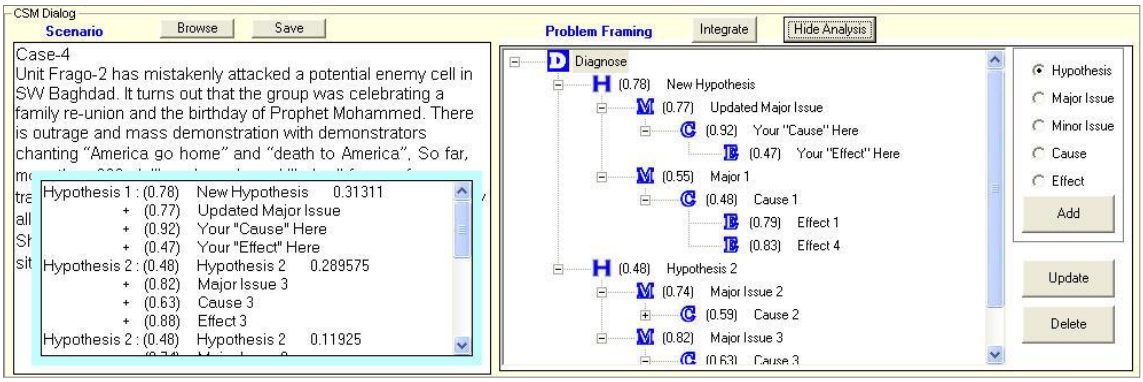

Figure 2. Visual analytics screen capture in S3

Good and his colleagues from PARC AI group (2004) developed the ACH_0 as an experimental program intended to aid intelligence analysis in sensemaking. ACH_0 is a table-oriented workspace for performing the Analysis of Competing Hypotheses (ACH). By accommodating multiple explicit hypotheses and systematic consideration of available evidence, the ACH method counteracts confirmation bias and other causes of inaccuracies. ACH_0 provides two simple algorithms for scoring evidence: an Inconsistency Counting Algorithm and a Normalized Algorithm. Both of these are intended only as rough guides for scoring hypotheses. The algorithms operate on the same data, but make different trade-offs.

Figure 3, a screen shot of ACH_0, illustrates its table format. The hypotheses under consideration in the example are the columns labeled H1, H2, and H3. Six items of evidence are present in the example in the rows labeled E1 through E6. In the ACH Method, each piece of evidence is assumed to be independent and the hypotheses are exhaustive and mutually exclusive. In Figure 3 an entry of "I" signals that this evidence is inconsistent with the corresponding hypothesis, and entry of "II" signals that it is very inconsistent with the evidence. The "C" and "CC" entries indicate two levels of consistency. Similarly, ACH_0 provides three levels of weight assigned to evidence. Roughly, this weight is a stand-in for a richer representation of the evidence quality.

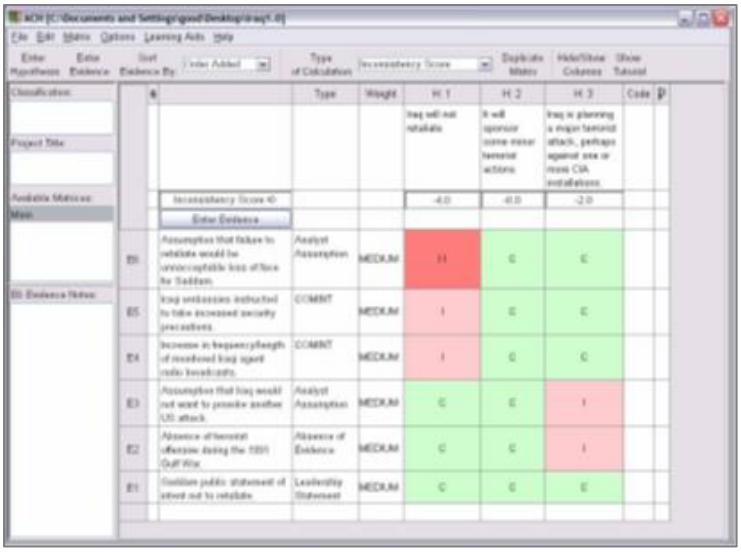

Figure 3. ACH_0 interface table (Good et al., 2004)

More recently, Lebiere et al., (2013) presented a computational cognitive model, developed in the ACT-R architecture of several core information-foraging and hypotheses-updating processes involved in a complex sensemaking task. In the context of an intelligence task analysis, the authors view sensemaking as the act of finding and interpreting relevant facts amongst the sea of incoming reports, images, and intelligence. They describe the computational module as an "explicit, unified, mechanistic and theoretical framework for cognitive biases that provides a computational understanding of the conditions under which such biases occur."

Using the Cognitive Architecture Model they provide a functional bridge from the qualitative theories of sensemaking to detailed neural models of brain functions. Testing the model entailed performance of experimental tasks using a task modeling approach for different sets of scenarios and human participants. The quantitative prediction of a number of cognitive biases by the model was then recorded and analyzed on a trial-to-trial basis. The model correctly predicted the presence and degree of four biases: confirmation, anchoring and adjustment, representativeness, and probability matching.

While there is a growing interest in sensemaking analytics, it is important to discuss the histories behind them. Among the first sensemaking support tools developed is the gIBIS (Conklin & Begeman, 1988). The gIBIS describes an application-specific hypertext system designed to capture early design deliberations. It implements a specific method, called Issue Based Information Systems (IBIS), which has been developed for use on large, complex design problems. An improvement on gIBIS is Compendium (Shum & Selvin, 1999), a software tool providing a flexible visual interface for managing the connections between information and ideas.

The Sensemaking Support Environment *by* Eggleston, Bearavolu, and Mostashfi (2005) is a tool developed to augment an intelligence analyst's cognitive capabilities. Similarly Sticha, Buede, and Rees (2005) have developed APOLLO, a software application that enables the analyst to reason through a prediction of a subject's decision making, to identify assumptions and determinant variables, and to quantify each variable's relative contribution to the prediction, by producing a graphical representation of the analysis with explicit levels of uncertainty.

CoSen (Furnas, Qu, &Sharma 2003) provides an integrated workspace for information gathering and sensemaking. It examines sensemaking activities across different levels of social aggregation and focuses on technological support of representations for sensemaking to improve knowledge enhancement in the context of information sourced from the web. A user with a sensemaking task searches the information on the web and organizes it into a hierarchical tree structure.

DECIDE (Cluxton & Eick, 2005) is an analytical engine for hypothesizing and visualizing structured arguments. The tool enables analysts to construct arguments, associate evidence with conjectures, sub-hypotheses, and hypotheses, set evidence credibility and

relevance, and score the arguments. WORKING BY WIRE (Gundry & Metes, 1996) is a software program that equips distributed team members to "work together apart". Going beyond the usual level of tool skills, WORKING BY WIRE addresses the behaviors, methods, approaches and protocols required to support distributed team work. A similar approach to sensemaking is seen in Livenet (Rura-Polley, Hawryszkiewycz, & Baker, 2000). DISCOVER (Milligan & Ahmed, 2005) and Battlesense (Klein, Long, Hutton, & Shafer 2004) have been developed specifically to support sensemaking in the battlefield environment.

COLAB (Morrison & Cohen, 2005) is a laboratory for studying tools that facilitate collaboration and sensemaking among groups of human analysts as they interpret unfolding situations based on accruing intelligence data. The laboratory has three components. The *Hats Simulator* provides a challenging problem domain involving thousands to millions of agents engaged in individual and collective behaviors, a small portion of which are terrorists. The second component, the *AIID Bayesian Blackboard*, is an instrumented working environment within which, analysts collaborate to interpret the problem domain. The third component is a web-based user interface that integrates the *Trellis* hypothesis authoring and management tool with a query language to allow human analysts to interact with AIID and each other. Collaboration Envelope (Nosek, 2005) follows a similar approach. In particular Collaboration Envelope develops architectures that support individual and group sensemaking.

SSIGS (Qu, 2003) is a sensemaking-supporting information gathering system whose workspace offers features that not only facilitate information search but also, a representation search and representation shift that are crucial for sensemaking tasks. ClaimSpotter (Sereno, Shum, & Motta, 2004) is a text-driven interface that facilitates the creation of argument maps expressing, for instance, the position of multiple annotators over a particular problem. Such

concept maps could be used to represent the perspective taken on a domain, according to the different annotators (and potentially authors) of the documents being connected. A critical look at the tools developed points to the gradual shift from decision support tools to sensemaking support tools. The latter focuses on augmenting the cognitive capability of the sensemaker during the whole process of sensemaking.

2.4 Chapter Summary

Chapter two reviews both, the qualitative and the analytical models of sensemaking. From qualitative analyses, most researchers focus on cognition where the primary sensemaking task is to construct a meaningful mental representation of the problem space. Schema-driven representation, mental models, and other cognitive constructs dominate the process models of sensemaking that are discussed. These models give an understanding of the meta-cognitive and cognitive acts that inform the sensemaking process and how they may be applied to understand and overcome the cognitive limitations of the human mind. The limitations of this approach lie primarily in the lack of a unifying paradigm of sensemaking. An additional challenge exists in the way this information may be used to develop a unifying framework or standardized guidance for the development of better sensemaking support systems.

Research on sensemaking analytics is presented as a tool to support the sensemaking process. In this approach, sensemaking models are defined as computational cognitive models whose primary task is to enable processing of information to achieve an understanding of the problem space and facilitate effective analysis process. Most of the models discussed have been developed for the fields of intelligence analysis, information foraging and knowledge management. The tools developed indicate a gradual shift from decision support tools to

sensemaking support tools which focus on augmenting the cognitive capability of the sensemaker during the whole process of sensemaking.

This research uses the tool-based approach to model the sensemaking process for two reasons: First, the advances in Computational Intelligence have led to the development of powerful and efficient algorithms and methods that can be used to computationally simulate some processes in sensemaking. For example, it is possible to represent sensemaking models in software and cognitive architectures. The algorithms also enable better user interaction with the models, thus simplifying the process of task performance and analysis in scenarios where sensemaking is required. Second, through the use of computational techniques such as Bayesian Networks and Abductive Inference, both the qualitative and quantitative approaches can be combined to provide a better representation of the sensemaking process.

CHAPTER 3

Bayesian Models for Sensemaking

3.1 Bayes Theory and Abductive Inference

Any situation in which we have to make decisions often necessitates hypothesizing from a sample space *H*, given some observed data *D*. Bayes Theorem provides a way of calculating the probability of a hypothesis based on its prior probability, the probabilities of observing various data given the hypothesis and the observed data itself. To define Bayes Theorem precisely, we first need to define the notations used. Let *P(h)* denote the initial probability that hypothesis *h* holds, before we incorporate any new data. *P(h)* is the prior probability of *h* and may reflect any background knowledge we have about the chance that *h* is a correct hypothesis. If no such prior knowledge exists, let *P(D)* denote the probability that evidence data *D* will be observed. *P(D)* represents the probability of evidence *D* given no knowledge about which hypothesis holds. Let *P(D|h)* denote the probability of observing data D given a situation where hypothesis *h* holds. We are interested in the probability *P(h|D)* that *h* holds given the observed data *D*. *P(h|D)* is called the posterior probability of *h* because it reflects our confidence that *h* holds after we have seen some evidence *D*.

Bayes Theorem provides a way to calculate the posterior probability *P(h|D)*, from prior probability *P(h)*,together with *P(D)* and *P(D|h)*. This is mathematically stated as,

$$P(h \mid D) = \frac{P(D \mid h)P(h)}{P(D)} \tag{1}$$

In this formalism, propositions are given numerical parameters signifying the degree of belief accorded to them under some body of knowledge, and the parameters are combined and manipulated according to the rules of the Probability Theory. For example, if *h* stands for the

statement " An attack on the subway is imminent ", then $P(h|w)$ stands for an individuals' subjective belief in *h* given a body of knowledge *w,* which might include that in the individuals assumptions about security in the city, specific threats were made by terror groups along with an assessment of the threat level.

In defining belief expressions, it is common to denote $P(h)$ or $P(\neg h)$, leaving out the constant *w*. This abbreviation is justified when *w* remains constant, since the main purpose of the quantifier *P* is to summarize *w* without explicating it. In situations where background information undergoes changes, there is a need to specifically identify the assumptions that account for our beliefs and articulate explicitly *w* or some of its elements. In Bayesian Formalism, belief measures obey the three basic axioms of Probability Theory:

- $0 \leq P(A) \leq 1$
- *P(Certain proposition) = 1*
- *P(A or B) = P(A) +P(B) if A and B are mutually exclusive*.

The third axiom states that the belief assigned to any set of events is the sum of the beliefs assigned to its nonintersecting components.

The basic expressions in the Bayesian formalism are statements about conditional probabilities, for example, $P(A|B)$ - which specify the belief in *A* under the assumption that *B* is known with absolute certainty. *A* and *B* are independent if $P(A|B) = P(A)$. If $P(A|B,C) = P(A|C)$ then *A* and *B* are conditionally independent given *C*. Bayesian philosophers see the conditional relationship as more compatible with the organization of human knowledge. In this view, *B* serves as a pointer to a context of the frame of knowledge, and $A|B$ stands for an event *A* in the context specified by *B*. Thus factual knowledge invariably is encoded in conditional probability

statements, while belief in joint events, if it is ever needed is computed from those statements via the product rule:

$$P(A,B)=P(A|B)P(B) \qquad (2)$$

The probability of any event *A* can be computed by conditioning it on any set of exhaustive and mutually exclusive events B_i, $i=1,2\ldots,n$:

$$P(A) = \sum_i P(A \mid B_i)P(B_i) \qquad (3)$$

This decomposition provides the basis for hypothetical or assumption-based reasoning in the Bayesian Formalism. It states that the belief in any event *A* is a weighted sum over the beliefs in all the distinct ways that *A* might be realized.

3.2 Related Sample Applications of Bayesian Networks in the Military Domains

Dynamic Bayesian Networks (Pearl, 1988; Pfeffer, 2000) have been used for military plan recognition. The translation of context independent (sensor) data to context dependent data (information) with respect to knowledge incompleteness has been successfully implemented with context-based navigation of troops (Su, Bai, Du, & Feng, 2011). The task of tactical engagement of entity agents is described by means of a *Behavior Definition Frame* and task allocation entails using a Task Allocation Processing Bayesian Network Module (Li et al., 2010)

Johansson and Falkman (2008) have used Bayesian Networks (BNs) and a ground target simulator to predict enemy intent for battle command. Expert elicitation was used to identify general parameters to predict the enemy's tactical intention in different ground combat scenarios. Such parameters include enemy intention, distance between the enemy and different targets, enemy type and target type, direction, targets protection value, and attraction.

Suzic (2003) used dynamic belief networks as a method for representing knowledge about the enemy and performing inference based on sensor data. In this case, the BN was used to solve a dynamic, stochastic policy recognition problem with the task characterized a s "an on-line multi-agent stochastic policy recognition." It aimed at detecting the policies an agent or a group of agents would execute by observing their actions and using apriori knowledge about them in a noisy environment. Inferencing was undertaken to derive belief measures for the enemy plans.

The BN is presented as a hierarchical model of a hostile tank company consisting of three tank platoons with each platoon containing three tanks as shown in Figure 4. For each level there is a certain set of policies invoked by the higher level. The simplest policies, their atoms, consist only of a set of actions.

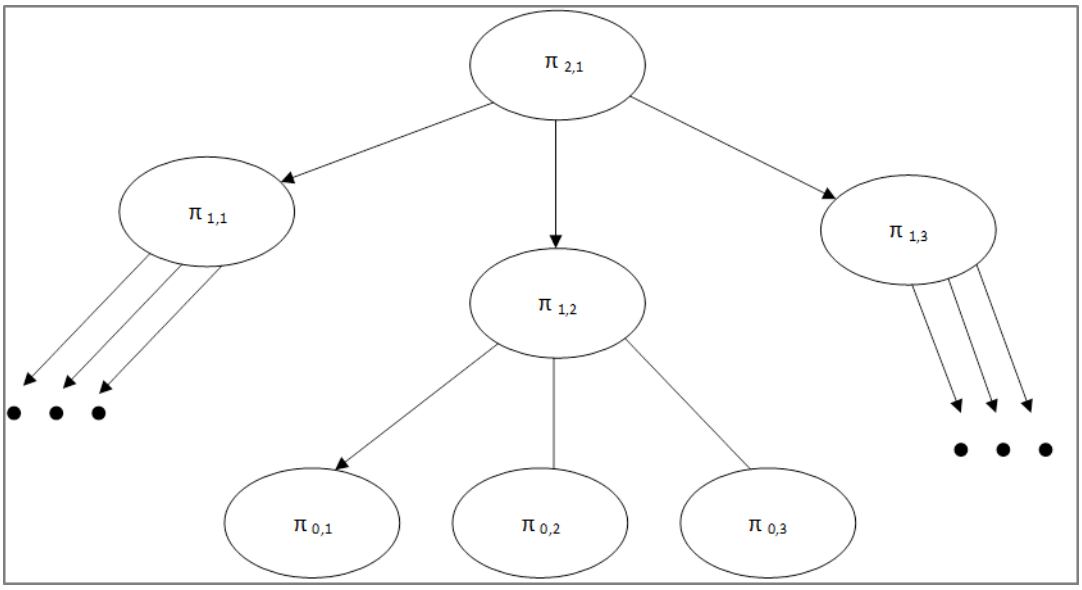

Figure 4. A BN representing the policy hierarchy model of a hostile company (Suzic, 2003), redrawn.

In this instance, the policy for each agent (hostile unit) is represented as a BN node with the simplest policy being on the tank (group) level, *k=0*. The variable $\pi_{0,i}$ represents Tank *i*'s policy

variable with various discrete states that define directional movement ($\pi_{0,i,}$), policy of the tank platoon; ($\pi_{1,i}$) and policy of the tank company ($\pi_{2,i}$). The network is then used to predict opponents behaviors based on observations, knowledge about the opponents' doctrines and terrain data.

Das (1999) describes the use of BNs to represent and update uncertainties encountered in the process of situation assessment using scenarios in naval anti-surface warfare. A set of hypotheses that adequately represent possible *enemy intentions* is generated with clarifying states - *Passive*, *Defensive*, *Offensive* and *Not Modelled*. *Enemy intention* directly influences *enemy activity* which may be *Logistics, Reconnaissance of a restricted zone, Mounting naval attack, Enemy vessel type, Position of the enemy unit, Mobility of the enemy unit* or *Communication activities of the enemy unit.*

Figure 5 shows the BN developed for situation assessment in a naval anti-surface warfare. Evidence to the network is supplied through the sensor and reconnaissance nodes. The network uses the evidence to update the probability distribution over the states of the *position* node. The parameters: *vessel type, position* and *mobility* are also detected through sensors and reconnaissance.

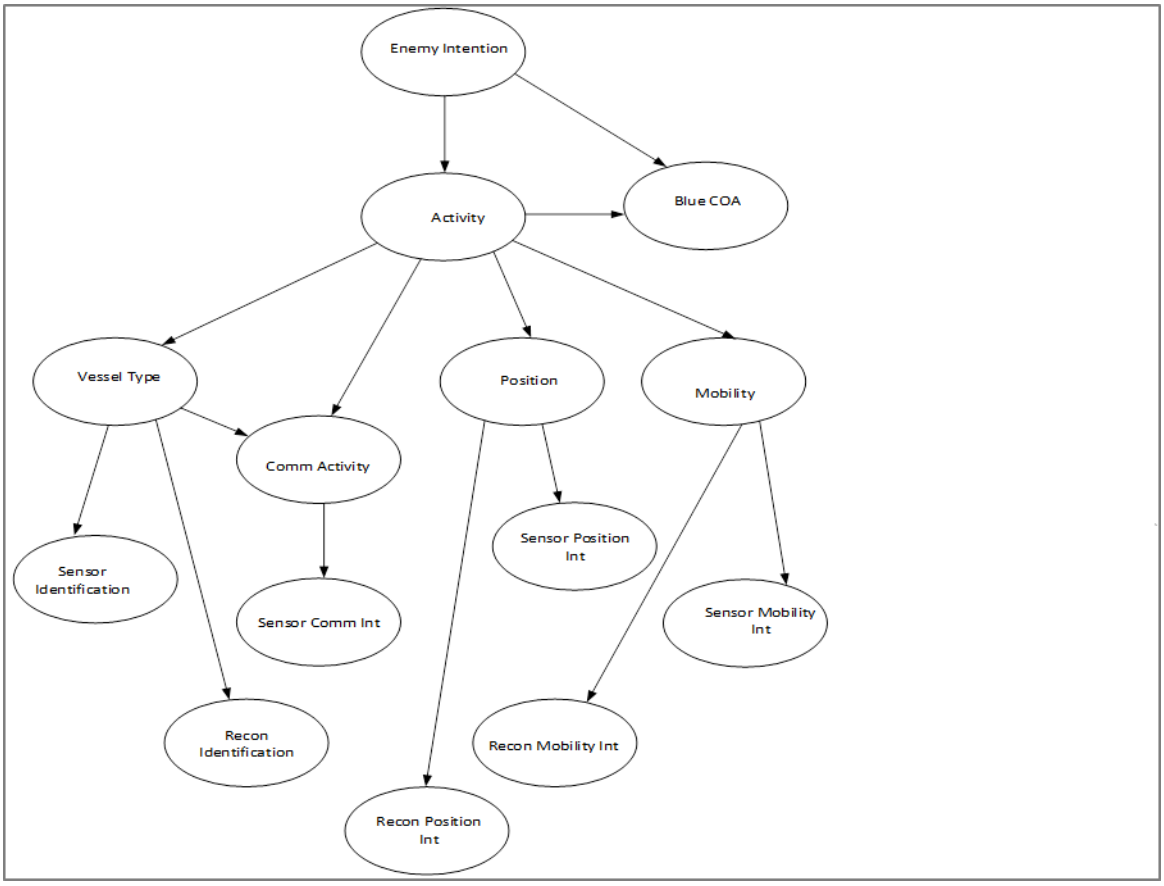

Figure 5. A BN for situational assessment in naval-anti-surface warfare (Das, 1999).

Santos (2003) used BNs to develop an adversary model that could capture goals, intentions, biases, beliefs and perceptions based on a dynamic cognitive architecture that evolved over time. The basic adversary intent architecture comprised three core components: *Goals/Foci*, *Rationale* and *Action*. The *Goal* component was a probabilistically prioritized short- and long-term goal list representing adversary intents, objectives or foci. The *Rationale* component was a probabilistic network representing what influences the adversary's beliefs, about himself, the Blue Forces, their goals, and certain high level actions associated with these goals. The *Actions* component was a probabilistic network, representing the detailed relationships between adversary goals and the actions they were likely to perform to realize them.

Bayesian Networks were developed for the *Rationale* and *Action* networks. Each random variable in the network was classified into one of four classes: *axioms, beliefs, goals* and *actions*. *Adversary axioms* represented the underlying beliefs of the adversary about himself and served as inputs or explanations to the other random variables. *Adversary beliefs* represented the adversary's beliefs regarding the Blue Forces. *Adversary goals* represented the goals or desired end-states of the adversary. *Adversary actions* represented the actions of the adversary that could typically be observed by friendly forces.

A computational framework for adversarial modeling and inferencing of adversary intent was developed as part of the Air Force Research Laboratory's Intelligence Preparation of the Battlespace (Bell, Santos, & Brown, 2002). Bayesian Networks and Bayesian Knowledge Bases were implemented in an adversary *Intent Inferencing Module* for COA prediction, explanation and inference of adversary intent. Simulation and proof-of-concept used scenarios from the battle of al Khafji - during the *Operation Desert Storm*. This simulation included a stream of direct enemy observables as they unfolded in the battlefield. The initial intent of the adversary (not to attack across the Saudi border into al Khafji) was known apriori. As the situation unfolded in the simulation, the adversary model evolved the underlying intent dynamically based on the observables and predicted enemy actions in accordance with the actions taken during the battle. With this simulation, the authors were able to demonstrate the viability of probabilistic network modeling approach to capturing such scenarios.

Falzon and Priest (2004) used Bayesian Networks in the development of the Center of Gravity (COG) Network Effects Tool (COGNET). COGNET provides a modeling framework and a generic database to aid knowledge reuse and knowledge transfer. The modeling framework is then used as a basis for the construction, population and analysis of Bayesian

Networks to support a rigorous and systematic approach to the COG analysis. The BN developed is a causal probabilistic network that represents the functional decomposition of the key concepts used by operational planners in COA development: end-state, center of gravity, critical vulnerabilities, decisive points and lines of operations.

Evans et al., (2003) used Dynamic Bayesian Nets to represent the causal relationship between lower-level friendly tasks and higher-level effects on adversary systems in order to guide plan generation and analyze the observed impact of planned military actions during plan execution. Pate-Cornell (2002) used a BN in intelligence analysis within tactical situations by developing a probabilistic method of assessing the intent and location of terrorists, their weapons and other enablers, as input to "local risk" analyses, in support of risk management decisions in the context of an unfolding crisis. McLaughlin and Pate-Cornell (2005) used Bayesian techniques to analytically illustrate Iraq's nuclear program intelligence.

3.3 Abduction in Bayesian Belief Networks

3.3.1 Abduction as the Most Probable Explanation (MPE) of Events

Gelsema (1995) notes that "a special class of problems in Bayesian belief networks is abductive reasoning, inference from effects to the best explanations of the effects." Similarly, Lacave and Diez (2002) note that explanations of evidence consist of determining which values of the unobserved variables justify the available evidence. This process is usually called abduction, and is based on the (usually implicit) assumption that there is a causal model. In this context, an explanation is a configuration of the unobserved variables, and the goal of the inference process is to obtain the Most Probable Explanation (MPE) or the k Most Probable Explanations (kMPEs). In general, the variables that take the value "present" or "positive" in the MPE are considered the causes that explain the evidence. This kind of explanation is basically to

offer a diagnosis for a set of observed anomalies. For instance, in medical expert systems, an explanation determines the disease or diseases that explain the evidence: symptoms, signs, test results, etc.

Lacave and Diez (2002), consider an explanation ***w*** which is an assignment of values to all the variables in a certain subset ***W*** of the variables of the network. Since the values of observed variables are known with certainty, only unobserved variables are the object of scrutiny in abductive methods. Abduction intends to find the MPE with the configuration ***w*** with the maximum a-posteriori probability $P(\boldsymbol{w}|\boldsymbol{e})$, where ***e*** is the available evidence. When ***W*** includes all the unobserved variables, the process is known as total abduction; else, it is partial abduction. In general, given an observation ***o,*** a hypothesis ***h*** and the knowledge that ***h*** causes ***o***, it is an abduction to hypothesize that ***h*** occurred. Abduction tries to synthesize a composite hypothesis explaining the entire observation from elementary hypotheses.

Pierce (1877) first described abductive inference by providing two intuitive characterizations: given an observation *d* and the knowledge that *h* causes *d, it* is an abduction to hypothesize that *h* occurred; and given a proposition *q* and the knowledge that $p \rightarrow q$, it is an abduction to conclude *p*. In either case, abduction is uncertain because something else might be the actual cause of *d, or* because the reasoning pattern is the classical fallacy of "affirming the consequent" and therefore, formally invalid. Additional difficulties can exist because *h* might not always cause *d,* or because *p* might imply *q* only by default. Generally, we can say that *h explains d* and *p explains q* and we shall refer to *h* and *p* as *hypotheses* and *d* and *q* as data. Peirce (1877) further defines the process of inquiry or discovery as including three fundamental inference processes:

1) Abduction generates hypotheses to explain new anomalous data.

2) Deduction performs the function of making a prediction as to what would occur if the hypotheses were to turn out to be the case.

3) Induction finds the ratio of the frequency by which the necessary results of deduction do in fact occur.

Abduction is then, a reasoning process that forms plausible explanations for abnormal observations. It is distinct from deduction and induction in that it is inherently uncertain since information or data supporting the abduction process is dynamic, leading to human construction of multiple and often competing hypotheses. It takes as input a set of data and yields as output a hypothesis that can best explain the input data. Consider the example from Bhatnagar and Kanal (1993);

"The surprising fact **C** is observed. However, if **A** were true, C would be a matter of course. Hence, there is reason to suspect that **A** is true. Here, **C** is an observed fact. The second sentence states the relationship, which is available from the domain knowledge, that the presence of **A** explains the presence of **C**. In the third statement, **A** is an abductively inferred hypothesis. The content of the inference is the premise "If **A** were true, **C** would be a matter of course" (pp.233)

The existing models of abduction are purely from the logical approach (Konolige, 1992). In the context of logic-based abduction, Eiter and Gottlob (1995) note that the main decision problems are:

(i) To determine whether an explanation for the given manifestations exists at all;

(ii) To determine whether an individual hypothesis $h \in H$ is relevant, that is, whether it is part of at least one acceptable explanation; and

(iii) To determine whether an individual hypothesis is necessary, that is, whether it occurs in all acceptable explanations.

3.3.2 Abduction Reasoning from Bayesian Belief Networks

The relationship between Bayesian reasoning and abduction is governed by the assertion that issues affecting reasoning for example semantics are abductive in nature. Our interest is in the probabilistic models of uncertainties that enable some explanation to occur in a sensemaking information network. A set of plausible explanations of a proposition characterizing the context of interest (Prakken, 2004) can be derived as follows:

$$\text{Let } P(w) = \sum P(E) \tag{4}$$

Where E is an explanation of world w

$$P(E) = \prod_{h \in E} P(h) \text{ (Assuming independent events E)} \tag{5}$$

$$P(w \mid E) = \frac{P(w \,\&\, E)}{P(E)} \tag{6}$$

The numerator term $P(w\&E)$ explains the conjunction of w and E while the denominator explains E. $P(w|E)$ may represent, say, a mass demonstration by Iraqi citizens because of a mosque being bombed by the coalition force. The abduction problem in sensemaking is: given $P(E)$, explain E, then try to explain w from these explanations. The difference between deduction and abduction is illustrated in Figures 6 a and b below. Abduction has been the principal model-based technique for diagnostic problem solving using models of abnormal behavior in terms of cause-effect relationships (Peng & Reggia, 1990).

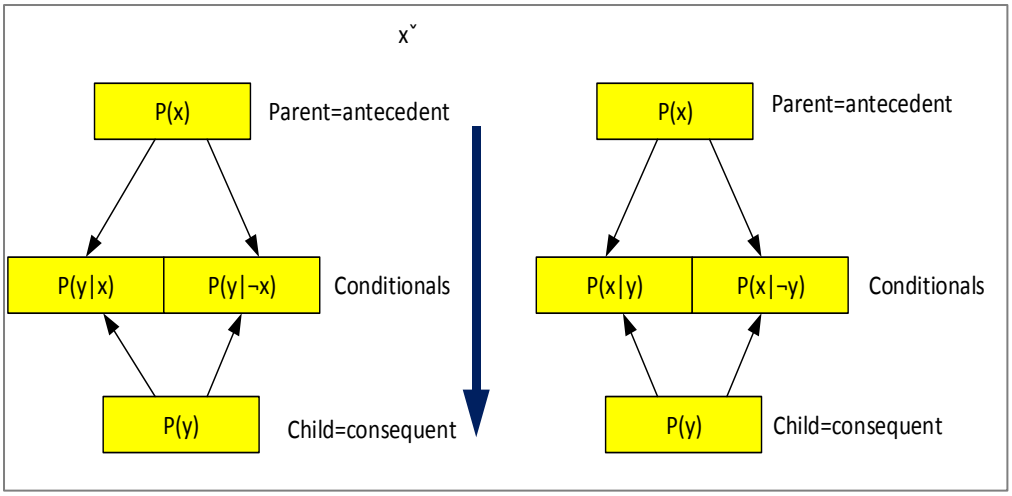

Figure 6. a) Deduction and b) Abduction (adopted from Josang, 2008).

In abductive reasoning, diagnostic problem solving consists of establishing a diagnosis using cause-effect relationships with a set of observed findings (effects) as the starting point. This is illustrated by three instances below:

1. Abduction inference makes "backward" inferences based on known causal relations, to explain or justify a conclusion. Here, the system reasons from effects to causes, instead of causes to effects. It is a reasoning process that is a reverse of deduction as shown in definition A1.

A1. Given: the truth of proposition Q

Given: P→ Q

Infer: P explains Q

Note that in definition A1, *P* can be background knowledge (also a theory) that describes a problem domain; *Q* represents an observation (or a set of observations). We want a hypothesis *H* that assumes that *P* is an abductive explanation for *Q*.

2. The main issue of abduction is to synthesize a composite hypothesis explaining the entire observation from elementary hypotheses. Abduction also supposes implicitly that a relationship is available between hypothesis and observations in the form of rule A2.

A2. Given: P→ Q

Given :Observation Q

Explain hypothesis H

Here, *Q* may be a fuzzy characterization of the situation.

3. Abduction is a type of reasoning that derives a set of hypotheses (causes) which explain a given set of events (symptoms) using causal knowledge (relational maps) of the system functionality. This can be represented in rule A3.

A3. Given: Observation, Q

Given: Hypothesis (H) of disorders

Infer: the knowledge of H causes or explains Q

As shown in rules A1-A3 above, the main issue of abduction is to synthesize a composite hypothesis explaining the entire observation from elementary hypotheses. In the sensemaking process, we tend to seek explanations to unexpected situations. Broadly speaking, abduction aims at finding explanations for, or causes of, observed phenomena or facts; it is an inference to the best explanation, a pattern of reasoning that occurs in such diverse places as medical diagnosis, scientific theory formation, accident investigation, language understanding, and jury deliberation.

Figure 7 (with only analysis of the left-hand side) illustrates a simple MPE. We define an end state of the network as a composite hypothesis H_0 and to this we assign a prior probability. The prior probability can be assumed based on the level of past information possessed about a particular situation that is of interest. For example, H_0 could be disrupting stability and support operations in an urban center. The estimated probability could be from the news media, intelligence briefings, or simply the commander's estimate.

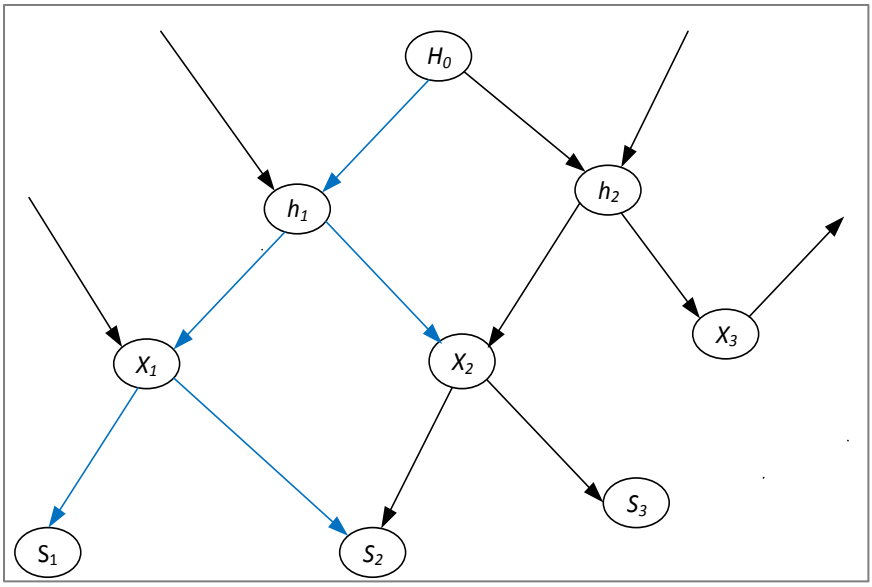

Figure 7. A Sample hierarchical network with different levels of evidence nodes for hierarchical Bayesian inference.

We can write, $P(H_o) = 0.4$. This means that we are only 40% confident of the plausibility of our chosen hypothesis. By the axioms of probability, the probability of an alternative hypothesis $P(\neg H_0)$ representing any other end state is therefore, $P(\neg H_0) = 0.6$ and this need not be explicitly stated. Similarly we can assign apriori probabilities for the conditional probabilities of interest representing the probabilities of the children events X_i and S_i given the parents, h_i and X_i respectively.

Assume for illustration, the following database is available:

$P(h_1|H_0) = 0.9;\ P(h_1|\neg H_0) = 0.8;\ P(x_1|h_1) = 0.7;\ P(x_1|h_2) = 0.4;\ P(S_1|x_1) = 0.5;\ P(S_1|x_2) = 0.6$

Next, we compute the prior probabilities of all the instantiated variables as follows:

$P(h_1) = P(h_1|H_0)P(H_0) + P(h_1|\neg H_0)P(\neg H_0) = (0.9)(0.4)+(0.8)(0.6) = 0.84\ ;P(h_2) = 0.16$

$P(x_1) = P(x_1|h_1)P(h_1) + P(x_1|h_2)P(h_2) = (0.7)(0.84)+(0.4)(0.16) = 0.652\ ;P(x_2) = 0.348$

$P(S_1) = P(S_1|x_1)P(x_1) + P(S_1|x_2)P(x_2) = (0.5)(0.652) + (0.6)(0.348) = 0.5348$

Considering the network shown in Figure 7,

$$P(S_1) = \sum_{S_1,..S_r} P(X_1 \mid S_1, S_2, S_3, ..S_r) \tag{7}$$

Because of the independence of $\{S_1, S_2, S_3...S_r\}$, we can write

$$P(S_1) = \sum_{S_1..S_r} P(X_1 \mid S_1..S_r) P(S_1) P(S_2) P(S_3) ... P(S_r) \tag{8}$$

$$P(S_1) = P(X_1 \mid S_1) P(S_1) + P(X_1 \mid S_2) P(S_2) + P(X_1 \mid S_3) P(S_3) ..... P(X_1 \mid S_r) P(S_r) \tag{9}$$

Clearly, there is a complexity arising from the computation, even for a relatively simple network. When new evidence is introduced, the analyst is interested in determining the possible effects on his most probable hypothesis, H_0. Suppose the new evidence points to a new target to be exploited by the insurgents, the new target may be a coalition Command and Control (C2) post in a previously secured part of the country. This would definitely require a level of sophistication, challenging the analyst's previous hypothesis about the end state of the insurgency.

Using Bayesian Abduction Inference, we can compute the state of the network with variable X_i instantiated as follows:

$$P(H_o \mid X_i) = \frac{P(X_i \mid H_o) P(H_o)}{P(X_i)}$$

$$P(X_i \mid H_o) = \sum_{h_1..h_n} (X_i \mid h_n, H_o) P(h_n \mid H_o)$$

$$P(X_i \mid H_o) = P(X_1 \mid h_1, H_o) P(h_1 \mid H_o) + P(X_1 \mid h_2, H_o) P(h_2 \mid H_o) ..... P(X_1 \mid h_n, H_o) P(h_n \mid H_o)$$

$$P(X_i \mid H_o) = P(X_1 \mid h_1) P(h_1 \mid H_o) + P(X_1 \mid h_2) P(h_2 \mid H_o) ..... P(X_1 \mid h_n) P(h_n \mid H_o) \tag{10}$$

3.3.3 An Application to Sensemaking Analytics

Case 1: Prospective (or Predictive) Sensemaking Analyses:

Based on Pearl (1988) we define a model of recursive Bayesian learning with data updates as follows: Let *H* denote a hypothesis, $d_n = d_1, d2,..d_n$ denote a sequence of data observed in the past ,and *d* denote a new fact. A brute force way to calculate the belief in *H*,$P(H|d_n, d)$ would be to append the new datum *d* to the past data d_n and perform a global computation of the impact on *H* of the entire data set $d_n+1=\{d_n,d\}$. Under certain conditions, this computation can be significantly curtailed by incremental updating; once we have computed $P(H|d_n)$,we can discard the past data and compute the impact of the new datum by the formula

$$P(H \mid d_n, d) = P(H \mid d_n)\frac{P(d \mid d_n, H)}{P(d \mid d_n)} \qquad (11)$$

Comparing equation (10) and (11), it is easy to see that the old belief $P(H|d_n)$ assumes the role of the prior probability in the computation of new impact; it completely summarizes the past experience and for updating need only be multiplied by the likelihood function $P(d|d_n, H)$,which measures the probability of the new datum *d*, given the hypothesis and past observations.

The likelihood function is independent on the past data and involves only *d* and *H*. For example, the likelihood that a patient will develop a certain symptom, given that he definitely suffers from a disease *H*, is normally independent of what symptoms the patient had in the past. This conditional independence assumption allows us to write $P(d|d_n, H) = P(d|H)$ and $P(d|d_n, \neg H) = P(d|\neg H)$. After dividing equation (11) by the complementary equation for $\neg H$, we obtain:

$$O(H \mid d_{n+1}) = O(H \mid d_n)L(d \mid H). \qquad (12)$$

Equation (12) describes a simple recursive procedure for updating the posterior odds. Upon the arrival of each new datum *d*, we multiply the current posterior odds $O(H|d_n)$ by the likelihood ratio of *d*. This is a prediction model which replicates the behavior of a prospective sensemaking on datum d_{n+1}.

Case 2: Retrospective Sensemaking Analysis:

Let *H* represent a set of hypotheses, H_i each of which is equally likely. We can modify Pearl's (1988) model to capture retrospective sensemaking as follows: Define an *m* x *n* matrix M_k, where *m* and *n* are the number of values that *H* and D_k might take, respectively; and the *(i,j)*-th entry of M_k stands for $M_{k_{ij}} = P(d_{k_j}|H_i)$. Then,

$$P(H_i \mid d_1,...,d_N) = \alpha P(H_i)[\prod_{k=1}^{N} P(d_k \mid H_i)] \quad (13)$$

Equation (13) can be rewritten as:

$$O(d_n \mid H_{i+1}) = O(dn \mid H_i)L(H \mid d_n). \quad (14)$$

3.4 Bayesian Belief Networks

A sensemaking problem often requires an eliciting of beliefs from experts. These beliefs can be framed as a set of hypotheses. For example, assume there is a bomb attack on a football stadium in a major university campus. A group of intelligence analysts is asked to build a sensemaking process model of the bomb attack. Assume also that the analysts start by suggesting three likely suspicious entities for the bomb attack. Let this be H = $\{h_1, h_2, h_3\}$. The analysts will take on each assumption h_i and identify major issues, suspected causes, and the likely effects. For the present discussion, ignore the effect and concentrate on the issues (I) and causes (C). Figure 8 is used to illustrate the analyst's belief tree about the problem with their associated belief values estimated to be a number between 0 and 1.

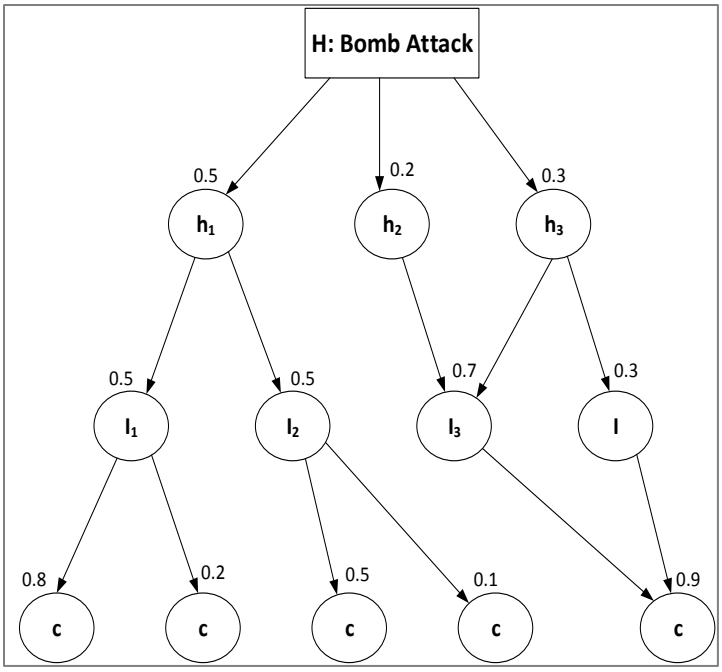

Figure 8. Belief tree representing a set of hypotheses about a bomb attack.

In Figure 8, the nodes H, I, and C represent a single analyst assessment of the situation by speculating on a set of hypotheses (H), the issues related to each hypothesis (I), and the possible causations (C).If beliefs are converted to probability values in the belief network, then a probability space can be modeled as a Bayesian Belief Network of propositional variables (nodes) which may be connected by directed arcs, pairwise. For example, if an arc exists from node I_1 to node C_1, the probability of node C_1 assuming a given state c_i depends on the actual state of node I_1 (I_1 is a direct cause of C_1). The absence of an arc between two nodes implies that there is no such direct dependence. If in a Bayesian Belief Network, for all states of the root nodes the prior probabilities are known, and in addition, for all non-root nodes the conditional probabilities given the parent states are known, the joint probability distribution is completely known. This is not the case with the belief network in which only event or causal nodes are estimated by experts.

As postulated by Pearl (1988) a belief network also referred to as Bayesian Belief network (BBN), probabilistic network, or causal network is a directed acyclic graph in which each node represents a random variable or uncertain quantity which can take two or more possible values. Arcs signify the existence of direct causal influences between the linked variables and the strengths of these influences are quantified by conditional probabilities. A BBN is an augmented directed acyclic graph, represented by a pair (V, E), where, V is a set of vertices; E is a set of directed edges joining the vertices; and no loops are allowed. Formally, the structure of the BN is a representation of the factorization of the joint probability distribution over all the states of the random variable (Heckerman, 1997).

For a BN consisting of *n* variables $X_1, X_2,..X_n,$ the overall joint distribution over the variables *is* given by the product

$$P(X_1, X_2,..., X_n) = \prod_{i=1}^{n} P(x_i \mid \prod_{X_i}) \qquad (15)$$

where ΠX_i represents parent variables of X_i. An advantage of network representation is that it allows people to express directly the fundamental qualitative relationship of direct dependency. The network then displays a consistent set of additional direct and indirect dependencies and preserves it as a stable part of the model, independent of the numerical estimates. The directionality of the arrows is essential for displaying non transitive dependencies. It is this computational role of identifying what information is relevant or not in any given situation that is attributed to the mental construct of causation (Zhaoyu &D'ambrosio, 1993).

In general, a BN consists of the following (Russell &Norvig, 2003):

a) A set of random variables (either discrete or continuous) that constitutes the nodes of the directed graph.

b) A set of directed edges (arrows) that connects pairs of nodes. If there is an edge from node *Y* to node *X*, *Y* is called the parent to *X* and *X* is referred to as the child to *Y*.

For every node X_i, there is a conditional probability distribution that quantifies the effect that any parent nodes have on the node in question. The graph is not allowed to have any directed cycles and from this, it follows that it is a directed acyclic graph.

According to Onisko (2002), a BN consists of a qualitative part, encoding the existence of probabilistic influences among a domain's variables in a directed graph, and a quantitative part, encoding the joint probability distribution over these variables. The quantification of a Bayesian Network consists of prior probability distributions over those variables that have no predecessors in the network and conditional probability distributions over those variables that have predecessors. These probabilities can easily incorporate available statistics and, where no data are available, expert judgment.

The most important type of reasoning in Bayesian Networks is belief updating, which amounts to computing the probability distribution over variables of interest conditional on other observed variables. For example, in a battle command situation, the commander might receive intelligence reports about rioting by the population in a contested area. He would be fairly certain of it being a civil unrest and so refrain from sending in a suppressive force. If in the next instance however, a routine patrol in the area of unrest did come under sustained fire, then, the probability of civil unrest would be lowered and his belief would be updated. The hypothesis "insurgent attack" gets more support and the probability density function over the hypothesis space changes. In the network situation of Figure 8, drawing such a conclusion is referred to as evidence propagation. The essence of the Bayesian approach is therefore to provide a formalism explaining how a person's existing beliefs can change in the light of new evidence. Depending

on the complexity of the network, belief updating in Bayesian Networks is considered NP-hard (Heckerman, 1997), meaning its solution (if it exists) cannot be verified in the polynomial space.

Using the example in Figure 9, we can show some derivations and representations of conditional probabilities. Consider a simple case of the example network where the variables have only binary true or false states. For forward inference, consider that the variables S_1 and S_2 are the variables of interest.

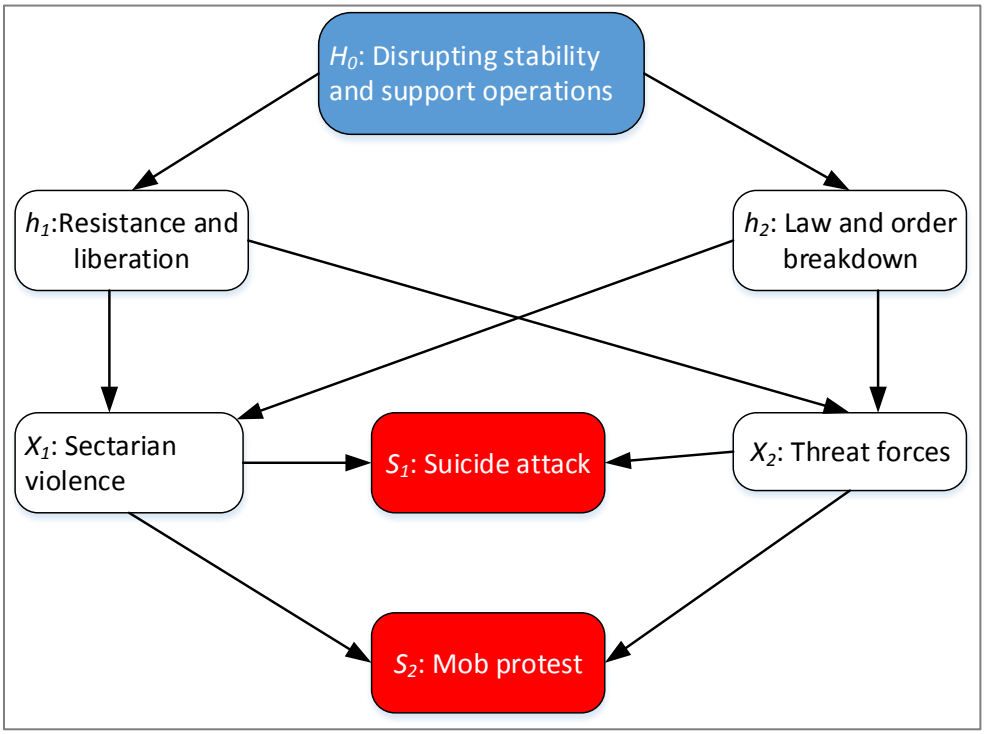

Figure 9. Example BN of a battle command situation.

S_1 is High Level Attrition Attack such as a *Suicide Bombing* while S_2 is a variable representing a *Mob Protest*. Variable X_1 represents *Sectarian Violence* while X_2 represents *Threat Forces*. The composite hypothesis H_0 (Disrupting Stability and Support Operations) is informed by a set of hypotheses h_1 (Resistance and Liberation) and h_2 (Law and Order Breakdown).

By abductive inference:

$$P(S_1, S_2)$$

$$= \sum_{H_0}\sum_{h_1}\sum_{h_2}\sum_{X_1}\sum_{X_2} P(H_0)P(h_1|H_0)P(h_2|H_0)P(X_1|h_1,h_2)P(X_2|h_1,h_2)P(S_1|X_1,X_2)P(S_2|X_1,X_2)$$

It is not reasonable to estimate $P(S_1,S2|H_0)$. That is, we cannot reasonably compute the probability of *Suicide Bombing* or *Mob Protest* even if we are certain both events are linked to an attempt to disrupt stability and support operations in the area of interest. In order to infer correctly and with a reasonable degree of confidence, we would like to assess more evidence such as whether the observed actions are a part of wider resistance and liberation movement or simply a result of a breakdown in law and order. If the evidence points to a wider resistance, then, we would be interested in knowing whether it is being perpetuated by sectarian militias or not.

If however, more evidence supports the hypothesis that it's a law and order breakdown, then, we would like to know, with a degree of confidence, whether the breakdown is being caused by threat forces and criminal elements or by organized sectarian militias. To assess this, we first have to assume some probability distributions for all the parent nodes and the prior conditionals for all the variables. Consider the data below as an example:

For node H_0

$P(H_0$=T)	$P(H_0$=F)
0.4	0.6

For nodes h_1, h_2

h_1	H_0=T	H_0=F
T	0.7	0.3
F	0.2	0.8

h_2	H_0=T	H_0=F
T	0.5	0.5
F	0.7	0.3

For nodes X_1, X_2

h_1	h_2	$P(X_1=\mathrm{T}\|h_1,h_2)$	$P(X_1=\mathrm{F}\|h_1,h_2)$
T	T	0.2	0.8
T	F	0.8	0.2
F	T	0.3	0.7
F	F	0.6	0.4

h_1	h_2	$P(X_2=\mathrm{T}\|h_1,h_2)$	$P(X_2=\mathrm{F}\|h_1,h_2)$
T	T	0.6	0.4
T	F	0.1	0.9
F	T	0.8	0.2
F	F	0.3	0.7

For nodes S_1, S_2

X_1	X_2	$P(S_1=T\|X_1,X_2)$	$P(S_1=F\|X_1,X_2)$
T	T	0.6	0.4
T	F	0.2	0.8
F	T	0.7	0.3
F	F	0.4	0.6

X_1	X_2	$P(S_2=\mathrm{T}\|X_1,X_2)$	$P(S_2=\mathrm{F}\|X_1,X_2)$
T	T	0.5	0.5
T	F	0.9	0.1
F	T	0.4	0.6
F	F	0.2	0.8

We can generalize the following from the examples above: The child node X_1 having states $\{ x_{i,1}, x_{i,2} \ldots x_{i,j}\}$, $j \geq 1$ is influenced by n parent nodes $, Y_2 \ldots Y_n$ (Das,2006). Any parent node Y_i has states $\{y_{i,1} y_{1,2} \ldots y_{i,k}\}$, $k \geq 2$. The parent nodes represent n random variables $Y_1 .. Y_n$ while the child node represents a random variable X .The network will consist of $k_1 \mathrm{x} \ldots . \mathrm{x}\, k_n$ such parental configurations requiring a Conditional Probability Table (CPT) with as many probability distributions over the child node X. Such a parental configuration will have a distribution of the form

$$\{P(x_{i,1}|y_{i1,} \ldots . , y_{ik}), P(x_{i,2}|y_{i1,} \ldots . , y_{ik}), \ldots P(x_{i,j}|y_{i1,} \ldots . , y_{ik})\}$$

Where $P(x_{i,1}|y_{i1,} \ldots . , y_{ik})$ is the conditional probability $P(X_1 = x_{i,j}|Y_1 = y_{i1,} \ldots , Y_n = y_{ik})$. Let π denote the parental configuration, then, the conditional probability may be written as $P(x_{i,j}|\pi)$.

We extend the simple network of Figure 9 into a multi-variable multi-attribute hierarchical network of Figure 10. Representative of a real world situation, the network will have many levels to account for the different types of observable evidence in the problem space. Each

level in the hierarchy will have a large but finite number of variables, each of which may have more than one state.

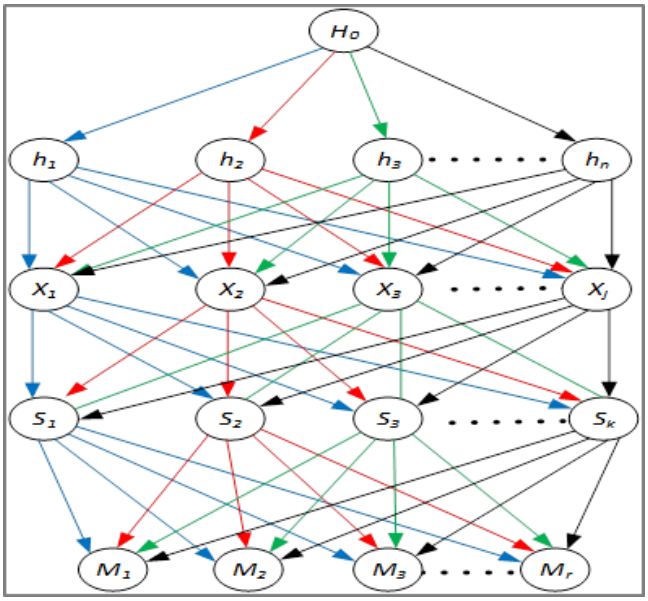

Figure 10. Hierarchical BN illustrating the research problem.

The following definitions are provided for the variables in the network displayed in Figure 10: H_0 is a composite hypothesis representing an analyst's apriori belief about a situation before new evidence arrives. It is the end state for which the analyst would like to make an inference. To account for multiple types of uncertainty in the problem domain, H_0 is an aggregation of sub-hypotheses h_1, h_2, h_3...h_n each of which has a defined apriori belief. The variables X_1, X_2, X_3...X_j define the first level of evidence variables. Variables S_1, S_2, S_3…S_k represent the second level of evidence variables directly influenced by the level one variables.

Depending on the complexity of the problem, the network could have more levels of evidence or informational variables, sometimes referred to as intermediate or step variables, to support the correct inference. Variables M_1, M_2, M_3…M_r represent the target variables which are typically directly observable evidence variables or variables of some specific significance to the analyst. Causal representation and the assumption of conditional independence make the

computation of the conditional probabilities of the evidence variables relatively straightforward. Table 1 shows the conditional probability values for the network of Figure 10 where each random variable has several states as shown below. The variable h_1 has states $h_{11}, h_{12}\ldots h_{1n}$.

Table 1

Conditional Probability Tables for the Network of Figure 10

h_1	h_{11}																	
h_2	h_{21}									h_{22}								
h_3	h_{31}			h_{32}			h_{33}			h_{31}			h_{32}			h_{33}		
h_n	h_{n1}	h_{n2}	h_{n3}	h_{n1}	h_{n2}	h_{n3}	h_{n1}	h_{n2}	h_{n3}	h_{n1}	h_{n2}	h_{n3}	h_{n1}	h_{n2}	h_{n3}	h_{n1}	h_{n2}	h_{n3}
X_1	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_{17}	a_{18}
X_2	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}	b_{11}	b_{12}	b_{13}	b_{14}	b_{15}	b_{16}	b_{17}	b_{18}
X_3	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}	c_{11}	c_{12}	c_{13}	c_{14}	c_{15}	c_{16}	c_{17}	c_{18}
X_j	d_1	d_2	d_3	d_4	d_5	d_6	d_7	d_8	d_9	d_{10}	d_{11}	d_{12}	d_{13}	d_{14}	d_{15}	d_{16}	d_{17}	d_{18}

Let the conditional probabilities of variable X_i for each state of h_i be denoted by $\{a_i.,b_i,..d_i$ }.Then, we can write

$a_i =$

$P(X_1|h_{11},h_{21},h_{31},h_{n1}), P(X_1|h_{11},h_{21},h_{31,}h_{n2}), P(X_1|h_{11},h_{21},h_{31,}h_{n3}),$

$P(X_1|h_{11},h_{21},h_{32},h_{n1}), P(X_1|h_{11},h_{21},h_{32,}h_{n2}), P(X_1|h_{11},h_{21},h_{32,}h_{n3}),$

$P(X_1|h_{11},h_{21},h_{33},h_{n1}), P(X_1|h_{11},h_{21},h_{33,}h_{n2}), P(X_1|h_{11},h_{21},h_{33,}h_{n3})$

$P(X_1|h_{11},h_{22},h_{31},h_{n1}), P(X_1|h_{11},h_{22},h_{31,}h_{n2}), P(X_1|h_{11},h_{22},h_{31,}h_{n3})$

$P(X_1|h_{11},h_{22},h_{32},h_{n1}), P(X_1|h_{11},h_{22},h_{32,}h_{n2}), P(X_1|h_{11},h_{22},h_{32,}h_{n3})$

$P(X_1|h_{11},h_{22},h_{33},h_{n1}), P(X_1|h_{11},h_{22},h_{33,}h_{n2}), P(X_1|h_{11},h_{22},h_{33,}h_{n3})$

Where $P(X_1|h_{11},h_{21},h_{31},h_{n1}) = P(h_{11}\&h_{21}\&h_{31}\&h_{n1}|X_1)P(X_1)/P(h_{11}\&h_{21}\&h_{31}\&h_{n1})$

$= P(h_{11}|X_1)P(h_{21}|X_1)P(h_{31}|X_1)P(h_{n1}|X_1)P(X_1)/\ P(h_{11}\&h_{21}\&h_{31}\&h_{n1})$

Similarly, we compute conditional probabilities b_i and c_i. In general, for the *jth* state of the random variable *X*, the conditional probability d_i is given by

$d_i =$

$P(X_j|h_{11}, h_{21}, h_{31}, h_{n1}), P(X_j|h_{11}, h_{21}, h_{31,}h_{n2}), P(X_j|h_{11}, h_{21}, h_{31,}h_{n3}),$

$P(X_j|h_{11}, h_{21}, h_{32}, h_{n1}), P(X_j|h_{11}, h_{21}, h_{32,}h_{n2}), P(X_j|h_{11}, h_{21}, h_{32,}h_{n3}),$

$P(X_j|h_{11}, h_{21}, h_{33}, h_{n1}), P(X_j|h_{11}, h_{21}, h_{33,}h_{n2}), P(X_j|h_{11}, h_{21}, h_{33,}h_{n3})$

$P(X_j|h_{11}, h_{22}, h_{31}, h_{n1}), P(X_j|h_{11}, h_{22}, h_{31,}h_{n2}), P(X_j|h_{11}, h_{22}, h_{31,}h_{n3})$

$P(X_j|h_{11}, h_{22}, h_{32}, h_{n1}), P(X_j|h_{11}, h_{22}, h_{32,}h_{n2}), P(X_j|h_{11}, h_{22}, h_{32,}h_{n3})$

$P(X_j|h_{11}, h_{22}, h_{33}, h_{n1}), P(X_j|h_{11}, h_{22}, h_{33,}h_{n2}), P(X_j|h_{11}, h_{22}, h_{33,}h_{n3})$

Variables with no predecessors are marginally independent while variables that have one or more common parents but no arc connecting them are conditionally independent of each other, given their common parents.

3.5 Chapter Summary

This chapter presented a Bayesian Formalism for representing sensemaking information. The belief network reflects a person's belief about the state of a variable in the real world through the use of joint probability distributions over the variables. Bayesian Networks are presented as normative cognitive models that support sensemaking under uncertainty. The networks are shown to support reasoning about evidence and actions not easily handled by other competing computational models. In Bayesian Belief Networks, the inference is done by abduction, meaning that we infer from effects to the best explanation of those effects. This reflects the behavior of a sensemaking problem. Forward (top-down) inference was shown to support information fusion in prospective sensemaking, while backward (bottom-up) inference implied support of information fusion in retrospective sensemaking.

CHAPTER 4

The BAMSS Model

4.1 BAMSS Description

The Bayesian Abduction Model for Sensemaking Support (BAMSS) is developed as an analytical model to support sensemaking information fusion. The model is validated with military COA that involves understanding adversary intent. BAMSS can be considered a knowledge management tool since it allows one to capture and represent knowledge about a sensemaking context as well as provide analytics for information fusion in the same context. BAMSS is developed with the Bayesian Network (knowledge construction) while abduction reasoning is used for inference via a belief network of expert information.

4.1.1. System Software Architecture Description

Figure 11 shows the system software architecture and components of BAMSS.

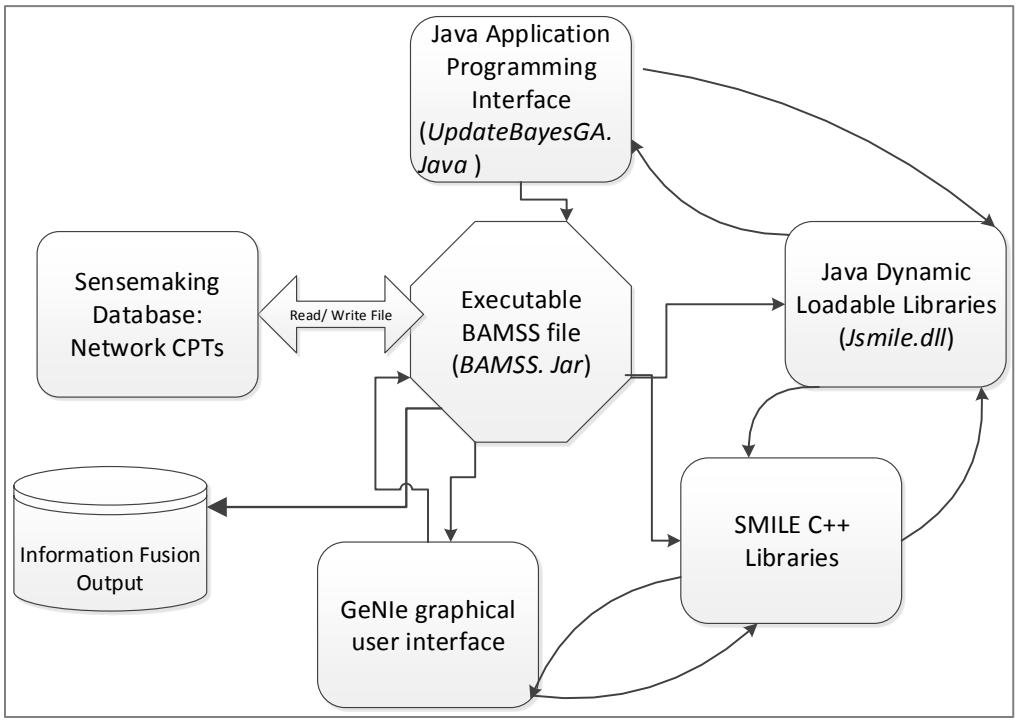

Figure 11. BAMSS software architecture and components.

The Structural Modeling, Inference and Learning Engine (SMILE) library of C++ classes provides the library of functions that are used to implement the Bayesian Network inference algorithm. SMILE is embedded in the BAMSS model through the use of an Application Programming Interface (API) that allows the C++ classes to be called within the model. The model creates a dynamically loadable library (.dll) file of the SMILE libraries called *Jsmile.dll* in the Java programming language. *Jsmile.dll* is configured to provide all the functionality necessary to implement the build and reasoning process of the Bayesian Network.

Using the *Jsmile.dll*, an executable file (*BAMSS.jar*) that stores the computational logic of the Bayesian inference algorithm is created within the NetBeans Integrated Development Environment (IDE). The executable *BAMSS.jar* is called by the user through a simple graphical user interface (GUI) command line. The *.dll* file interacts with the executable file in a read/write mode as shown in Figure 11. The network module is created through the GeNIe graphical user interface. GeNIe is accessed through a web browser on the client side of a client-server model and contains all the functionality necessary to create a network with nodes and arrows representing variables and causal linkages respectively. The networks developed in GeNIe are loaded into the model by a simple command on the BAMSS GUI.

BAMSS GUI facilitates user interaction with the main building blocks of the model in a read-only mode. The GUI is implemented in Java with the Java file *ProbabilityUI.java* and hosts command lines for all the model functionalities as well as the data input fields. The *BayesianNetworkFitness.java* is compiled to create the Java class that contains the subroutine for calculating the genetic algorithm fitness function. It interfaces with the SMILE library using the Java API for Genetic Algorithms (JAGA). JAGA API is an extensible API for implementing genetic algorithms in Java and contains a range of genetic algorithms, genotype representations

and genetic operators. *UpdateBayesGA.java* contains classes for the algorithmic implementation of the Bayesian Genetic Algorithm. *GAResults.java* is a Java bean class which contains the final results of the *Fitness* subroutine after evaluation.

The sensemaking database can be regarded as a repository of conditional probability tables that represent the knowledge base for the sensemaker. Initially, the database is loaded with apriori beliefs about the hypothesis variables and apriori conditionals for all the other evidence variables. The results of the *BAMSS.jar* executable file run are the posterior probabilities of a network loaded in the model and represent the updated beliefs of the sensemaker. These results are added into the database using a GUI command line and form the apriori beliefs for the next round of computation in read/write format. The results are saved and made available to the user for analyses.

Software development for the model was implemented in a dedicated Java IDE known as NetBeans. An IDE is a software application that provides a comprehensive build environment for software development. The NetBeans IDE consists of a source code editor, build automation tools and a code debugger. Currently, the network module is implemented and hosted in GeNIe; the graphical interface to SMILE. The web-based interface to the network module resides on the client-server model hosting the GeNIe software. The computational module and the GUI are standalone applications developed in the NetBeans IDE. Open Source code for the Bayesian Clustering Algorithm and the Genetic Algorithm was downloaded and configured in the IDE using a Java API. An API specifies how the software components should interact with each other to produce the desired functionality. The final result of the build process is an executable .jar file which contains the business logic of the computational module, a library of functionalities, the

GUI, and is operable on the Windows suite of Operating Systems (98/NT/2000/XP). BAMSS is supported by a suite of software and hardware systems as shown in Table 2.

Table 2

Supporting Hardware and Software Suite for BAMSS

Software	Description	As used in BAMSS	Advantage	Disadvantages	Manufacturer
Java	Java programming language	Graphical user interface and computational algorithm implementation	Class based, object-oriented and platform independent. Has few implementation dependencies, is dynamic and robust	Longer execution times as it runs first on JVM (Java Virtual Machine). Also requires larger memory allocation than other languages	Oracle Network Corporation
JRE	Java Runtime Environment	Development of the Java applications	Combines the Java virtual machine, platform core classes and supporting libraries	JRE requires a substantial memory allocation.	Oracle Corporation
Java API	Application Programming Interface	Facilitates interaction with the SMILE C++ libraries	Allows easy use of C++ libraries using inbuilt callable functions, portable and platform independent	Slower and takes more memory space	Oracle Corporation
NetBeans IDE	NetBeans Integrated Development Environment	Development environment for BAMSS algorithm source codes	Extensible and easy modular design .Also has a large library of most commonly used APIs		Oracle Corporation
Python 2.7	Interactive object-oriented programming language	Genetic algorithm implementation.	Platform independent, easy modular design, extensible in C++ and for applications that need API.	Slower computation time compared to C++ or Java, user has to maintain external library dependencies	Python Software Foundation
PySide 1.2.2	A Python Software for generating bindings to the cross platform GUI toolkit QT4	Implementing the graphical library of the genetic algorithm	Platform independent and simple to use when creating menus	Gets complicated to debug. Not too much documentation to support development	Qt Project
JAGA	Java API for Genetic Algorithms	Genetic algorithm implementation in Java	Free and open source, contains an extensive library of GAs, GA operators and genotype representations	None	University College London, available at www.jaga.org

Table 2

Cont.

GeNIe	Graphical Network Interface	Windows user interface to SMILE; network module development	Open source software, intuitive and easy to learn and use	Too much bugs; Exception handling is difficult	Decision Systems Laboratory University of Pittsburg
SMILE	Structural Modeling, Inference, and Learning Engine	C++ libraries of hierarchical Bayesian network inference algorithms	Open source, platform independent and can be implemented in Java and Python	The software is provided as is, lack of development documentation.	Decision Systems Laboratory, University of Pittsburg

Hardware	Laptop (PC)	
Bandwidth	Operates on 2.4 GHz and 5.0 GHz radio frequencies (RF) bands • 802.11g : < 54 Mbps • 802.11n : < 150 Mbps	
Processor	• Intel Core 2 Dual Core (2.93 GHz)	
Operating System	• Windows (98,NT,2000,XP) • Red Hat Linux • Mac OS X	
Scalability	• Dual Band : < 64 (32 for the 2.4 GHz and 32 for the 5.0 GHz)	

BAMSS is implemented using Open Source software freely available under the GNU General Public License, the most widely used free software license. It consists of three modules: A network module, a computational module and a GUI for user interface. The modular architecture and the Open Source implementation ensure that the model can be modified with additional modules or developed further to address new challenges.

The BAMSS Network module uses the existing GeNIe library and allows the user to develop a Bayesian Network representation of the problem domain. This module is important because it allows users to define causal relations among the domain variables of interest. The user develops a Bayesian Network which qualitatively represents the problem domain to be modeled from these relations and by using directed acyclic graphs (DAG). Quantitatively, the user defines the network nodes and assigns prior probabilities which serve as inputs to the

computational module. Prior conditionals and marginal probability distributions are all input by the user based on his apriori knowledge of the problem domain. The user can develop several networks based on his/her core knowledge of the problem domain and store such networks in a repository on the client side of the network.

The Computational module takes the input data from the Network and performs belief updating and abductive inference using two inference algorithms. The Clustering Algorithm (Lauritzhen & Spiegenhalter, 1988; Jensen et al, 1990) is implemented to perform Bayesian belief updating. The Clustering Algorithm is an exact algorithm that works by compiling the DAG into a junction tree and then, updating the probability there. The Genetic Algorithm (GA) introduced by Goldberg (1989) and Mengshoel (1999) is an evolutionary search and optimization algorithm for quick variable classification and identification of complete solution sets. In the Bayesian Network module, abductive inference using the GA is accomplished by computing the MPE or *k*MPE of events in the Bayesian Network. Both algorithms in the main user interface have been implemented in Java.

The GUI module enables user interaction with BAMSS. It integrates the network module and the computational module and allows the user to manipulate inputs (evidence) while observing the changes in the outputs. The textual and graphical output helps in the analysis of the effects of the new evidence on the hypotheses or target variables. The interface is the front-end to the computational module and enables easy and intuitive data input into it while the visualization of the output makes it easier to for the user to understand. It enables the user to directly input values for new evidence or load a network from file. The GUI for the computational module has been designed as a standalone application to be hosted on the client PC and runs on Windows or Linux Operating Systems.

An example code for BAMSS implementation in Java is shown in Figure 12.

```
ntw.setBayesianAlgorithm(Network.BayesianAlgorithmType.Lauritzen);
            ntw.updateBeliefs();
            logger.info("Network initialisation completed.....");
         } catch (Error ex) {
            this.showMessage("SMILE", ex.getMessage());
            logger.debug(ex.getMessage(), ex);
         }
      }
……
…….
     private void updateBeliefbayesActionPerformed(java.awt.event.ActionEvent evt) {//
GEN-FIRST:event_updateBeliefbayesActionPerformed

      if (fileChooserTextField.getText().equals("")) {
         this.showMessage("SMILE- XDSL file not found", "Please select Model file first");
         return;
      }

      double xd = 0, x12 = 0, x13 = 0, x21 = 0, x22 = 0, x23 = 0, x24 = 0, x31 = 0, x32 = 0,
x33 = 0;
      double md = 0, m12 = 0, m13 = 0, m21 = 0, m22 = 0, m23 = 0, m24 = 0, m31 = 0, m32 =
0, m33 = 0, m41 = 0, m42 = 0, m43 = 0, m44 = 0;
      double td = 0, t12 = 0, t13 = 0, t21 = 0, t22 = 0, t23 = 0, t31 = 0, t32
……
……
 this.updateBayes(xd, x12, x13, x21, x22, x23, x24, x31, x32, x33, yd, y12, y13, y14, y21,
y22, y31, y32, y33, y41, y42, y43, md, m12, m13, m21, m22, m23, m24, m31, m32, m33,
m41, m42, m43, m44, td, t12, t13, t21, t22, t23, t31, t32);

      } catch (Exception ex) {
         this.showMessage("SMILE", ex.getMessage());
         logger.debug(ex.getMessage(), ex);
         ex.printStackTrace();
      }
   }//GEN-LAST:event_updateBeliefbayesActionPerformed

   private void x31InputActionPerformed(java.awt.event.ActionEvent evt) {//GEN-
FIRST:event_x31InputActionPerformed
      // TODO add your handling code here:
   }//GEN-LAST:event_x31InputActionPerformed
……
……...
```

Figure 12. Sample BAMSS implementation in Java.

4.1.2 Informational Flow Architecture in BAMSS

A generic representation of the architecture and information flow in the BAMSS model is shown in Figure 12. Initially, a user defined domain specific BBN is created and loaded into the model from file or any other linked database.

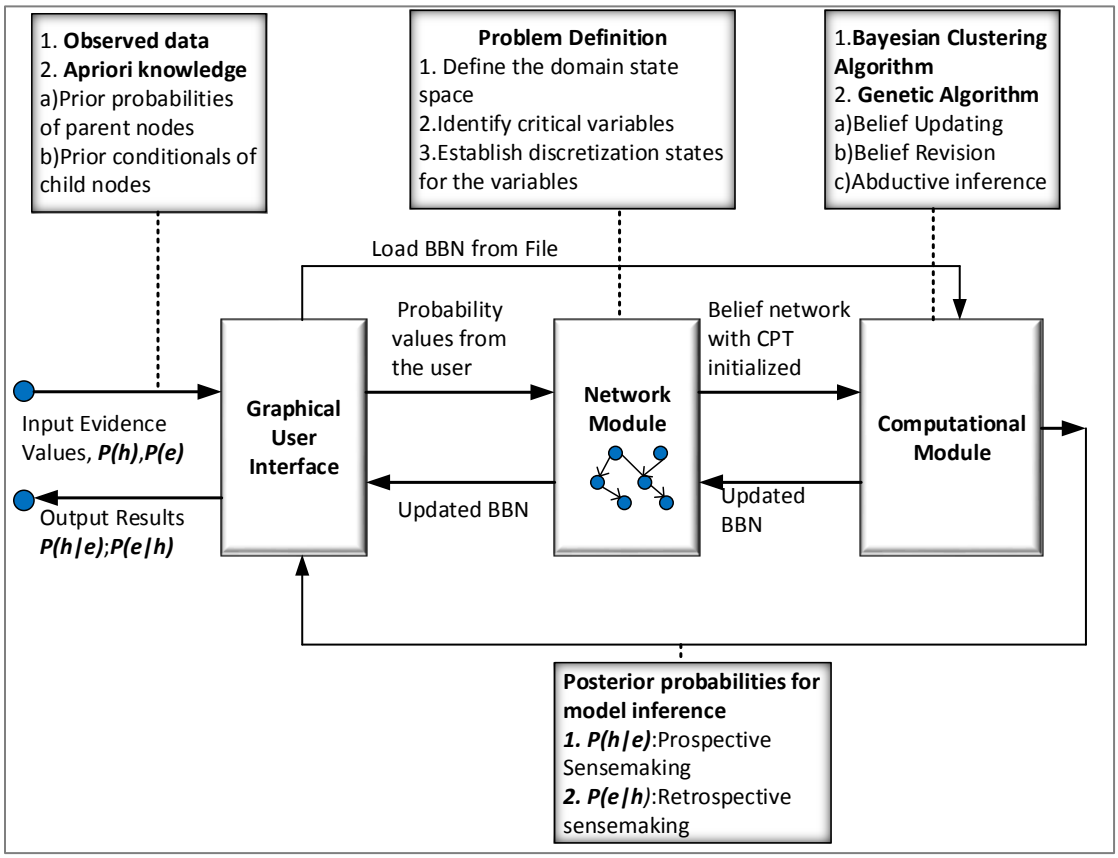

Figure 13. Information flow architecture in BAMSS.

Problem definition is undertaken in the network module during the development of the Belief Network. This involves defining the domain state space, identifying all the critical causal variables and their relationships, and establishing discretization states for all the identified variables. The network topology is also defined at this stage. New evidence such as observed data from the field or user defined prior probabilities of the parent nodes and the prior conditional probabilities of the child nodes are input into the developed network through the

GUI. The prior probabilities are obtained from expert judgment based on the user's tacit knowledge or historical records which document similar cases and their outcomes. In a collaborative work setting, the choice of priors may be a simple case of conjecture where several analysts brainstorm and agree on values that may be deemed representative of the domain-specific problem.

In the topology of the Network, the user defines the hypothesis variables, the evidence variables and the target variables of interest. A fully defined BBN with a defined topology and CPTs is then, loaded into the model through the GUI functionality. With the network loaded and initialized, evidence in the form of probabilities is input into the model through the GUI. The network module retrieves the input evidence from the user and initializes the appropriate BBN. The Belief Network with the initialized CPTs is then loaded into the computational module. The computational module is the inference engine of the model and undertakes updating of the Network Beliefs, Belief Revision, and Abductive Inference. Two algorithms are defined for this module; a clustering algorithm which is the fastest exact algorithm for the hierarchical Bayesian Network inference and a GA which is an approximate fast search and optimization algorithm for performing the Abductive Inference.

The GUI provides the option of selecting one or both of the algorithms and inputting parameters that are appropriate for each algorithm. The results of the computation are received as output by the user through the GUI and comprise of textual output of the posterior probabilities of the variables in the Belief Network and a graphical display of the updated Belief Network. The updated Belief Network is also loaded and stored in the Network module and can be retrieved by the computational module for the next iteration of Belief updating. Updated Beliefs form the prior probabilities for the network when the new evidence arrives.

The user can draw inferences through the posterior probability output derived from the computational module, concerning the best (most probable hypothesis) variable by Abductive Inference and this is referred to as prospective sensemaking. In the domain of asymmetric warfare, the "probability of attack| evidence" requires the best COA selection $P(h|e)$ from among all the hypotheses variables H in the updated Network. The user may also designate target nodes in the evidence variables and compute the probability $P(e|h)$ in the case of retrospective sensemaking. In the problematic domain under study, the "probability of attack" is known or set to a certain value by the user and the change in the value of the target nodes "probability of evidence|attack" is observed. In this case, the analyst is interested in finding out the most probable causal variable(s) that could produce the selected hypothetical outcome.

4.1.3 Inference Algorithm in BAMSS

To draw the Bayesian Network inference, the Bayesian Clustering Algorithm is used for data classification (Lauritzen & Spiegelhalter, 1988; Jensen et al., 1990). The algorithm works by first transforming the hierarchical Bayesian Network into a clique tree where each node in the tree corresponds to a subset of variables in the original graph. Message propagation is done over the clique tree. By transmitting information between the variables in the local clique rather than the full joint probability, one can realize and make tractable an efficient inference algorithm and inference in complex Bayesian Networks. The choice of the algorithm may be made based on the requirements for exact and efficient solution using BAMSS. These requirements, as first discussed by Lauritzen and Spiegelhalter (1988), for a hierarchical Bayesian network are described below:

1) *Initialization*: Generating internal representations of beliefs from which the marginal distributions on individual nodes may be easily obtained.

2) *Absorption of evidence*: The effect of multiple pieces of evidence should be independent of the order of their arrival
3) *Global propagation*: The algorithm should enable the propagation of the effects of the evidence received through the Network and enable for Belief revision in the nodes that are still not established.
4) *Hypothesizing and propagating single items of evidence*: The algorithm should allow for the ability to condition on a node taking on a particular value and observe its effect throughout the network.
5) *Planning*: For nodes of particular interest, the algorithm should provide for the ability to efficiently assess the informational value in eliciting the response to nodes corresponding to potentially obtainable data.
6) *Influential findings*: After the data are in, the algorithm should have an ability to retract their effect in order to identify the strong causal factors.

The clustering algorithm satisfies these requirements for BAMSS. The algorithm works hierarchically starting with the nodes at the top of the network and randomly (depending on the node distribution) selecting a state. This state will then be set and will influence the probabilities of all the nodes that have that node as a parent. The algorithm moves through all the nodes this way, randomly selecting states and setting them as evidence. The sampling is complete when a state is assigned to all the nodes and Belief updating is then performed.

According to the second requirement, BAMSS uses information from multiple sources of uncertainty as input. The evidence variables are informational variables since they reveal information about hypothesis variables. The process of computationally combining these informational variables to perform inferences on some target variable (usually a hypothesis

variable) is referred to as information fusion. The pseudo code for BAMSS inference algorithm is shown in Figure 14.

```
1. Load model from file
2. Set evidence for the node(s)
        a. Select the node of interest
        b. Set evidence for this node
3. While (stopping criteria not met) {
    Update the network by performing inference
        Read out the posterior probabilities of the variables of interest
          a. Select node of interest
          b. Loop over all the states and collect the probabilities
          c. End loop
    End if < condition> met
            }
4. Output the posterior probabilities
```

Figure 14. Bayesian inference algorithm for BAMSS.

4.1.4 BAMSS Working Memory

Figure 15 shows a screen capture of the GUI for the BAMSS working memory. In the first operation, the domain specific BBN from a file residing on the client computer is loaded into the module. With the BBN loaded, the user can use the GUI to perform other required functions such as inputting new evidence, using commands for computing posterior probabilities, performing inference and so on. The interface can be divided into four quadrants. The first quadrant contains the input fields for all the random variables defined in the Network module. The Network residing on the client side database is loaded into the GUI using the "Select Model File" command line. Evidence in the form of numeric probabilities is then typed into the evidence input fields. The fields are grouped according to the defined network hierarchical levels

with the topmost level containing fields for hypothesis variables, followed by fields for Level 1 evidence variables, Level 2 evidence variables, Level 3 evidence variables and Level 4 evidence variables. The evidence input fields are non-mandatory, that is, the user can input evidence for a single variable or can select multiple variables on different levels.

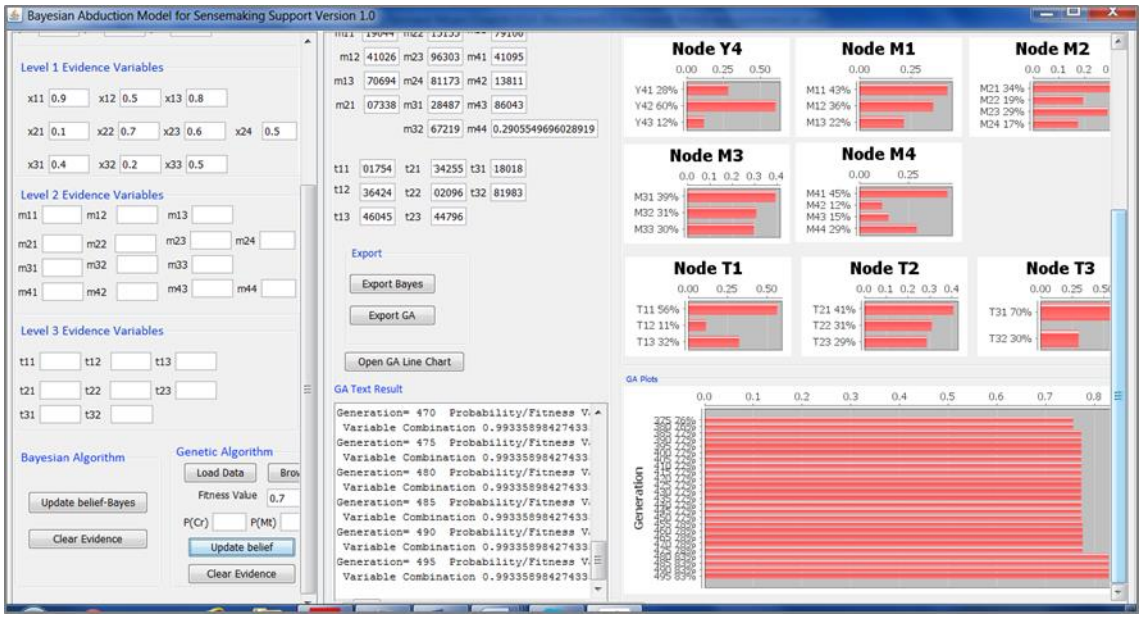

Figure 15. Graphical user interface for the BAMSS model.

To perform computational inference, the appropriate algorithm is selected from the command buttons at the bottom of the first quadrant. Selecting "Update Belief-Bayes" will enable the computation of the posterior beliefs of the Network variables given new evidence using the clustering algorithm. The algorithm gets the query and goes through the cyclic process of hierarchically sampling the nodes and assigning states until all the nodes in the network have an assigned state. Belief updating is then undertaken and the completed results are compiled and output by the appropriate function in the *ProbabilityUI.java* subroutine. Selection of the GA requires input of a fitness value and some optional GA parameters such as the probability of mutation. The results for both algorithms can be exported into a text file format using the appropriate "Export" command button.

The second and third quadrants show the results of the Belief updating process for the selected algorithm, both textually and graphically. The GA textual results fields display the gene/variable combination that constitutes a network solution for the input data. The last quadrant on the bottom right shows the graphical plots of the GA search process for all the network variables for the specified number of generations until the stop criterion is met. The "Clear Evidence" command button allows the user to clear the input and output fields of the GUI and input new evidence at any point of time.

4.2 Sample Application: Sensemaking in Asymmetric Warfare Domain

4.2.1 Identification of Domain Variables

The US Army led invasion of Iraq − *Operation Iraqi Freedom* (OIF, Iraq, 2003-2009) and Afghanistan, − *Operation Enduring Freedom* (OEF, Afghanistan, 2001-2014) and the Arab-Israeli conflict − particularly the Israeli-Hezbollah War (Lebanon, 2006) were used as case studies for domain understanding, variable identification and extracting the BAMSS data set. The identified domain variables and their relationships were iteratively refined following interactions with the domain experts before the final set of variables and links was selected to create the Network structure. By expert consensus, four key effects that supported a commander's asymmetric battlespace analysis were also identified.

The first level variables identified were Strategic Effects. In the Network topology, these were defined as the level 1 hypotheses variables representing the end states, target states, or goals of the adversary that the Blue Force commander would have to correctly infer for successful counterinsurgency operations. These effects could be both short-term and long-term. These top level effects informed the commander of the adversary's strategies and were key for effective COA planning. Strategic effects were directly influenced by Political Operational

Effects which constituted level 2 evidence variables. Political Operational Effects were defined as informational variables that represented the Political, Military, Economic, Social, Information and Infrastructural (PMESII) variables of the battlespace. The operational environment would need to integrate the PMESII variables to fully define the battlespace. The PMESII variables were identified as causal mechanisms that could influence the Strategic Effects.

Military Operational Effects were informational variables that the adversary could exploit to achieve the desired end state or target state. In the Network topology, these variables constituted level 3 evidence variables that commanders and their staffs would need to analyze to correctly infer the desired end state of the adversary. The adversary could aim at generating and exploiting fine scale complexity and seek to prevent the counterinsurgents from acting at the scale they were organized for: large scale but limited complexity environment (Ryan, 2008). These effects could be deemed dynamic variables that changed constantly depending on changes in both the internal and external factors of a group. These variables could also directly influence the Political Operational Effects.

Tactical effects were identified as informational variables that represented the tactical effects of the battlespace and constituted level 4 evidence variables in the Network topology. These were sensor observable and represented actions taken by the insurgents to influence certain outcomes in the battlespace. Depending on the choice of targets, the range of Tactical Effects was considered to be very extensive and diverse. Most of these effects were kinetic and their strategic outcome was usually second order and not necessarily a direct outcome. Destruction of a key military installation for example, could have value not in the physical destruction of the target but in the psychological impact the COA would generate among the

population. Figure 16 shows an example network to represent the levels of information discussed in the preceding section.

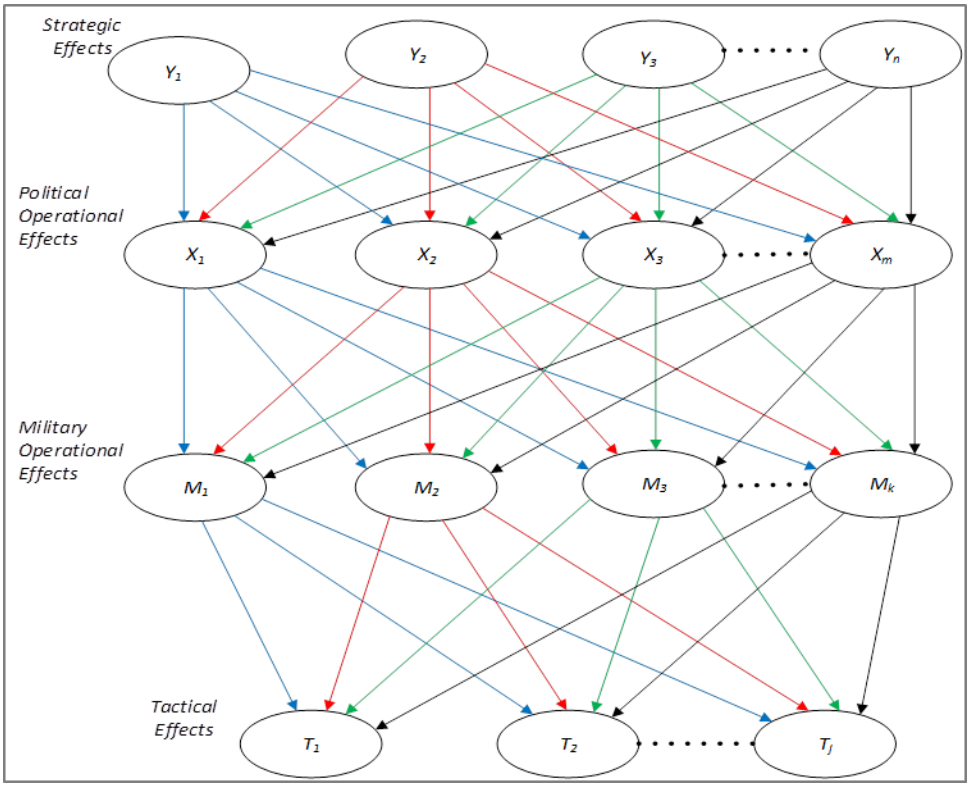

Figure 16. BN topology for adversary intent inference in asymmetric battlespace.

4.2.2 Discretization of the Bayesian Network Variables

The variables in the Network as shown in Figure 16 are discretized into nonnumeric sub factors so as to use the exact search algorithm implemented in BAMSS. The discretization is based on factors obtained from literature review as well as expert judgment. The states of each node in the Network are sub-factors, and they represent all the possible indicators each variable can take within the domain state space. With the Network topology defined and all the variables discretized, we can fully specify its parameters.

Network parameterization is completed by learning the prior probabilities of all the nodes without parents and the conditional probabilities of all the nodes with parents, conditional on

these parents. A description of all the Network variables along with their discrete states or indicators is provided in Appendix A. With the discretization of the variables and the discrete states defined, the next step is to perform simulation with the model.

4.3 Experimental Evaluation

4.3.1 The Simulation Process

A simulation experiment was used to validate BAMSS using historical data. Initial probabilities for the parent nodes were obtained from intensive research of databases and reports on insurgency and counterinsurgency operations in the Middle East. An example of a database used is the RAND Database of Worldwide (RDWTI), available at http://www.rand.org/nsrd/projects/terrorism-incidents.html (web accessed on 12/16/2013). The RDWTI is a compilation of data from 1968 through 2009 and is free and publicly accessible for research and analysis.

Although the database deals primarily with terrorism incidents, these data were considered relevant because terrorism is always used as an operations tactic by insurgents. The attributes of terrorism considered relevant to this study are available in the RDWTI and include factors such as its use as a military tactic, psychological intentions to cause fear and alarm among the population, targeting of civilians and the military forces, group dynamics, and political motivation. More apriori data was obtained from the Global Terrorism Data base (GTD), an Open Source database hosted by the University of Maryland and the Brookings Institution (http://www.start.umd.edu/gtd/ web accessed on 12/16/2013). Other information from the databases was derived based their proportion (percentage) of occurrences. Where appropriately defined, these data provided initial prior probabilities. Tables 3, 4, and 5 contain data obtained from these available databases. The data are summarized and reformatted to focus

only on the key variables in the problem domain. Table 3 gives the range of targeted actions used by insurgents in the region. In the asymmetric battlespace domain, we have focused on some of these targeted actions to inform our range of adversary Tactical Effects. Table 4 lists the weapons used to implement the targeted actions, an important part of the Tactical Effects modelling.

Table 3

The RAND Database of Worldwide Terrorism Incidents, Middle East Region: Targeted Actions 2003-2007

Tactic	Count	Percentage
Bombing	6261	52.23 %
Armed Attack	4248	35.44 %
Kidnapping	816	6.81 %
Assassination	435	3.63 %
Unknown	140	1.17 %
Arson	42	0.35 %
Other	21	0.18 %
Unconventional Attack	9	0.08 %
Barricade/Hostage	8	0.07 %
Other	5	0.04 %
Hijacking	2	0.02 %

Table 4

The RAND Database of Worldwide Terrorism Incidents, Middle East Region: Weapons, 2003-2007

Weapon	Count	Percentage
Explosives	6103	50.91 %
Firearms	4850	40.46 %
Unknown	455	3.8 %
Remote-detonated explosive	349	2.91 %
Fire or Firebomb	115	0.96 %
Knives & sharp objects	67	0.56 %
Other	40	0.33 %
Chemical Agent	8	0.07 %

Table 5

The RAND Database of Worldwide Terrorism Incidents, Middle East Region: Targets, 2003-2007

Target	Count	Percentage
Police	3827	31.93 %
Private Citizens & Property	2589	21.6 %
Government	1773	14.79 %
Other	1123	9.37 %
Religious Figures/Institutions	705	5.88 %
Utilities	458	3.82 %
Business	418	3.49 %
Transportation	220	1.84 %
Educational Institutions	216	1.8 %
Journalists & Media	198	1.65 %
Diplomatic	146	1.22 %
Unknown	130	1.08 %
Military	70	0.58 %
NGO	47	0.39 %
Telecommunication	29	0.24 %
Airports & Airlines	16	0.13 %
Terrorists/Former Terrorists	12	0.1 %
Tourists	5	0.04 %
Food or Water Supply	4	0.03 %

The data were input into the BAMSS model and a simulation run was performed. CPTs for all nodes conditional on the predecessor nodes were also populated. For the CPT elicitation, a Noisy-Max canonical model function built in GeNIe was used to provide a logarithmic reduction in the complexity of parameter estimation in the BN (Pradhan et al., 1994; Onisko et al., 2000). In this canonical model, the presence of one causal factor in the parent node was sufficient to produce an impact in the child node. This canonical model was especially useful for the BAMSS network because the influence of each parent node on the child node needed to be considered independent of the other parents. Additionally, we did not need to specify all the causal factors necessary to produce an outcome in order to define the CPTs because this could be difficult for

the experts and computationally intractable to learn from datasets. Therefore, the Noisy-Max model was deemed best applicable to real life problems. The use of this canonical model for multi-valued variables has been advocated by Zagorecki and Druzdzel (2006) Zagorecki, Voortman and Druzdzel (2006), and Dietz (1993). Figure 17 shows a complete 14 node network developed for the simulation .As an example, Table 6 defines the nodes and the states for each level 2 (Political Operational Effects) variable node used in the CPT computation.

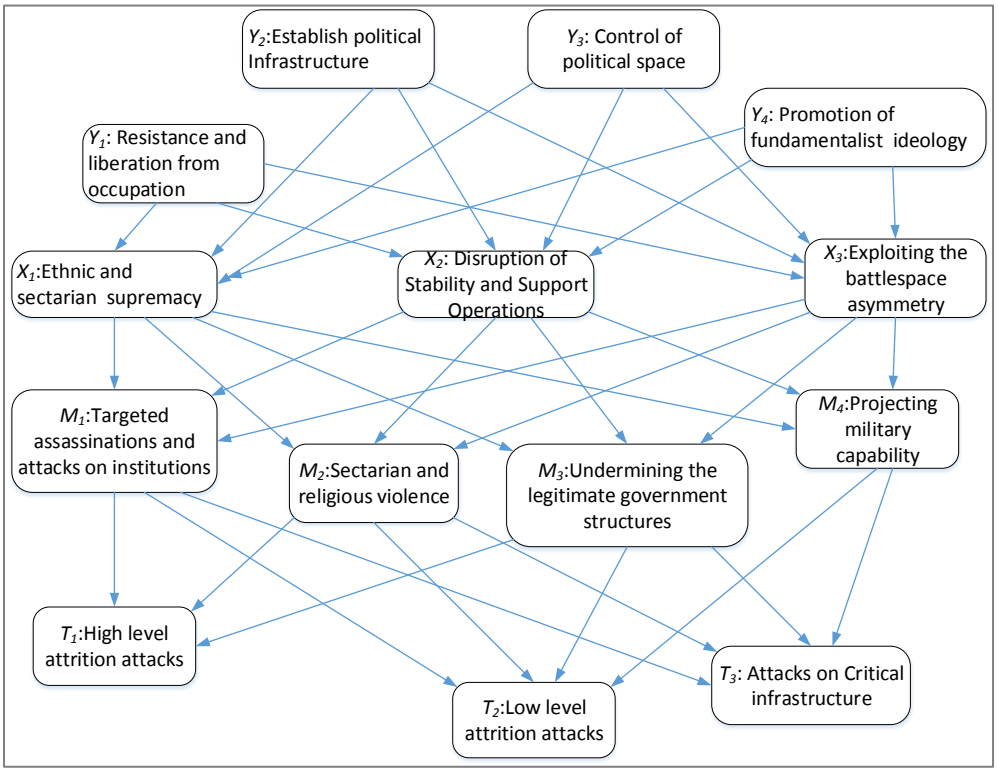

Figure 17. BAMSS course of action analysis network.

An example of the populated CPTs for the *Political Operational Effects* variables X_1, X_2 and X_3 conditional on the *Strategic Effects* nodes Y_1,Y_2, Y_3 and Y_4 is shown in Tables 6 - 9.

Table 6

Complete CPT Elicited for Level 2 Nodes of the BAMSS COA Analysis Network

Y_1	y_{11}= *Resistance and liberation*																	
Y_2	y_{21}=*Sectarian Governance Structures*									y_{22}=*Insurgent Ideology*								
Y_3	y_{31}=*Political opposition*			y_{32}=*Control of security Space*			y_{33}=*Disruption of civic processes*			y_{31}=*Political opposition*			y_{32}=*Control of security space*			y_{33}=*Disruption of civic processes*		
Y_4	y_{41}	y_{42}	y_{43}	y_{41}	y_{42}	y_{43}	y_{41}	y_{42}	y_{43}	y_{41}	y_{42}	y_{43}	y_{41}	y_{42}	y_{43}	y_{41}	y_{42}	y_{43}
x_{11}	0.43	0.43	0.43	0.44	0.44	0.44	0.43	0.43	0.43	0.41	0.41	0.44	0.42	0.42	0.42	0.41	0.41	0.41
x_{12}	0.32	0.33	0.32	0.31	0.31	0.31	0.32	0.33	0.32	0.33	0.34	0.33	0.32	0.32	0.32	0.33	0.33	0.33
x_{13}	0.23	0.23	0.23	0.24	0.23	0.24	0.24	0.24	0.24	0.24	0.24	0.24	0.24	0.24	0.24	0.25	0.24	0.25
x_{21}	0.23	0.23	0.19	0.23	0.23	0.19	0.19	0.19	0.14	0.19	0.19	0.15	0.19	0.19	0.15	0.15	0.15	0.10
x_{22}	0.44	0.44	0.47	0.44	0.44	0.47	0.47	0.47	0.49	0.46	0.46	0.49	0.46	0.46	0.49	0.49	0.49	0.52
x_{23}	0.15	0.15	0.16	0.15	0.15	0.16	0.16	0.16	0.17	0.16	0.16	0.17	0.16	0.16	0.17	0.17	0.17	0.18
x_{24}	0.15	0.15	0.16	0.15	0.15	0.16	0.16	0.16	0.17	0.16	0.16	0.17	0.16	0.16	0.17	0.17	0.17	0.18
x_{31}	0.47	0.48	0.47	0.44	0.44	0.44	0.44	0.44	0.44	0.47	0.48	0.47	0.44	0.44	0.44	0.44	0.44	0.44
x_{32}	0.36	0.36	0.36	0.39	0.38	0.39	0.39	0.38	0.39	0.32	0.32	0.32	0.34	0.34	0.34	0.34	0.34	0.34
x_{33}	0.15	0.15	0.15	0.16	0.16	0.16	0.16	0.16	0.16	0.19	0.19	0.19	0.20	0.20	0.20	0.21	0.20	0.21

Table 7

Complete CPT Elicited for Level 2 Nodes of the BAMSS COA Analysis Network

Y_1	y_{12}=*Law and order breakdown*																	
Y_2	y_{21}=*Sectarian governance structures*									y_{22}=*Insurgent ideology*								
Y_3	y_{31}=*Political opposition*			y_{32}=*Control of security space*			y_{33}=*Disruption of civic processes*			y_{31}=*Political opposition*			y_{32}=*Control of security space*			y_{33}=*Disruption of civic processes*		
Y_4	y_{41}	y_{42}	y_{43}	y_{41}	y_{42}	y_{43}	y_{41}	y_{42}	y_{43}	y_{41}	y_{42}	y_{43}	y_{41}	y_{42}	y_{43}	y_{41}	y_{42}	y_{43}
x_{11}	0.40	0.40	0.40	0.41	0.41	0.41	0.40	0.40	0.40	0.38	0.38	0.38	0.39	0.39	0.39	0.38	0.38	0.38
x_{12}	0 20	0.20	0.20	019	0.19	0.19	019	0.19	0.19	0.21	0.21	0.21	0. 19	0.19	0.19	0.19	0.20	0.19
x_{13}	0.39	0.38	0.39	0.39	0.39	0.39	0.40	0.39	0.40	0.40	0.39	0.40	0. 40	0.40	0.40	0.41	0.40	0.41
x_{21}	0.23	0.23	0.19	0.23	0.23	0.19	0.19	0.19	0.14	0.19	0.19	0.15	0.19	0.19	0.15	0.15	0.15	010
x_{22}	0.44	0.44	0.47	0.44	0.44	0.47	0.47	0.47	0.49	0.46	0.46	0.49	0.46	0.46	0.49	0.49	0.49	0.52
x_{23}	0.15	0.15	0.16	0.15	0.15	0.16	0.16	0.16	0.17	0.16	0.16	0.17	0.16	0.16	0.17	0.17	0.17	0.18
x_{24}	0.15	0.15	0.16	0.15	0.15	0.16	0.16	0.16	0.17	0.16	0.16	0.17	0.16	0.16	0.17	0.17	0.17	0.18
x_{31}	0.47	0.48	0.47	0.44	0.44	0.44	0.44	0.44	0.44	0.47	0.47	0.47	0.44	0.44	0.44	0.44	0.44	0.44
x_{32}	0.36	0.35	0.36	0.38	0.38	0.38	0.38	0.38	0.38	0.31	0.31	0.31	0.33	0.33	0.33	0.33	0.33	0.33
x_{33}	0.16	0.16	0.16	0.17	0.17	0.17	0.17	0.16	0.17	0.20	0.20	0.20	0.22	0.21	0.22	0.22	0.22	0.22

Table 8

Complete CPT Elicited for Level 2 Nodes of the BAMSS COA Analysis Network

Y_1	y_{13}=Population control																	
Y_2	y_{21}=Sectarian governance structures									y_{22}=Insurgent ideology								
Y_3	y_{31}=Political opposition			y_{32}=Control of security space			y_{33}=Disruption of civic processes			y_{31}=Political opposition			y_{32}=Control of security space			y_{33}=Disruption of civic processes		
Y_4	y_{41}	y_{42}	y_{43}	y_{41}	y_{42}	y_{43}	y_{41}	y_{42}	y_{43}	y_{41}	y_{42}	y_{43}	y_{41}	y_{42}	y_{43}	y_{41}	y_{42}	y_{43}
x_{11}	0.50	0.50	0.50	0.51	0.51	0.41	0.50	0.50	0.50	0.48	0.49	0.48	0.49	0.49	0.49	0.48	0.49	0.48
x_{12}	0 20	0.20	0.20	019	0.19	0.19	019	0.19	0.19	0.20	0.21	0.20	0. 19	0.19	0.19	0.20	0.20	0.20
x_{13}	0.29	0.29	0.29	0.29	0.29	0.29	0.30	0.29	0.30	0.30	0.29	0.30	0. 30	0.30	0.30	0.30	0.30	0.30
x_{21}	0.23	0.23	0.19	0.23	0.23	0.19	0.19	0.19	0.14	0.19	0.19	0.15	0.19	0.19	0.15	0.15	0.15	010
x_{22}	0.44	0.44	0.47	0.44	0.44	0.47	0.47	0.47	0.49	0.46	0.46	0.49	0.46	0.46	0.49	0.49	0.49	0.52
x_{23}	0.15	0.15	0.16	0.15	0.15	0.16	0.16	0.16	0.17	0.16	0.16	0.17	0.16	0.16	0.17	0.17	0.17	0.18
x_{24}	0.15	0.15	0.16	0.15	0.15	0.16	0.16	0.16	0.17	0.16	0.16	0.17	0.16	0.16	0.17	0.17	0.17	0.18
x_{31}	0.32	0.33	0.32	0.28	0.29	0.28	0.28	0.29	0.28	0.32	0.33	0.32	0.28	0.29	0.28	0.28	0.29	0.28
x_{32}	0.50	0.50	0.50	0.53	0.53	0.53	0.53	0.53	0.53	0.45	0.45	0.45	0.48	0.48	0.48	0.48	0.48	0.47
x_{33}	0.16	0.16	0.16	0.17	0.17	0.17	0.17	0.17	0.17	0.21	0.21	0.21	0.22	0.22	0.22	0.22	0.22	0.22

Table 9

Complete CPT Elicited for Level 2 Nodes of the BAMSS COA Analysis Network

Y_1	y_{14}=Excessive force																	
Y_2	y_{21}=Sectarian governance structures									y_{22}=Insurgent ideology								
Y_3	y_{31}=Political opposition			y_{32}=Control of security space			y_{33}=Disruption of civic processes			y_{31}=Political opposition			y_{32}=Control of security space			y_{33}=Disruption of civic processes		
Y_4	y_{41}	y_{42}	y_{43}	y_{41}	y_{42}	y_{43}	y_{41}	y_{42}	y_{43}	y_{41}	y_{42}	y_{43}	y_{41}	y_{42}	y_{43}	y_{41}	y_{42}	y_{43}
x_{11}	0.40	0.40	0.40	0.41	0.41	0.41	0.40	0.40	0.40	0.38	0.38	0.38	0.39	0.39	0.39	0.38	0.38	0.38
x_{12}	0 20	0.20	0.20	019	0.19	0.19	019	0.19	0.19	0.21	0.21	0.21	0. 19	0.19	0.19	0.19	0.20	0.19
x_{13}	0.39	0.38	0.39	0.39	0.39	0.39	0.40	0.39	0.40	0.40	0.39	0.40	0. 40	0.40	0.40	0.41	0.40	0.41
x_{21}	0.18	0.18	0.14	0.18	0.18	0.14	0.14	0.14	0.09	0.14	0.14	0.09	0.09	0.14	0.09	0.09	0.09	0.04
x_{22}	0.47	0.47	0.50	0.47	0.47	0.50	0.50	0.50	0.53	0.49	0.49	0.52	0.52	0.49	0.52	0.52	0.52	0.55
x_{23}	0.16	0.16	0.17	0.16	0.16	0.17	0.17	0.17	0.18	0.17	0.17	0.18	0.18	0.17	0.18	0.18	0.18	0.19
x_{24}	0.16	0.16	0.17	0.16	0.16	0.17	0.17	0.17	0.18	0.17	0.17	0.18	0.18	0.17	0.18	0.18	0.18	0.19
x_{31}	0.31	0.32	0.31	0.27	0.28	0.27	0.27	0.28	0.27	0.31	0.32	0.27	0.28	0.27	0.27	0.27	0.28	0.27
x_{32}	0.46	0.46	0.46	0.49	0.49	0.49	0.49	0.49	0.49	0.40	0.40	0.43	0.43	0.43	0.43	0.43	0.43	0.43
x_{33}	0.21	0.21	0.21	0.22	0.22	0.22	0.22	0.22	0.22	0.27	0.27	0.28	0.28	0.28	0.28	0.28	0.28	0.28

Belief update was undertaken after the CPT computation and the resultant posterior probabilities for all the nodes were displayed. Figure 18 shows this in a forward inference scheme. The output displayed on the right side of the GUI is both graphical and textual.

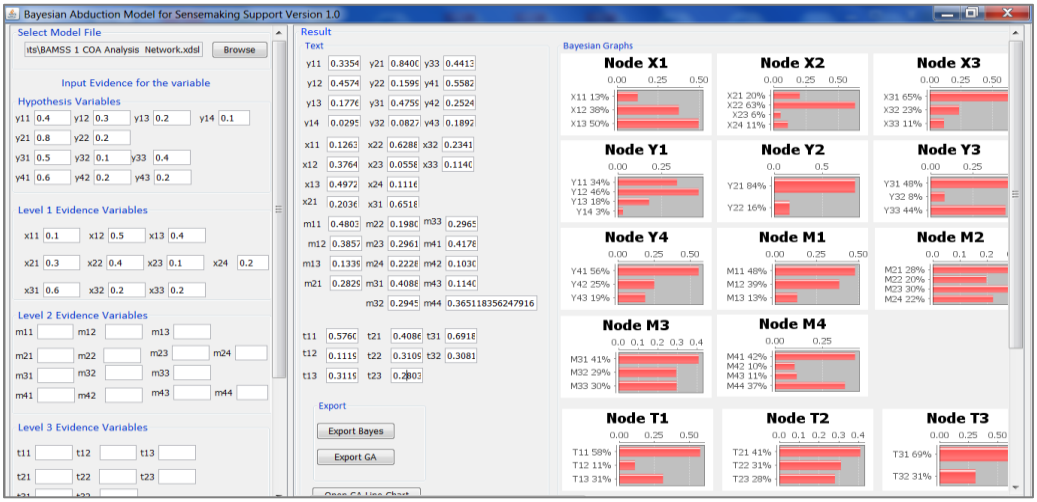

Figure 18. Belief updating (posterior probabilities) of the nodes in the network after new evidence is introduced.

For illustration purposes, assume that the evidence for the hypotheses variables Y_1,Y_2, Y_3 and Y_4 is set as follows: Let the probability of node Y_1 being in state y_{11}= 0.4 represent the belief that there is a 40% chance that the objective of the insurgency is resistance and liberation of the country from occupation. Node $Y_1 = y_{12}$ is ascribed a probability of 0.3, meaning there is a 30% chance that a breakdown in law and order to disrupt counterinsurgent control of the local security situation is the effect under observation. Less belief $Y_1 = y_{13}$= 0.2 is given to probability that the insurgent's intent is to exercise local population control. By the axioms of probability, the complement $Y_1 = y_{14}$ = 0.1 represents our belief that the effect under observation is simply an intent by the insurgents to provoke excessive raids by the counterinsurgent forces and use the second order effects of that action as a strategy for resistance.

To account for multiple sources of information, the input fields are not mutually exclusive and the values for nodes Y_2, Y_3 and Y_4 may be input. Assume that there is reason to believe that the end state of the insurgency is to establish some form of political infrastructure to legitimize the armed struggle (Y_2). If this hypothesis is chosen, then, it is believed that the effect under observation is related to the development of sectarian governance structures with a probability $Y_2 = y_{21} = 0.8$. The complement $Y_2 = y_{22} = 0.2$ is attributed to the hypothesis that the insurgency political agenda is driven purely by radical ideologies to which the followers subscribe. Variables Y_3 ($y_{31} = 0.5$, $y_{32} = 0.1$, $y_{33} = 0.4$) and Y_4 ($y_{41} = 0.6$, $y_{42} = 0.2$, $y_{43} = 0.1$) are similarly defined.

Next, we input the evidence values for level 2 evidence variables, the Political Operational Effects X_1, X_2 and X_3. This is evidence that is obtainable by direct observation of battlefield conditions or by analyzing information from various sources. It is known that a major influencing factor for conflict in the Middle East is ethnic and sectarian supremacy (X_1). By analyzing reports, the indicators are weighted such that fundamentalist ideology $X_1 = x_{12}$ is most probable at 50%. Equally probable is the legitimacy of Jihad or armed struggle against non-believers $X_1|x_{13} = 0.4$. Sectarian identity ($X_1 = x_{11}$), though a dominant concept in insurgencies, is weakly supported with a 0.1 probability. For factor X_2, evidence for disruption of the ability to carry out nation-building and stability operations is assessed. To this, there is slightly more evidence of operational modularity ($X_2 = x_{22} = 0.4$), than the exploitation of local environment and feedback mechanisms ($X_2 = x_{21} = 0.3$). Little evidence supports the notion of ad hoc threat forces, criminal networks or part time forces ($X_2 = x_{23} = 0.1$) while direct force projection to send a message of capability to the population ($X_2 = x_{24} = 0.2$) is marginally better. Similarly, evidence

values for variable X_3 (x_{31} = 0.6, x_{32} = 0.2, x_{33} = 0.2) are input. More evidence may be entered for level 3 (Military Operational Effects) and level 4 (Political Operational Effects) variables.

The right hand side of Figure 18 shows the textual and graphical output of the computed posterior beliefs of all the network variables after Belief Update in the light of new evidence is performed. For the input evidence values discussed above, the computed posterior beliefs (correct to three decimal places) are as follows: For variable Y_1, y_{11} = 0.335, y_{12} = 0.457, y_{13} = 0.178, y_{14} = 0.030. The net effect of the new evidence was to decrease our belief in hypothesis $Y_1 = y_{11}$ from 40% to 34% and increase our belief in hypothesis $Y_1 = y_{12}$ from 30% to 46%. For variable Y_2, y_{21} = 0.840 and y_{22} = 0.150. In this case, the new evidence did not significantly change our belief concerning the variable. The same conclusion may be drawn for variables Y_3 and Y_4, whose posterior beliefs are y_{31} = 0.476, y_{32} = 0.082, y_{33} = 0.441, y_{41} = 0.558, y_{42} = 0.252, y_{43} = 0.189.

The computed posterior beliefs for the Political Operational Effects nodes X_1, X_2 and X_3 are: X_1[x_{11} = 0.126, x_{12} = 0.376, x_{13} = 0.497], X_2[x_{21} = 0.203, x_{22} = 0.629, x_{23} = 0.056, x_{24} = 0.112] and X_3[x_{31} = 0.652, x_{32} = 0.234, x_{33}=0.114]. The computed posterior probabilities for the Military Operational Effects nodes M_1, M_2, M_3 and M_4 are: M_1[m_{11} = 0.480, m_{12} = 0.386, m_{13} = 0.134], M_2[m_{21} = 0.283, m_{22} = 0.198, m_{23} = 0.296, m_{24} = 0.223], M_3[m_{31} = 0.408, m_{32} = 0.295, m_{33} = 0.297] and M_4 [m_{41} = 0.418, m_{42} = 0.103, m_{43} = 0.114, m_{44} = 0.365]. Posterior distribution results for the Tactical Effects nodes T_1, T_2 and T_3 are: T_1[t_{11} = 0.576, t_{12} = 0.112, t_{13} = 0.312], T_2[t_{21} = 0.409, t_{22} = 0.311, t_{23} = 0.280], and T_3[t_{31} = 0.692, t_{32} = 0.308]. Posterior beliefs for the entire Network are displayed in graphical format under the “Bayesian Graphs” data field as displayed as shown in Figure 18. The posterior probability of each state of variable (textual result) is displayed by a bar chart under the variable node.

Several simulation runs were performed to test the model. A simulation run consisted of mapping of the level 1 Strategic Effects (Y), the level 2 Political Operational Effects (X), the level 3 Military Operational Effects (M), and the level 4 Tactical Effects (T). Dimensionally, the simulation space was an Y * X* M * T design. The complexity of the Network was determined by the number of elements in Y, X, M, and T respectively. In this case Y = 12, X = 10, M = 14, and T = 8, there were 13,440 possible trial runs by the BAMSS model. However, the mappings were also realized through probabilistic decision nodes. The minimum number of experiments were then equal to 1 (assume Y = 1, X = 1, M = 1, T = 1). Hence, the probabilistic (expected) number of experiments depended on the user's input and could be constrained by $1 \leq NE \leq \#E$ where, #E = Y * X * M * T, and at least one Y, X, M, or T had elements greater than 1. For the simulation runs discussed in the next section new evidence was introduced to nodes selected randomly for each variable level. Belief Updating was performed and the results of the updating for all the nodes were recorded. Four simulations were conducted, one for each level of network variables for a total of 44 simulation experiments.

4.3.2 Evidence Propagation in the Bayesian Network

Posterior distributions were obtained for different variables in the Network using random input evidence for different simulated scenarios. The hierarchical BBN was initialized with prior probabilities for the parent nodes and prior conditional probabilities for all the child nodes at each Network level and loaded into the model. A node was randomly in the Network was randomly selected and used as an input node for new evidence introduced into the model. With the input evidence varying from 0.1 to 0.9 in the range [0, 1], several simulation runs were performed on the model and the posterior belief distribution for each value of input evidence recorded. With these simulations experimental data were collected and used to evaluate the

robustness of the model as well as validation for accuracy. Some simplifications were made for purposes of demonstration such as the completeness of the CPT specification in the model. In practice however, it is extremely difficult to fill the CPTs with appropriate numbers. With large datasets, it is possible to learn the CPTs from real world data (Neapolitan, 2004).

In the asymmetric warfare domain, such data is difficult to access because of restrictions imposed by national security concerns. Tables 10-17 show the posterior belief distributions from the experimental simulation. These distributions represent the updated Beliefs for the nodes in the Network as new evidence is introduced. The propagation of the new evidence at all levels of the network nodes is shown graphically in Figures 19, 20, and 21. Sample statistics are displayed for each simulation run showing the mean belief accrual and the standard deviation per value of input evidence for all the variables at the selected level.

Table 10

Belief Update in Level 1(Strategic Effects) Nodes

Simulation Run	**Posterior Belief**											
	Strategic Effects											
Input Variable $X_1=x_{11}$	y_{11}	y_{12}	y_{13}	y_{14}	y_{21}	y_{22}	y_{31}	y_{32}	y_{33}	y_{41}	y_{42}	y_{43}
0.1	0.19	0.46	0.26	0.09	0.60	0.40	0.30	0.30	0.40	0.30	0.40	0.30
0.2	0.19	0.45	0.27	0.09	0.60	0.40	0.30	0.30	0.40	0.30	0.40	0.30
0.4	0.20	0.42	0.29	0.10	0.60	0.40	0.30	0.30	0.40	0.30	0.40	0.30
0.5	0.20	0.40	0.30	0.10	0.60	0.40	0.30	0.30	0.40	0.30	0.40	0.30
0.7	0.21	0.36	0.32	0.11	0.60	0.40	0.30	0.30	0.40	0.30	0.40	0.30
0.8	0.21	0.34	0.34	0.11	0.59	0.40	0.30	0.30	0.40	0.30	0.40	0.30
0.9	0.21	0.32	0.35	0.12	0.61	0.39	0.29	0.30	0.40	0.30	0.40	0.30

In Table 10, variables Y_3 and Y_4 exhibit steady state values of posterior probabilities for all values of the input variable X_1. To explain this behavior, we examine the CPTs and in particular, the priors of Y_3 and Y_4 and prior conditionals such as $P(X_1 = x_{11}|Y_3 = y_{33})$ or P(X_1 =

$x_{11}|Y_4 = y_{41}$). $X_1 = x_{11}$ represented the factor *Sectarian Identity* while $Y_4 = y_{41}$ represented the factor *Nationalism*. The expression P($X_1 = x_{11}|Y_4 = y_{41}$) or *P(Nationalism| Sectarian Identity*) could not be defined in the context of the problem. These inadmissible combinations led to oversampling by the algorithm resulting into steady state values of posterior probabilities and incompatible hypotheses. Table 11 shows a statistical analysis of the posterior belief distribution. The sample size refers to the total state space in Table 10 while the mean evidential accrual and the standard deviation are derived from the posterior distribution of Table 10.

Table 11

Statistical Analysis of Posterior Belief Distribution of Level 1 Nodes

Simulation Run	**Posterior Belief**		
Input Variable $X_1=x_{11}$	**Sample Size**	**Mean**	**Std. Deviation**
0.1	12	0.333	0.125
0.2	12	0.333	0.124
0.4	12	0.334	0.119
0.5	12	0.333	0.117
0.7	12	0.333	0.113
0.8	12	0.332	0.111
0.9	12	0.332	0.113

Table 12 shows the posterior belief distribution for the level 2 (*Political Operational Effects*) evidence nodes with the statistical analysis in Table 13.The variable $X_2 = x_{24}$ exhibits steady state values for all the simulation runs. During network development, the prior conditional P($X_2 = x_{24}|$ $M_2 = m_{22}$) was set at 20%. Contextual analysis showed that the expression P($X_2 = x_{24}|$ $M_2 = m_{22}$) = 0.20 was not admissible contributing to the steady state values for the variable.

Table 12

Belief Update in Level 2(Political Operational Effects) Nodes

Simulation Run	**Posterior Belief**									
	Political Operational Effects									
Input Variable M_2=m_{22}	x_{11}	x_{12}	x_{13}	x_{21}	x_{22}	x_{23}	x_{24}	x_{31}	x_{32}	x_{33}
0.1	0.38	0.27	0.35	0.24	0.41	0.22	0.13	0.51	0.20	0.29
0.2	0.40	0.24	0.37	0.24	0.40	0.22	0.13	0.51	0.20	0.29
0.4	0.42	0.19	0.40	0.25	0.40	0.23	0.13	0.51	0.21	0.28
0.5	0.43	0.16	0.41	0.25	0.40	0.23	0.13	0.50	0.21	0.28
0.7	0.45	0.12	0.43	0.25	0.39	0.23	0.13	0.50	0.21	0.28
0.8	0.45	0.10	0.44	0.25	0.39	0.23	0.13	0.50	0.22	0.28
0.9	0.46	0.09	0.45	0.25	0.39	0.23	0.13	0.50	0.22	0.28

Table 13

Statistical Analysis of Posterior Belief Distribution in Level 2 Nodes

Simulation Run	**Posterior Belief**		
Input Variable M_2=m_{22}	**Sample Size**	**Mean**	**Std. Deviation**
0.1	10	0.301	0.107
0.2	10	0.300	0.110
0.4	10	0.302	0.116
0.5	10	0.300	0.119
0.7	10	0.299	0.128
0.8	10	0.299	0.131
0.9	10	0.300	0.135

Table 14 shows the posterior belief distribution for the level 3 (*Military Operational Effects*) nodes. Evidence in the input variable $T_3 = t_{31}$ was varied from 0.1 to 0.9 and the posterior probabilities for all the *M* nodes, recorded. The posterior belief for node $M_2 = m_{22}$ and $M_2 = m_{23}$ did not change with variations in the input variable. Table 15 shows the statistical analysis with the mean evidential accrual at 0.29 for all the simulation runs.

Table 14

Belief Update in Level 3 (Military Operational Effects) Nodes

Simulation Run		**Posterior Belief**												
		Military Operational Effects												
Input Variable $T_3=t_{31}$	m_{11}	m_{12}	m_{13}	m_{21}	m_{22}	m_{23}	m_{24}	m_{31}	m_{32}	m_{33}	m_{41}	m_{42}	m_{43}	m_{44}
0.1	0.60	0.25	0.15	0.94	0.02	0.03	0.02	0.47	0.26	0.27	0.44	0.13	0.20	0.23
0.2	0.55	0.28	0.17	0.93	0.02	0.03	0.02	0.47	0.27	0.27	0.43	0.13	0.20	0.25
0.4	0.47	0.33	0.20	0.93	0.02	0.03	0.02	0.46	0.27	0.27	0.41	0.12	0.19	0.28
0.5	0.44	0.35	0.21	0.93	0.02	0.03	0.02	0.46	0.27	0.27	0.41	0.12	0.19	0.29
0.7	0.39	0.38	0.23	0.93	0.02	0.03	0.02	0.45	0.27	0.27	0.40	0.12	0.18	0.30
0.8	0.37	0.39	0.24	0.93	0.02	0.03	0.02	0.45	0.27	0.28	0.39	0.12	0.18	0.31
0.9	0.35	0.40	0.25	0.93	0.02	0.03	0.02	0.45	0.28	0.28	0.39	0.12	0.18	0.32

Table 15

Statistical Analysis of Posterior Belief Distribution in Level 3 nodes

Simulation Run	**Posterior Belief**		
Input Variable $T_3=t_{31}$	**Sample Size**	**Mean**	**Std. Deviation**
0.1	14	0.286	0.246
0.2	14	0.287	0.238
0.4	14	0.286	0.231
0.5	14	0.286	0.229
0.7	14	0.285	0.227
0.8	14	0.286	0.227
0.9	14	0.287	0.226

Table 16 shows the posterior belief distribution for the level 4 (*Tactical Effects*) nodes. Evidence in the input variable $M_4 = m_{41}$ was varied from 0.1 to 0.9 and the posterior probabilities for all the *T* nodes recorded. Table 17 shows the statistical analysis of the posterior belief distribution.

Table 16

Belief Update in Level 4(Tactical Effects) Nodes

Simulation Run	**Posterior Distribution**							
	Tactical Effects							
Input Variable $M_4=m_{41}$	t_{11}	t_{12}	t_{13}	t_{21}	t_{22}	t_{23}	t_{31}	t_{32}
0.1	0.57	0.11	0.32	0.41	0.31	0.28	0.70	0.30
0.2	0.57	0.11	0.32	0.41	0.31	0.28	0.70	0.30
0.4	0.56	0.11	0.32	0.41	0.31	0.29	0.70	0.30
0.5	0.56	0.11	0.32	0.41	0.31	0.29	0.70	0.30
0.7	0.56	0.11	0.33	0.40	0.31	0.29	0.69	0.31
0.8	0.58	0.11	0.30	0.40	0.32	0.28	0.69	0.31
0.9	0.56	0.11	0.32	0.39	0.31	0.28	0.69	0.31

Table 17

Statistical Analysis of Posterior Belief Distribution in Level 4 Nodes

Simulation Run	**Posterior Belief**		
Input Variable $M_4=m_{41}$	**Sample Size**	**Mean**	**Std. Deviation**
0.1	8	0.375	0.172
0.2	8	0.375	0.172
0.4	8	0.375	0.170
0.5	8	0.375	0.170
0.7	8	0.375	0.166
0.8	8	0.374	0.171
0.9	8	0.371	0.167

The posterior probabilities of randomly selected network variables were plotted against the probability of evidence of a select input variable to show the propagation of evidence through the network. For each plot, a random variable from each level of the hierarchical network was selected and its posterior probability plotted for each simulation run.

The results of the evidence propagation (belief revision) for the selected variables in the network are shown and discussed below.

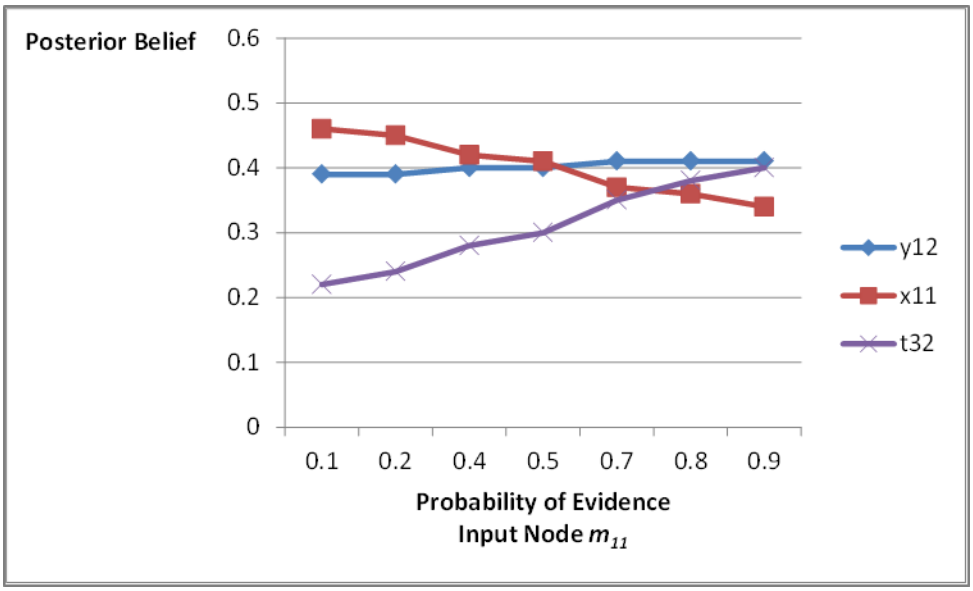

Figure 19. Belief revision in nodes $Y_1 = y_{11}$, $X_1 = x_{11}$ and $T_3 = t_{32}$ after new evidence is introduced in node $M_1 = m_{11}$.

In this sensemaking vignette, the hypothesis variable is $Y_1 = y_{12}$ (*Law and Order Breakdown*) and the informational variables are $X_1 = x_{11}$ (*Sectarian Identity*) and $T_3 = t_{32}$ (*Infrastructure Sabotage*). New evidence was introduced in node $M_1 = m_{11}$, the *Insurgent Security Target Engagement*. Figure 19 shows the posterior probability distribution of nodes after seven simulation runs. We noted the strong positive correlation (r = 0.883) between the evidence of attacks on security targets (*Insurgent Security Target Engagement)* and the targeted action (*Infrastructure Sabotage*). By inspection, as there was more evidence on security target engagement, there was an observable marginal increase in breakdown in law and order, increasing sabotage of infrastructure, and a decreasing trend in sectarian identity. The last node indicated the possibility of no evidence of the groups responsible for sabotage to national infrastructures. The minor variability in the posterior distribution for variable $Y_1 = y_{12}$ (*Law and*

Order Breakdown) would seem to indicate that evidence introduced in the variable node $M_1 = m_{11}$ was non informative, meaning that it did not significantly impact the hypothesis variable Y_1.

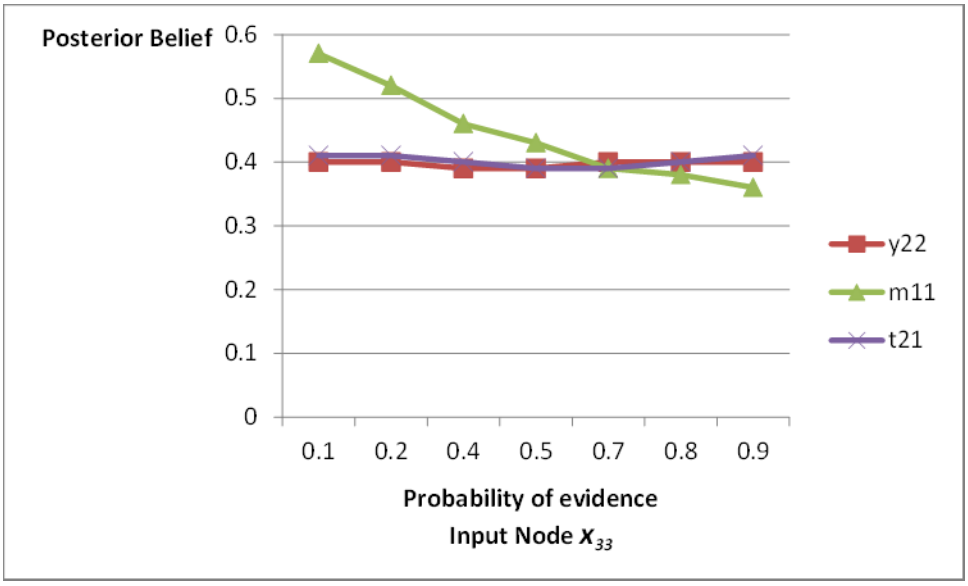

Figure 20. Belief revision in nodes $Y_2 = y_{22}$, $M_1 = m_{11}$ and $T_2 = t_{21}$ after new evidence is introduced in node $X_3 = x_{33}$.

For the second sensemaking vignette, the hypothesis variable was selected as $Y_2 = y_{22}$ (*Insurgent ideology*) and the informational variables were $M_1 = m_{11}$ *(Insurgent Security Target Engagement)* and $T_2 = t_{21}$ (*Insurgent Small Arms Attacks*). New evidence was introduced in node $X_3 = x_{33}$ (*Intelligence Asymmetry*). Figure 20 shows the posterior probability distribution of the variables after 7 simulation runs. We observed that when evidence for the input variable ($X_3 = x_{33}$) was set to 70%, the posterior probabilities for nodes $M_1 = m_{11}$, $Y_2 = y_{22}$, and $T_2 = t_{21}$ converged supporting the hypothesis of an attack on security targets such as police and military leaders using small arms. Increasing the advantage of intelligence asymmetry was non-informative on the selected variables. In addition, it seemed that as the reliability of intelligence increased (x_{33}), security target engagement decreased (r = -0.987). Under the same scenario,

support for the insurgent ideology remained fairly constant. Correlation analysis for the selected variables is shown in appendices B, C, and D.

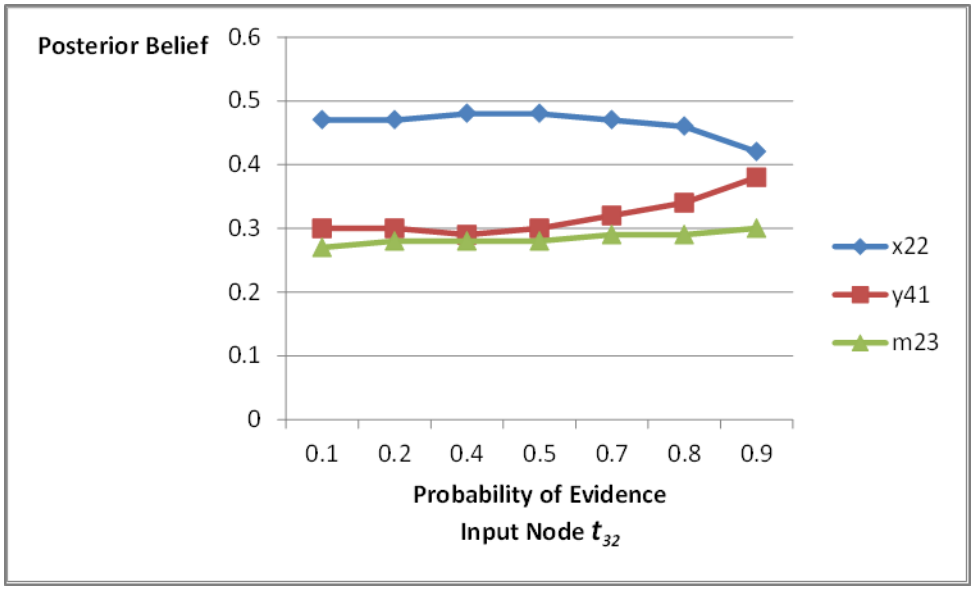

Figure 21. Belief revision in nodes $X_2 = x_{22}$, $Y_4 = y_{41}$ and $M_2 = m_{23}$ after new evidence is introduced in node $T_3 = t_{32}$.

In the last sensemaking vignette, we considered the hypothesis variable $Y_4 = y_{41}$ the insurgent concept of *Nationalism*. For informational variables, we set $X_2 = x_{22}$ (*Insurgent Modular Operations*) and $M_2 = m_{23}$ *(Civilian Shelters)*. New evidence was introduced into variable $T_3 = t_{32}$ (*Arson*). Figure 21 shows the posterior probability distributions after 7 simulation runs. The hypothesis variable $Y_4 = y_{41}$ recorded the highest evidential accrual as new evidence was introduced to $T_3 = t_{32}$. The wider implication of this was to identify most arson attacks and property destruction in that particular area of operations as being carried out by the local population angered or motivated by nationalistic feelings. It was also easy to conclude that the probability distributions for $X_2 = x_{22}$ (*Insurgent Modular Operations*) and $M_2 = m_{23}$ *(Civilian Shelters)* were almost non-informative, or had no effect on whether arson occured or not.

4.3.3 Inference and Courses of Action Analysis

To analyze the potential courses of action, we consider the results from sensemaking vignettes discussed in section 4.3.2.

1. Insurgent Security Target Engagement ($M_1=m_{11}$).

a) By examining the evidence propagation in Figure 19, *P*(*Law and Order Breakdown*) remains relatively stable at 40% with increasing evidence of the adversary targeting of the counterinsurgent security personnel. *P*(*Law and Order Breakdown*) refers to the probability of disrupting counterinsurgent control of the local security situation by limiting their ability for military maneuvers and restricting interaction with the population in stability and support operations. The relative stability of the posterior belief distribution implies that the causal effect of this variable is limited hence it does not carry much weight as a course of action.

b) The probability that the Insurgent Security Target Engagement as a mode of operation is influenced by *Sectarian Identity* ($X_1= x_{11}$) decreases from 50% to 30% as evidence of Insurgent Security Target Engagement increases from 0.1 to 0.9. This implies that operations against security personnel cannot be attributed to a particular group. Infact focusing on the sectarian identity of the group is detrimental to the course of action selection because of the negative correlation. This effect should therefore be discarded.

c) *P*(*Infrastructure Sabotage*| *Insurgent Security Target Engagement*) increases from 20% to 40% as the evidence of Insurgent Security Target Engagement increases from 0.1 to 0.9. Increase in infrastructure sabotage is the most likely tactical effect of the increase in Insurgent Security Target Engagement probably due to the vacuum created by this particular military operational effect. The COA would require the commander to increase protection for critical infrastructure and security targets

2. Insurgent Intelligence Asymmetry ($X_3 = x_{33}$).

a) *P*(*Insurgent Security Target Engagement*| *Intelligence Asymmetry*) decreases from 60% to 35% as evidence for intelligence asymmetry increases from 0.1 to 0.9. Intelligence asymmetry refers to insurgents evolving new tactics that strain or defeat the counterinsurgent Intelligence, Surveillance and Reconnaissance (IS&R) assets. This implies that better intelligence by the insurgent group may not directly influence this mode of operation. The insurgents may in fact be using the intelligence to select soft less protected targets instead of security personnel. The commanders COA is to invest more resources in recruiting intelligence assets to counteract the asymmetry.

b) *P*(*Small Arms Attacks*| *Intelligence Asymmetry*) shows minor variability at 40% similar to the *P*(*Insurgent Ideology*|*intelligence asymmetry*). The tactical effect *Small Arms Attacks* is not significantly influenced by the insurgent intelligence assets. Both these effects are inadmissible as COA.

3. Tactical Effect Arson ($T_3 = t_{32}$).

a) *P*(*Insurgent Modular Operations*| *Arson*) decreases from 50% to 40% (approximately) with increase in evidence of *Arson* as a tactical effect from 0.1 to 0.9. Probability of the insurgent concept of *Nationalism* increases from 30% to 40% while the *P*(*Civilian Shelters*| *Arson*) remains constant at 30%. Most arson attacks and property destruction in a particular area of are carried out by the local population .The commanders' COA should be to consider the tactical effect as a reflection of nationalistic feelings and take appropriate measures in the PMESII spectrum to address this effect. The first and the last probability expressions are inadmissible for COA analysis.

Table 18 gives a summary of the Network's inferential conditions and the supportable courses of action for the evidence propagation results.

Table 18

Summary of Inferential Conditions and Courses of Action for Sample Sensemaking Tasks

Inferential Condition	**Conditional Probability of Evidence (%)**	**Course of Action**	**Results Interpretation**
P(Law and order| Insurgent Security Target Engagement)	40	Not supported	Insufficient evidence to show that insurgent attacks on coalition security targets are the cause of the breakdown in law and order
P(Sectarian Identity|Insurgent Security Target Engagement)	50→30	Not supported	Operations against coalition security targets cannot be attributed to a particular group
P(Infrastructure Sabotage| Insurgent Security Target Engagement)	20→40	Weakly supported	Increase in infrastructure sabotage may be a second order effect of targeting security because of the security gaps created.
P(Insurgent Security Target Engagement| Intelligence Asymmetry)	60→35	Strongly supported	Insurgents may be using the intelligence advantage to select soft targets and avoid the hard security targets
P(Small Arms Attacks| Intelligence Asymmetry)	40	Not admissible	The inferential condition is incompatible with the hypothesis
P(Insurgent ideology| Intelligence Asymmetry)	40	Not admissible	The inferential condition is incompatible with the hypothesis
P(*Insurgent Modular Operations| Arson*)	50→40	Weakly supported	Consider incidents of arson as effects of operational modularity by the insurgents.
P(Nationalism|Arson)	30→40	Strongly supported	Consider the tactical effect *arson* as a reflection of nationalistic feeling by the local population.
P(Civilian Shelters|Arson)	30	Not admissible	The inferential condition is incompatible with the hypothesis

4.3.4 Discussion

The probability distributions for Strategic Effects provide an insight into the end state of the adversary. By performing the inference at this level, an analyst can reasonably draw

conclusions about both the short term and long term objectives or goals of an adversary. For example, considering Figure 19, the correlation between an increase in attacks on the security targets (*Security Target Engagement)* and the targeted action (*Infrastructure Sabotage*) should prompt more defensive resource allocations for critical infrastructures. Additionally, the observable marginal increase in the breakdown in law and order may imply the necessity to deploy more security forces in the affected areas with the resultant effects on manpower requirements.

The probability distributions for Operational Effects (Military and Political) give the analyst inference on the areas of focus that will enable the adversary to achieve their desired Strategic Effects. From the simulation experiment (Figure 20), the strong evidence of small arms attacks (a targeted action) against security targets may require a change in force protection conditions, for example necessitating convoy protection and reduced foot patrols in the affected areas.

Probability distributions for Tactical Effects provide inference into the actual methods, techniques, tactics, and procedures that the adversary may employ to attack selected targets. In Figure 21, the analyst may note the rise in nationalistic or sectarian sentiment and the corresponding increase in cases of arson. Arson as a weapon is more effectively employed by the local population. It can be inferred then, that this tactical effect is being carried out by segments of the population sympathetic to the insurgent goals by linking them to nationalist ideals.

Depending on the complexity of the asymmetric battlespace, the potential range of Tactical Effects is quite extensive and diverse. For purposes of simplicity only a few effects were modelled in the Network. With these probabilities, the analyst could infer the likelihood of a specific attack mode, target type, whether or not the target would be attacked based on its

symbolic or iconic value, whether it would be a single attack or a set of coordinated attacks and the relative location of the attack. It should be emphasized that the importance of these posterior belief distributions lies in the threat levels posed by each variable and not so much the specificity of the actual numbers.

4.4 Model validation

4.4.1 Sensitivity Analysis

Sensitivity analyses were performed on BAMSS to demonstrate its robustness and efficacy in responding to probability changes in information. The purpose of sensitivity analysis in this research is to enable the analyst to see the various effects of high influence variables or events based on their occurrence probabilities on the overall battlefield information. A good discussion on the methodology for sensitivity analysis in Bayesian Networks can be found in Woodberry et al. (2004; 2007). For the BAMSS Network, target nodes representing Tactical Effects were selected and the probability of each of the parent nodes representing the Strategic Effects was varied over the [0,1] probability space by directly introducing evidence while keeping all the other nodes fixed. Changes in the target nodes were then observed and plotted graphically.

Table 19

Probability of New Evidence Introduced in the Network

Simulation Run	**Input evidence**											
	Strategic Effects											
Run #	y_{11}	y_{12}	y_{13}	y_{14}	y_{21}	y_{22}	y_{31}	y_{32}	y_{33}	y_{41}	y_{42}	y_{43}
1	0.2	0.4	0.6	0.1	0.99	0.8	0.2	0.1	0.7	0.5	0.9	0.7
2	0.4	0.5	0.8	0.2	0.7	0.7	0.4	0.4	0.8	0.4	0.1	0.8
3	0.6	0.1	0.5	0.3	0.6	0.6	0.6	0.5	0.9	0.8	0.4	0.2
4	0.8	0.7	0.4	0.4	0.5	0.4	0.8	0.7	0.2	0.3	0.5	0.6
5	0.9	0.8	0.3	0.5	0.4	0.3	0.9	0.9	0.1	0.2	0.3	0.5

Table 20

Posterior Probability of Target Nodes

Simulation Run	**Posterior belief**							
	Tactical Effects							
Run#	t_{11}	t_{12}	t_{13}	t_{21}	t_{22}	t_{23}	t_{31}	t_{32}
1	0.57	0.11	0.32	0.41	0.31	0.29	0.7	0.30
2	0.56	0.09	0.31	0.40	0.30	0.28	0.69	0.30
3	0.54	0.13	0.28	0.42	0.30	0.28	0.72	0.28
4	0.55	0.10	0.25	0.39	0.32	0.26	0.66	0.34
5	0.53	0.08	0.29	0.36	0.33	0.31	0.74	0.26

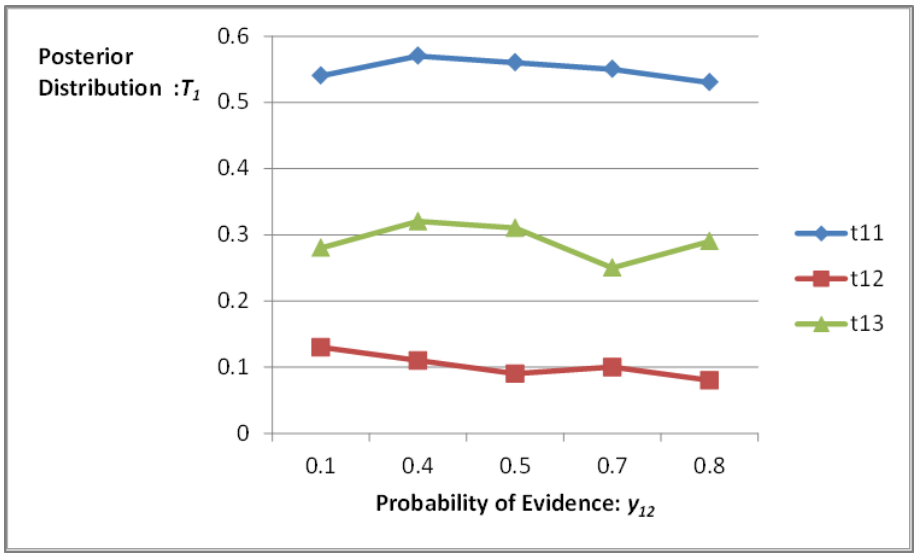

Figure 22. Sensitivity of posterior probabilities for Tactical Effects $T_1 = t_{11}$, $T_1 = t_{12}$ and $T_1 = t_{13}$: Parent node $Y_1 = y_{12}$ is varied.

In the sensitivity analyses of the Tactical Effects node T_1 (t_{11}, t_{12}, *and* t_{13}) it was observed that the BAMSS model did not significantly respond to changes in parent variable $Y_1 = y_{12}$ (*Law and Order Breakdown*). It is simplistic to argue that the *Tactical Effects* (t_{11}, t_{12} *and* t_{13}) have very little influence on the breakdown in the security situation as the sensitivity charts portray. A reasonable explanation would be that the causal linkage is tenuous and needs to be redefined during the development of the network topology. Further examination of the sensitivity analysis

charts indicates that the posterior distributions of the effects t_{11}, t_{12} and t_{13} are mutually exclusive on the effect y_{12}. The posterior probability of $T_1 = t_{11}$ is the highest for every level of input peaking at 58% implying that civilian suicide bombing is the most prevalent tactical effect for the insurgent group. With evidence for law and order breakdown greater than 70%, there is a marked increase in incidents of remotely detonated IEDs ($T_1 = t_{12}$). Correspondingly, there is a drop in the probability of firing RPGs ($T_1 = t_{13}$).

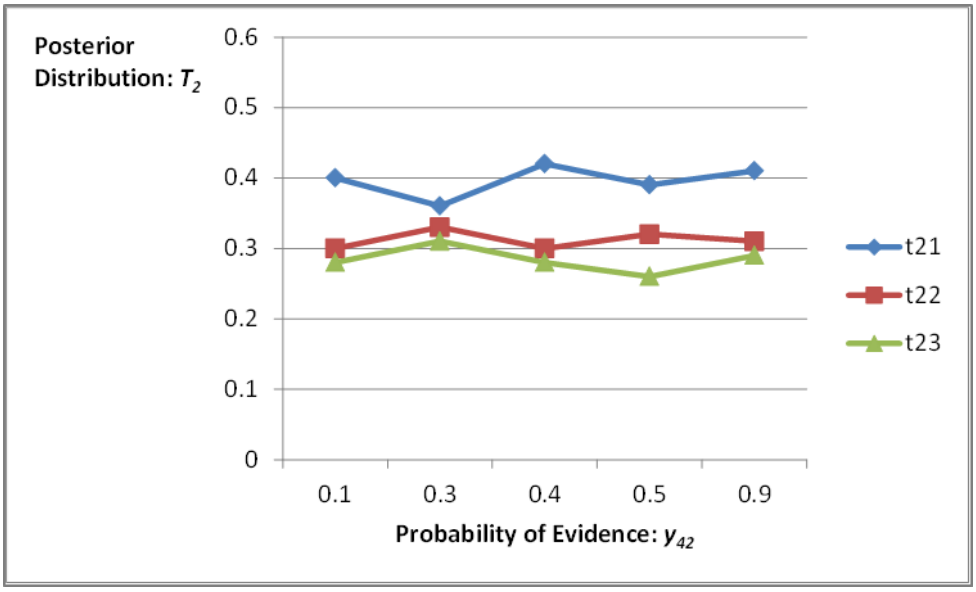

Figure 23. Sensitivity of posterior probabilities for Tactical Effects $T_2 = t_{21}$, $T_2 = t_{22}$ and $T_2 = t_{23}$: Parent node $Y_4 = y_{42}$ is varied.

In the second simulation, a sensitivity analysis was applied to the node $Y_4 = y_{42}$ (*Sectarian Violence*) by varying the input (evidence) to the node, keeping all the other nodes fixed and observing the variations in the posterior distributions of the target nodes. In the results shown in Figure 23, node $T_2 = t_{22}$ *(Coercive Threats)* and $T_2 = t_{23}$ *(Convoy Ambushes)* displayed low sensitivity to the evidence variation while node $T_2 = t_{21}$ *(Small Arms Attacks)* showed an increase in the posterior probabilities accompanied by steeper changes. An examination of the sensitivity charts revealed that the posterior distributions of effects *Coercive Threats* ($T_2 = t_{22}$) and *Convoy*

Ambushes ($T_2 = t_{23}$) co-existed indicating the possibility of some interaction effects. The most significant changes occurred in the effect *Small Arms Attacks* which recorded the highest posterior probability (0.43) for the input variable.

Lastly, sensitivity analysis was done for target nodes $T_2 = t_{23}$ (*Convoy Ambushes*), $T_3 = t_{31}$ (*Infrastructure sabotage*), and $T_3 = t_{32}$ (*Arson*), varying the inputs and keeping all the other nodes fixed. The results were plotted in Figure 24. The posterior distribution for *Infrastructure Sabotage* recorded the highest sensitivity (0.75) to the input variable $Y_2 = y_{22}$ (*Insurgent Ideology*).

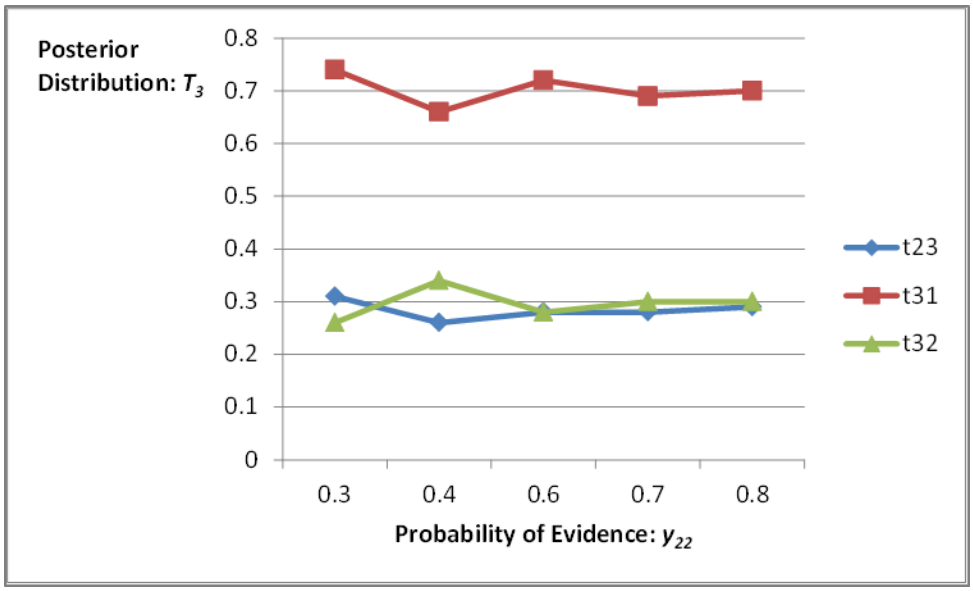

Figure 24. Sensitivity of the posterior probabilities for Tactical Effects node $T_2 = t_{23}$, $T_3 = t_{31}$ and $T_3 = t_{32}$: Parent node $Y_2 = y_{22}$ is varied.

Additional examination of Figure 24 also revealed that the posterior distribution for effects *Infrastructure Sabotage* and *Arson* were mutually exclusive, indicating some interaction effects between the two factors. The response trajectory for t_{23} and t_{31} is the same for changes in y_{22} although the magnitude was different. This could imply strong causal linkages between the two effects. When the input evidence was varied between 0.1 and 0.4, both effects showed a negative

gain response. When the input range increased beyond 0.4, both displayed a positive gradient, peaking at 0.72 for t_{31} and 0.29 for t_{23}.

4.4.2 Inference and Courses of Action Analysis

Sensitivity analysis allows the commander to infer about the levels of uncertainty for the select hypothesis variables. It also allows analysts to perform a what-if analysis to assess the effects of the likelihood of the target variables. In the sensemaking vignettes used in this simulation, we varied the hypothesis nodes and observed the uncertainty concerning the tactical effects nodes. *P*(*Law and Order |High Level Attrition Attacks*) did not show significant variation to changes in input evidence from 0.1 to 0.9. *P*(*Civilian Suicide Bombing*) showed the highest posterior belief accrual peaking at 58% demonstrating that the new evidence on this variable could confirm the most likely posteriori hypothesis ($Y_1 = y_{12}$). On average, *P*(*Remotely Detonated IEDs|Law and Order Breakdown*) was 10% while *P*(*Rocket Propelled Grenades|Law and Order Breakdown*) was 28%. Summarizing from these statistics, the commander should consider variables with posterior distributions that exhibit the greatest variation in response to changes in the input variable for additional analysis.

From Figure 23, *P*(*Small Arms Attacks*| *Sectarian Violence*) recorded the highest aposteriori probability at 44%. A COA analysis by the commander requires a closer examination of the differences between t_{22} (*Coercive Threats*, 30%) and t_{23} (*Convoy Ambushes*, 30%) which seemed to exhibit interaction effects. From Figure 24, *Infrastructure Sabotage* recorded the highest variations and posterior belief at 75% as evidence in the input variable $Y_2 = y_{22}$ (*Insurgent Ideology*) was varied from 0.1 to 0.9. The high degree of sensitivity to the variation in input should prompt the commander to perform additional what-if analyses to identify additional causal factors. Similar analysis could be extended to *P*(*Convoy Ambush*| *Sectarian Violence*) and

P(*Arson*| *Sectarian Violence*), both with average aposteriori probability of 30% since they exhibit mutually exclusive behavior. Table 21 gives a summary of the inferential conditions and the courses of action for the sensitivity analysis results.

Table 21

Summary of Sensitivity Analysis Inferential Conditions and Courses of Action

Inferential Condition	**Conditional Probability of Evidence (%)**	**Course of Action**	**Results Interpretation**
P(Civilian Suicide Bombing|Law and order Breakdown)	55	Strongly supported	Law and order breakdown is likely to occur 55% of the time because of suicide bombing of civilian targets
P(Remotely Detonated IEDs|Law and Order Breakdown	10	Weakly supported	Remotely denotated IEDs are not a major contributing factor to the law and order breakdown (only 10% of the time)
P(Rocket Propelled Grenades|Law and Order Breakdown	28	Weakly supported	Rocket Propelled Grenades is not a significant contributory factor to law and order breakdown
P(Small Arms Attacks| Sectarian Violence)	44	Strongly supported	Evidence supports the increase in the use of small arms as a targeted action in sectarian violence
P(Coercive Threats| Sectarian Violence	30	Additional analysis	No conclusive evidence to support this COA. Additional analysis needed.
P(Convoy Ambushes|Sectarian Violence)	30	Additional analysis	No conclusive evidence to support this COA. Further analysis is needed to isolate the causal factors
P(*Infrastructure sabotage|Sectarian Ideology*)	75	Strongly supported	Strong evidence to show that the ideology of the insurgents is linked to attacks on certain critical infrastructure.
P(Convoy Ambush|Sectarian Ideology)	30	Additional analysis	No conclusive evidence to support this COA. Further analysis is needed to isolate the causal factors
P(Arson |Sectarian Ideology)	30	Additional analysis	No conclusive evidence to support this COA. Further analysis is needed to isolate the causal factors

4.5 Chapter Summary

This chapter presented experiments and validations of the BAMSS model using a case study in asymmetric warfare. Some examples on using BAMSS for sensemaking in the context of the simulation experiment were presented. We developed and analyzed different vignettes representative of the asymmetric warfare domain. In the first vignette, the sensemaking task required an analyst to create a hypothesis variable $Y_1 = y_{12}$ where y_{12} represented Law *and Order Breakdown*. New evidence was then introduced in the node $M_1 = m_{11}$, where m_{11} was an indicator for the *Security Target Engagement* by varying the input data from 0.1 to 0.9. Results from seven simulation runs were then analyzed for select informational variables $X_1 = x_{11}$ (*Sectarian Identity*) and $T_3 = t_{32}$ (*Infrastructure Sabotage*).

By examining the evidence propagation in the first vignette, the probability of (*Law and Order Breakdown*) remained relatively stable at 40% with increasing evidence of adversary targeting of the counterinsurgent security personnel. The relative stability of the posterior belief distribution implied that the causal effect of this variable was limited hence did not carry much weight as a COA. The probability that the Insurgent Security Target Engagement as a mode of operation as influenced by *Sectarian Identity* ($X_1 = x_{11}$) decreased from 50% to 30% implying that operations against security personnel could not be attributed to a particular group. In fact, focusing on the sectarian identity of the group could be detrimental to the course of action selection because of the negative correlation and this effect ought to be discarded. Probability of (*Infrastructure Sabotage| Insurgent Security Target Engagement*) increased from 20% to 40%. Increase in infrastructure sabotage was the most likely tactical effect of the increase in Insurgent Security Target Engagement probably due to the vacuum created by this particular military

operational effect. This COA would require the commander to increase protection for critical infrastructure and security targets.

For the second vignette, the hypothesis for the sensemaking task was changed to $Y_2 = y_{22}$ (*Insurgent ideology*). Evidence was introduced in node $X_3 = x_{33}$ (*Intelligence Asymmetry*) and the posterior probabilities for informational variables $M_1 = m_{11}$ *(Security Target Engagement)* and $T_2 = t_{21}$ (*Small Arms Attacks*) were computed. Probability of (*Insurgent Security Target Engagement*| *Intelligence Asymmetry*) decreased from 60% to 35% as evidence for intelligence asymmetry increased from 0.1 to 0.9. This implied better intelligence by the insurgent group did not directly influence this mode of operation. The commander's COA would be to invest more resources in recruiting intelligence assets to counteract the asymmetry. Probability of (*Small Arms Attacks*| *Intelligence Asymmetry*) showed minor variability at 40% similar to the *P*(*Insurgent Ideology*|*intelligence asymmetry*). The tactical effect *Small Arms Attacks* was not significantly influenced by the insurgent intelligence assets. Both these effects were inadmissible as COA.

In the last sensemaking vignette, we considered the hypothesis variable $Y_4 = y_{41}$, the insurgent concept of *Nationalism*. For informational variables we set $X_2 = x_{22}$ (*Insurgent Modular Operations*) and $M_2 = m_{23}$ *(Civilian Shelters)*. New evidence was introduced into variable $T_3 = t_{32}$ (*Arson*). The probability of (*Insurgent Modular Operations*| *Arson*) decreased from 50% to 40% (approximately) with an increase in evidence of *Arson* as a tactical effect from 0.1 to 0.9. The probability of *Nationalism* increased from 30% to 40% while the *P*(*Civilian Shelters*| *Arson*) remained constant at 30%.The commanders' COA would then be to consider the tactical effect as a reflection of nationalistic feelings and take appropriate measures in the PMESII spectrum to

address this effect. *P*(*Insurgent Modular Operations*| *Arson*) and P(*Civilian Shelters*| *Arson*) were not admissible for COA analysis.

A sensitivity analysis was performed on the model output for the second sensemaking problem using three simulation experiments. The first experiment entailed the selection of target nodes representing Tactical Effects variable T_1 (t_{11}, t_{12}, *and* t_{13}). The probability of (*Law and Order* |*High Level Attrition Attacks*) did not show significant variation to changes in input evidence from 0.1 to 0.9. *P*(*Civilian Suicide Bombing*) showed the highest posterior belief accrual peaking at 58% demonstrating that the new evidence on this variable could confirm the most likely aposteriori hypothesis ($Y_1 = y_{12}$). On average, *P* (*Remotely Detonated IEDs*|*Law and Order Breakdown*) was 10% while *P*(*Rocket Propelled Grenades*|*Law and Order Breakdown*) was 28%. The commander would consider the variable Civilian Suicide Bombing for additional analysis since it exhibited the greatest variation in response to changes in the input variable.

In the second simulation, a sensitivity analysis was performed on variable T_2 (t_{21}, t_{22}, t_{23}), varying the input to node $Y_4 = y_{42}$ (*Sectarian Violence*). *P*(*Small Arms Attacks*| *Sectarian Violence*) recorded the highest aposteriori probability at 44%. A COA analysis by the commander would require a closer examination of the differences between t_{22} (*Coercive Threats*, 30%) and t_{23} (*Convoy Ambushes*, 30%) which seemed to exhibit interaction effects. Lastly, sensitivity analysis was done for target nodes $T_2 = t_{23}$ (*Convoy Ambushes*), $T_3 = t_{31}$ (*Infrastructure sabotage*), and $T_3 = t_{32}$ (*Arson*). *Infrastructure Sabotage* recorded the highest variations and posterior belief at 75% as evidence in the input variable $Y_2 = y_{22}$ (*Insurgent Ideology*) was varied from 0.1 to 0.9. Additional analysis could be extended to *P*(*Convoy Ambush*| *Sectarian Violence*) and *P*(*Arson*| *Sectarian Violence*) both with average aposteriori probability of 30% since they exhibited mutually exclusive behavior.

CHAPTER 5

Optimizing Abductive Inference in BAMSS with Genetic Algorithm

5.1 Genetic Algorithms

The Bayesian Clustering Algorithm (Lauritzen &Spiegelhalter, 1988) described in Chapter 4 has limitations in terms of resource utilization and the bounded search space. The BAMSS model overcomes these limitations by using the GA, thereby increasing its efficiency, scalability and robustness. A GA is a variable search procedure that is based on the principle of evolution by natural selection (Goldberg, 1989). The procedure works by evolving sets of variables (*Chromosomes*) that fit certain criteria from an initial random population via cycles of differential replication, recombination and mutation of the fittest chromosomes.

GAs have several advantages over other methods. Conventional search methods are not robust, as discussed in Goldberg (1989). GAs improve over the local scope of traditional methods by searching in parallel many subspaces in multidimensional spaces with complex topologies. Under time constraints, enumerative approaches are often not feasible or too slow. Goldberg notes that GAs differ from other methods in the following ways: 1) GAs work with a coding of the parameter set, not the parameters themselves; 2) GAs search from a population of points, not from a single point; 3) GAs use an objective function without any auxiliary knowledge; and 4) GAs use probabilistic transition rules, not deterministic rules. A population representing candidate solutions is evaluated for fitness using a fitness function. Genetic operators such as crossover and mutation then create a new population from the old population. The probability of transfer of the genetic material of an individual is a function of its fitness.

Previous research on the use of GAs for BN inference has been done by Rojas-Guzman and Kramer (1993, 1996); Gelsema (1995); Lin et al., (1990); Santos, Shimony and Williams (1996); and Welch (1996). de Campos et al., (1999, 2002) did extensive research on partial abductive inference in Bayesian Belief Networks using GAs. By focusing only on a subset of network variables (partial abduction) known as the *explanation set*, de Campos et al. were able to solve the *maximum a posteriori* (MAP) probability problem using approximate GA algorithms. Mengshoel (1998) used GA in function optimization (finding the *most probable explanation*) focusing particularly on the role of niching and scaling to solve the problems of premature convergence and diversity preserving. This was followed by research in using GAs with probabilistic crowding replacement for fast and efficient search to perform Network inference (1999). A good review of evolutionary algorithms in Bayesian network learning and inference tasks is provided by Larranaga, et al., (2013)

5.1.1 Representation

In GAs, a solution or individual is conventionally represented by a string of integers or chromosomes which encodes the individual genotype. Each position or gene in the string corresponds to one variable in the belief network. Each gene can take a number of values (alleles) from a finite discrete alphabet which may be different for each gene and corresponds to the number of discrete values that the variable can assume in the Belief Network.

GAs require the existence of a metric in the space of possible solutions. In this case, a clearly defined metric is the absolute probability of each possible solution (or point in the search space or system state in the BN space).Within the Belief Network framework, performing this calculation is straightforward for the special case in which all the nodes have been instantiated. The fitness metric corresponds to the individual phenotype and is a product with one factor for

each node. Each factor is either a prior probability for parent nodes or a conditional probability (for child nodes). These probabilities are efficiently retrieved using multidimensional arrays. A phenotype (fitness metric or probability) corresponds to each genotype (set of variable-value assignments).

5.1.2 Parameters

BAMSS requires the specification of two GA parameters; the probability of *Crossover* and the probability of *Mutation*. Crossover (reproduction) is the GA operator that enables reproduction between two parents to create new members of the population from the previous generation. Two parents can create one or two children in the case where a choice is necessary to avoid losing useful new individuals in the resultant population. The genotype of each new individual is made up by combining the genotypes of the parents. In traditional GAs, where two parents are copied into two children, two positions are randomly chosen in the new strings and the genes located between the two positions are interchanged.

The mutation operator introduces random changes in one allele of the genotype of one individual. The mutation frequency is usually very low and its goal is to maintain diversity in the population to avoid premature convergence. A BN can be used for predictive reasoning or diagnostic abductive inference in which case, any arbitrary subset of variables may be instantiated during the inference process. The instantiated values are not changed by the mutation to guarantee that all individuals retain legal and meaningful genotypes.

5.1.3 Fitness Function

The Bayesian Network Inference Algorithm computes the probability density over a variable *H* given new evidence *D* formally denoted as *P(H|D)*.The two abductive inference tasks in the BN are *belief updating* and *belief revision*. *Belief updating* computes the posterior belief

over a hypothesis node H given instantiated evidence nodes $D_1, D_2 \ldots D_m$ as identified by $P(H|D_1=d_1,D_2=d_2,\ldots D_m=d_m)$. *Belief revision* computes the posterior belief over a set of hypothesis nodes $H_1,H_2..H_k$ given the evidence nodes $D_1, D_2 \ldots D_m$, more formally written as $P(H_1,H_2 \ldots H_k|D_1=d_1,D_2=d_2,\ldots D_m=d_m)$. For the case where all nodes are instantiated, belief revision is known as computing an explanation and the task of computing the Most Probable Explanation (MPE) or the k Most Probable Explanations (kMPE) is referred to as abductive inference in the model. The following definitions related to the BAMSS model are made:

Definition 1

The posterior probability $P(h|D)$ of a network variable as defined by equation(1) in Chapter 3 is computed as follows:

$$P(h \mid D) = \frac{P(D \mid h)P(h)}{P(D)}$$

The fitness function to be used then is based on the posterior probability $P(h|D)$ of the Network as defined above. Let all the explanations be ordered according to their posterior probability:

$$P(h_1|d) \geq P(h_2|d) \geq P(h_3|d) \geq \ldots\ldots P(h_n|d) \qquad (16)$$

Here, the most probable explanation (MPE) is h_1. The k most probable explanations (k-*MPE*) are $h_1, h_2, \ldots h_k\ (k \leq n)$. The experimental population consists of a set of explanations or chromosomes $\{ h_1, h_2, \ldots h_n\}$ where n is the population size. The objective is to obtain the posterior probabilities of a set of variables $(X_1,X_2,..X_n)$ that can be regarded as influencing a particular effect, for example, the probability that insurgents adopt certain Tactical effects given that we can infer their *Sectarian Identity* and the *Fundamentalist Ideology* they adhere to. The overall joint probability of the set of variables is given by the product

$$P(X_1, X_2, \ldots, X_n) = \prod_{i=1}^{n} P(x_i \mid \prod_{X_i}) \qquad (17)$$

The fitness function is a simple look-up function that computes the overall joint probability of the network (known as the network solution) for different combinations of variables and returns MPE for the Network based upon a user selected fitness value. Formally, the fitness function for BAMSS model can be represented as:

$$fitness(X_i) = \arg\max_{Xi} \prod_{i=1}^{n} P(x_i \mid \prod_{X_i}) \tag{18}$$

where X_i is the set of all the variables in the network and the right hand side returns the maximum argument of the product term. Owing to the ability of the GA to undertake parallel search, multiple network solutions compliant with the fitness value (*k*MPE) may be generated and its left to the analyst to evaluate the probability profile of each of the solutions for the best COA selection. The combination of variables in the network solution (MPE) constitutes the phenotype of interest to the analyst.

Definition 2

Since a BN is a directed acyclic graph, a topological sort can be used to linearly order the nodes in a BN and a GA string (chromosome) is organized according to the linear order. Let $X_j = x_j$ be the assignment to node *j* in the BN. If all the nodes are binary, i.e $x_j \in \{0, 1\}$ then the one to one mapping from the random variable X_j to the chromosome a_j in position *j* is fully defined by the vector a_j where a_j is a string of zeros and ones for example [10011011101]. In the case of the BAMSS model, the random variables have cardinality greater than 2 i.e, $x_j \in \{0,1,2..n\}$ where *n* represents the *nth* state of the higher cardinality alphabet hence, more appropriately we define the vector string a_j as a string of real valued integers. [0112211220102112] is an example of a string where the *nth* state of alphabet is represented by the integer 2 in a string of cardinality 3.

5.2 Implementing the Genetic Algorithm in BAMSS

A schematic representation of the information flow and processing in GA is shown in Figure 25.

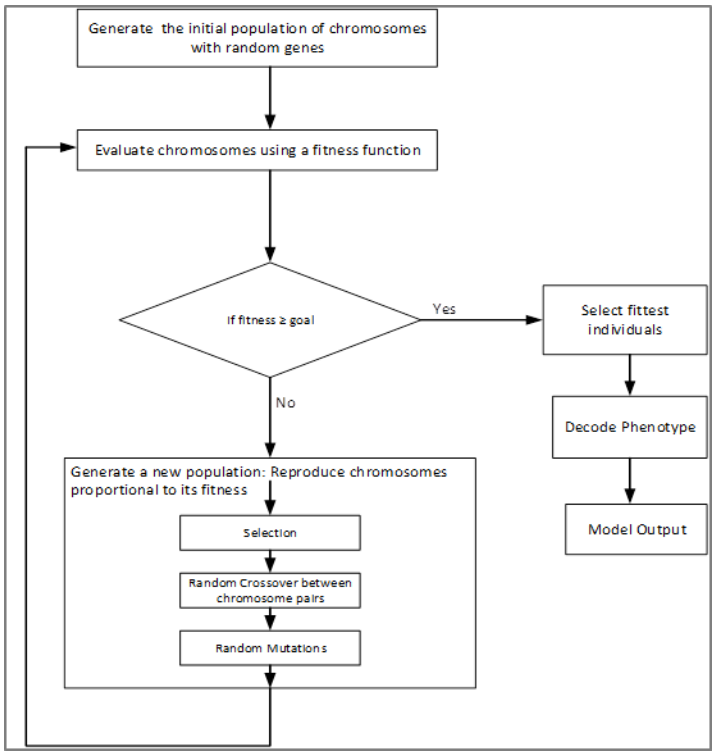

Figure 25. The canonical GA procedure as applied to the BAMSS model.

The initial step involves a generation of a population of chromosomes (random variable sets). Each chromosome in the population is then evaluated according to a user selected fitness value. If the chromosome has a score higher than a set threshold value (τ^*), this chromosome is selected and the procedure stops. The chromosome is then decoded for its real value (phenotype) and output by the model as the MPE for the set of random variables.

If the chromosome has a lower score than τ^*, the chromosomes are reproduced proportional to their fitness to create a new population. Chromosomes with a higher fitness score will reproduce more numerous offspring. In the crossover stage, the genotype of the replicated parents is combined by randomly selecting two parent chromosomes and swapping their genetic

information. In this way, two new chromosomes are created adding to the range of possible solutions to the Network. To avoid premature convergence of the solutions, mutations are introduced in the chromosomes randomly to diversify the gene pool. Mutation also ensures that the entire state space is searched. The newly created population is then re-evaluated again using the fitness function and the fittest individuals selected. This cycle (also called a generation) is repeated until a predefined threshold is met.

The pseudo code for the canonical genetic algorithm or Simple Genetic Algorithm (Goldberg, 1989; Mengshoel, 1999) is described below:

```
gen :=1
randomize (oldpop)
repeat
      j:=1
      repeat
            mate1 := select(oldpop)
            mate2 :=select(oldpop)
            crossover(oldpop[mate1].chrom.oldpop[mate2].chrom ,
                  newpop[j].chrom,newpop[j+1].chrom,
                  P(Crossover))
            newpop[j].chrom:= mutate(newpop[j].chrom, P(Mutation)
            newpop[j+1].chrom:= mutate(newpop[j].chrom, P(Mutation)
            newpop[j].fitness:= objfunc(decode(newpop[j].chrom))
            newpop[j+1].fitness:= objfunc(decode(newpop[j+1].chrom))
            j:=j+1
        until j > n
        oldpop := newpop
        gen := gen +1
 until gen>maxgen
```

Figure 26. A simple genetic algorithm (Mengshoel, 1999).

Note that *maxgen* is the iteration threshold and the outermost loop is repeated until this threshold is reached. For each generation, the GA functions *select*, *crossover*, *mutate* and the objective function *objfunc* are iterated. *select(pop)* selects an individual from the input population. *P(crossover)* takes chromosomes $chrom_1$ and $chrom_2$ as input and creates new chromosomes as output by crossing over with a probability *P(crossover)*. *P(Mutation)* mutates

each allele in the chromosome (*chrom*) and then returns a mutated chromosome. *Objfunc* refers to the objective function which is used for computing the fitness of the two new individuals. *Decode* maps the genotype to a phenotype (real value) of the chromosome. The fitness function *objfunc* takes a value from the phenotypic space and assigns it a fitness value.

5.3 BAMSS Analysis with GA

5.3.1 Data Encoding and Input for Simulation

Chromosomes in a BBN network are represented using real integers instead of binary encodings. The reason for selecting higher order cardinality alphabet is because of: 1) The complex nature of the problem which makes binary encodings infeasible and 2) Research by Antonise (1989), Bhattacharyya and Koehler (1994), and Davis (1991) which shows that higher cardinality alphabets provide better results. We used the *BAMSS COA Analysis* network developed in the GeNIe Network module to evaluate the model GA. The node probabilities were obtained by querying the Bayesian Inference module while belief updating was done using the Bayesian Clustering Algorithm implementation. Discrete states of each node in the network corresponding to the states of a selected random variable and their corresponding prior and conditional probabilities were encoded as shown in Tables 22-25.

Since Level 1 nodes are parent nodes, Table 22 gives the marginal distribution of all the variables that constitute that level.

Table 22

Level 1 Nodes Chromosome Encoding

Y_1	$P(Y_1)$	Y_2	$P(Y_2)$	Y_3	$P(Y_3)$	Y_4	$P(Y_4)$
1	0.5	1	0.6	1	0.3	1	0.2
2	0.3	2	0.4	2	0.3	2	0.6
3	0.2			3	0.4	3	0.2
4	0.1						

Tables 23-25 give the conditional distribution of the rest of the informational variables in the Network. Since all Level 2, Level 3 and Level 4 variables are child nodes, the conditional dependencies must be encoded as shown. For ease of computation, it is assumed that all the variables have non-zero conditional probabilities and non-zero mutual information.

Table 23

Level 2 Nodes Sample Chromosome Encoding

X_1	Y_1	Y_2	Y_3	Y_4	$P(X_1 \mid Y_1Y_2Y_3Y_4)$	X_2	Y_1	Y_2	Y_3	Y_4	$P(X_2 \mid Y_1Y_2Y_3Y_4)$
1	1	1	1	1	0.45	1	1	1	1	1	0.50
2	1	1	1	1	0.30	2	1	1	1	1	0.80
3	1	1	1	1	0.62	3	1	1	1	1	0.60
1	2	1	1	1	0.80	4	1	1	1	1	0.35
2	2	1	1	1	0.78	1	2	1	1	1	0.80
3	2	1	1	1	0.19	2	2	1	1	1	0.70
1	3	1	1	1	0.55	3	2	1	1	1	0.37
2	3	1	1	1	0.45	4	2	1	1	1	0.23
3	3	1	1	1	0.88	1	3	1	1	1	0.40
1	4	1	1	1	0.34	2	3	1	1	1	0.20
2	4	1	1	1	0.70	3	3	1	1	1	0.92

Table 24

Level 3 Nodes Sample Chromosome Encoding

M_1	X_1	X_2	X_3	$P(M_1 \mid X_1X_2X_3)$	M_2	X_1	X_2	X_3	$P(M_2 \mid X_1X_2X_3)$
1	1	1	1	0.60	1	1	1	1	0.22
2	1	1	1	0.40	2	1	1	1	0.43
3	1	1	1	0.54	3	1	1	1	0.60
1	2	1	1	0.90	1	2	1	1	0.50
2	2	1	1	0.62	2	2	1	1	0.88
3	2	1	1	0.10	3	2	1	1	0.15
1	3	1	1	0.33	1	3	1	1	0.23
2	3	1	1	0.85	2	3	1	1	0.54
3	3	1	1	0.70	3	3	1	1	0.34
1	1	2	1	0.30	1	1	2	1	0.65
2	1	2	1	0.85	2	1	2	1	0.45

Table 25

Level 4 Nodes Sample Chromosome Encoding

T_1	M_1	M_2	M_3	M_4	$(P(T_1 \mid M_1M_2M_3M_4)$	T_2	M_1	M_2	M_3	M_4	$P(T_2 \mid M_1M_2M_3M_4)$
1	1	1	1	1	0.45	1	1	1	1	1	0.20
2	1	1	1	1	0.30	2	1	1	1	1	0.67
3	1	1	1	1	0.62	3	1	1	1	1	0.32
1	2	1	1	1	0.80	1	2	1	1	1	0.89
2	2	1	1	1	0.78	2	2	1	1	1	0.45
3	2	1	1	1	0.19	3	2	1	1	1	0.60
1	3	1	1	1	0.55	1	3	1	1	1	0.55
2	3	1	1	1	0.45	2	3	1	1	1	0.70
3	3	1	1	1	0.88	3	3	1	1	1	0.10
1	1	2	1	1	0.34	1	1	2	1	1	0.50
2	1	2	1	1	0.70	2	1	2	1	1	0.45

The complete state of the Network can thus be represented by a chromosome of 50 genes, each gene representing a network variable. The chromosome is a configuration of all the network variables, represented as a string of integers and it encapsulates the conditional probability of a variable in a given state. Considering the rows in Tables 22-25, a sample population of five chromosomes representing the complete state of the network is represented as follows:

$$\begin{bmatrix} \boldsymbol{Y_1} & \boldsymbol{Y_2} & \boldsymbol{Y_3} & \boldsymbol{Y_4} & \boldsymbol{X_1} & \boldsymbol{X_2} & \boldsymbol{X_3} & \boldsymbol{M_1} & \boldsymbol{M_2} & \boldsymbol{M_3} & \boldsymbol{M_4} & \boldsymbol{T_1} & \boldsymbol{T_2} & \boldsymbol{T_3} \\ 1111 & 11111 & 11111 & 11111 & 1111 & 1111 & 1111 & 1111 & 11111 & 11111 & 11111 \\ 2111 & 21111 & 21111 & 21111 & 2111 & 2111 & 2111 & 2111 & 21111 & 21111 & 21111 \\ 3111 & 31111 & 31111 & 31111 & 3111 & 3111 & 3111 & 3111 & 31111 & 31111 & 12111 \\ 4111 & 12111 & 41111 & 12111 & 1211 & 4111 & 1211 & 4111 & 12111 & 12111 & 22111 \\ 1211 & 22111 & 12111 & 22111 & 2211 & 1211 & 2211 & 1211 & 22111 & 22111 & 13111 \end{bmatrix}$$

Note that the gene position in the chromosome array represents the actual order of the variable nodes in the topology of the network. The phenotype for these chromosomes is decoded to the following linearly ordered array:

$$\begin{bmatrix} \boldsymbol{Y_1} & \boldsymbol{Y_2} & \boldsymbol{Y_3} & \boldsymbol{Y_4} & \boldsymbol{X_1} & \boldsymbol{X_2} & \boldsymbol{X_3} & \boldsymbol{M_1} & \boldsymbol{M_2} & \boldsymbol{M_3} & \boldsymbol{M_4} & \boldsymbol{T_1} & \boldsymbol{T_2} & \boldsymbol{T_3} \\ 0.5 & 0.6 & 0.3 & 0.2 & 0.45 & 0.5 & 0.8 & 0.6 & 0.22 & 0.47 & 0.75 & 0.5 & 0.2 & 0.8 \\ 0.3 & 0.6 & 0.3 & 0.2 & 0.3 & 0.8 & 0.6 & 0.4 & 0.43 & 0.82 & 0.62 & 0.8 & 0.67 & 0.15 \\ 0.2 & 0.6 & 0.3 & 0.2 & 0.62 & 0.8 & 0.5 & 0.54 & 0.6 & 0.23 & 0.9 & 0.33 & 0.32 & 0.88 \\ 0.1 & 0.6 & 0.3 & 0.2 & 0.8 & 0.35 & 0.6 & 0.9 & 0.5 & 0.7 & 0.4 & 0.45 & 0.89 & 0.55 \\ 0.5 & 0.4 & 0.3 & 0.2 & 0.78 & 0.8 & 0.6 & 0.62 & 0.88 & 0.2 & 0.7 & 0.65 & 0.45 & 0.8 \end{bmatrix}$$

Considering only the first two levels of the model with seven nodes (Level 1 and Level 2 nodes) the search space comprises of $\{(Y_1)^4 * (Y_2)^2 * (Y_3)^3 * (Y_4)^3 * (X_1)^3 * (X_2)^4 * (X_3)^3\} = 2592$ points .With each gene having two or more discrete values (alleles) the search space for all possible combinations of variables in the Network is exponentially large making abductive inference in such a network to be considered an NP-hard problem (Shimony, 1994).

The GA used in the BAMSS model development was implemented in Java using the JAGA API. JAGA runs on Java version 1.4 and higher and is freely available under the GNU General Public License Version 2.0. After downloading the appropriate libraries, an executable .jar file was developed in the NetBeans IDE and modified for the fitness function and other problem-specific GA operators. For the standalone GA module, the original version was developed in the Python 2.7 programming language in order to better capture the graphical results of the GA. The graphical library used is *Pyside*, a python version of QT4. The *jpype* library was used to interface with the *smile.jar* library in the main BAMSS model. The plot graphing was done using *pyqtgraph*, which required *NumPy* and *SciPy* as dependencies. All development was done in the IDE.

5.3.2 Experimental Evaluation

The BAMSS Network described in Chapter 4 is used to evaluate the model using the BAMSS- GA. The Network consists of 14 variables each of which has 2, 3 or 4 different states. The pseudo code for the BAMSS GA algorithm is described in Figure 27 and a sample Java-based implementation algorithm is given in Figure 28.

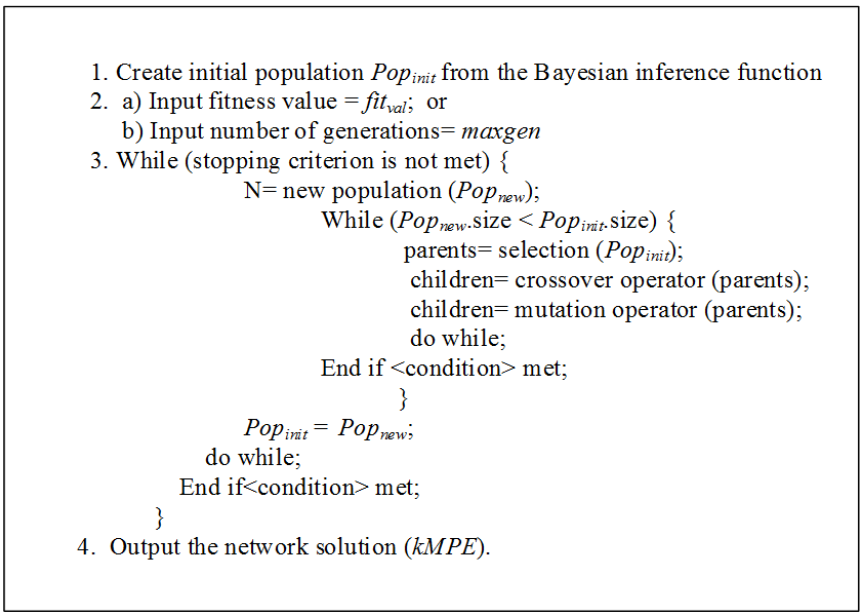

Figure 27. BAMSS genetic algorithm.

```
//  GA algorithm work

        Configuration gaConfig=new DefaultConfiguration();
          DefaultConfiguration.reset();
          // Adding mutation and crossover
          GeneticOperator gcr=new CrossoverOperator(gaConfig,pcr, true);
          GeneticOperator gmr=new GaussianMutationOperator(gaConfig,pmt);
          gaConfig.addGeneticOperator(gcr);
          gaConfig.addGeneticOperator(gmr);

        IChromosome chromosome=new Chromosome(gaConfig,new DoubleGene(gaConfig,0,
1),14);
        gaConfig.setSampleChromosome(chromosome);
        gaConfig.setPopulationSize(populationSize);
        gaConfig.setFitnessFunction(new ByesianNetworkFitness(fitnessValue));

        Population pop=new Population(gaConfig, populationSize);
        for(int c=0;c<populationSize;c++)
        {
        Gene[]gene=chromosome.getGenes();
         Gene[]newGene=new Gene[gene.length];
         for(int j=0;j<gene.length;j++)
         {
            newGene[j]=gene[j].newGene();
            newGene[j].setAllele(cbMatrix[c][j]);
         }
         IChromosome chrom = new Chromosome(gaConfig);
         chrom.setGenes(newGene);
         pop.addChromosome(chrom);
        }
       logger.info("Gene initialisation completed");
        // Now we need to construct the Genotype.
          Genotype genotype=new Genotype(gaConfig, pop);
```

Figure 28. Sample Java code for BAMSS-GA implementation.

The termination condition is a user-defined fitness value which specifies the probability of the Network solutions that we are interested in or the maximum number of generations that is set for algorithmic computations. Any solution that does not meet the stopping criterion is discarded by the model and does not appear in the output results. For BAMSS simulation experiments, a fitness value of 70% was used for all the experimental configurations. A common problem with GA is that it does not provide a window into the piecewise examination of the output. This makes the interpretation of the results challenging. To overcome this challenge, a decode function was added to convert the genotype to the phenotype for output interpretation. . This is shown in the algorithm in Figure 29.

```
public class GAResult
{
   private int generation;
   private double fitnessValue;
   private String geneCombination;
   public int getGeneration() {
      return generation;
   }
   public void setGeneration(int generation) {
      this.generation = generation;
   }
   public double getFitnessValue() {
      return fitnessValue;
   }
   public void setFitnessValue(double
fitnessValue) {
      this.fitnessValue = fitnessValue;
   }
   public String getGeneCombination() {
      return geneCombination;
   }
   public void setGeneCombination(String
geneCombination) {
      this.geneCombination = geneCombination;
  }

}
```

Figure 29. Sample Java code for decoding the BAMSS-GA genotype.

5.3.3 Simulation Results

Three simulation runs were performed, varying the algorithm parameters for each run. For each simulation, the GA parameters were set as shown in Table 26.

Table 26

GA Parameters for Three Simulation Experiments

Experiment 1	Experiment 2	Experiment 3
Initial Population= 200 *Probability of Transition=50%* *Probability of Crossover=49%* *Probability of Mutation =1%* *Stop Criterion = 20* *Desired number of results=20*	*Initial Population= 200* *Probability of Transition=50%* *Probability of Crossover=40%* *Probability of Mutation =10%* *Stop Criterion = 20* *Desired number of results=20*	*Initial Population= 200* *Probability of Transition=50%* *Probability of Crossover=35%* *Probability of Mutation =15%* *Stop Criterion = 20* *Desired number of results=20*

The initial population was entirely randomized for a faster convergence to a good solution. Following de Campos et al. (1999) we added a parameter for probability of transition (selection) to ensure the diversity of the population and avoid convergence to local optima. By setting the probability to 50%, we ensured that the best 50% of the chromosomes were carried over from the initial population to the population at the next generation. The probability of crossover ensured that 49% of the new population is selected by crossover. The choice of the parent to be selected for crossover was proportional to the fitness of that parent. The final 1% of the new population was selected by mutation. The chromosomes to be mutated were selected randomly from the initial population, mutated with a given probability of mutation and copied into the new population.

The algorithm terminated when the stopping criterion (20 generations) had been reached. The desired number of network solutions (k) was set to 20 so that the model would output 20 *MPEs* for the network. Figure 30 shows the interface for the GA standalone module of BAMSS with the parameter input menu displayed.

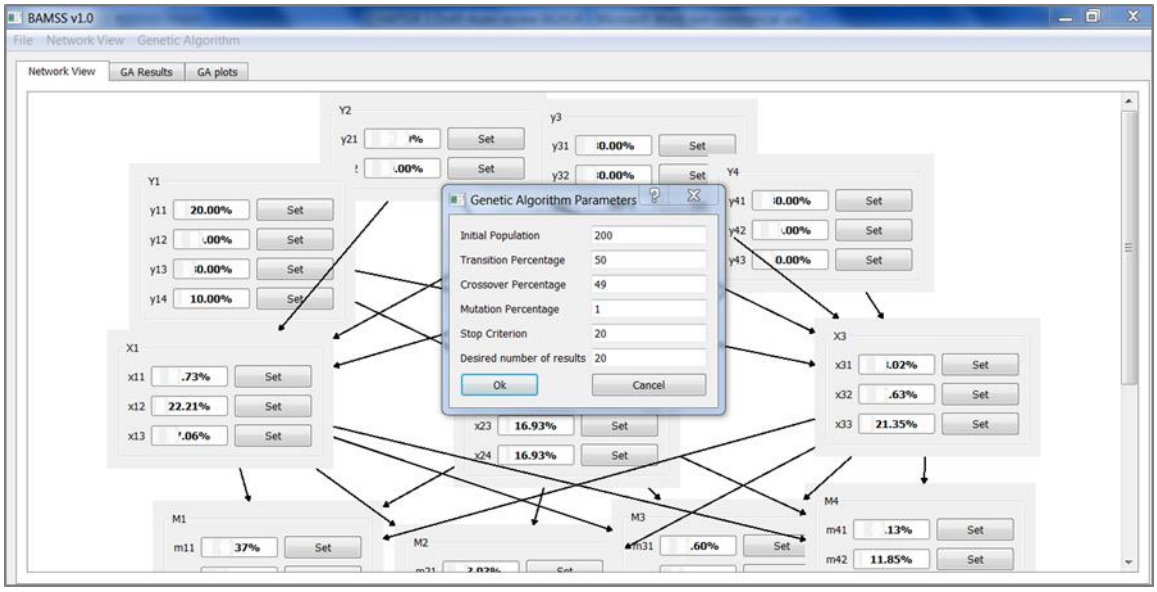

Figure 30. Graphical user interface for the BAMSS-GA module.

The complete GA processing returned a table with the *k* most probable network states as shown in Figure 31. The first column here, represents the probability of the selected MPE defined as the probability that the network will be in the chosen state. The second column is the genotype, a string representation of the MPE where each gene represents a specific node in the network (random variable) and the outcome of that node. The third column is the graphical representation of the phenotype, showing all the nodes in the appropriate state. Each node has the state of the random variable set according to the genotype of the MPE.

Belief Updating and Abductive Inference is performed when the user selects the phenotype of the MPE. The resultant Network and posterior probabilities are displayed as shown in Figure 32. The kMPEs are stored in a sensemaking database and when appropriately selected are loaded into BAMSS by the "Select Model File" command in the BAMSS GUI. When new evidence is available, inference is performed using the Bayesian Clustering Algorithm as described in Chapter 4.

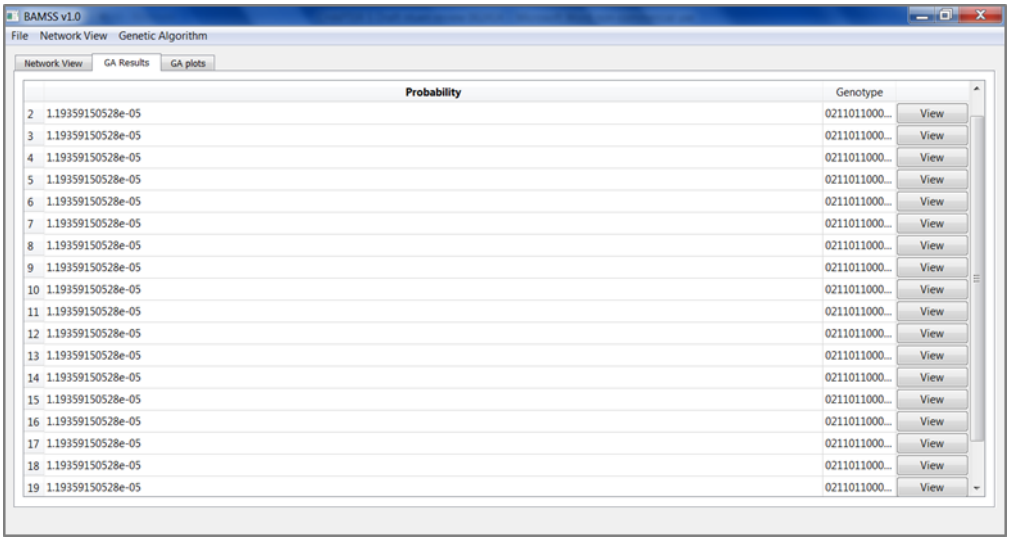

Figure 31. The *kMPE* output of the BAMSS-GA module.

Figure 32 shows the network view of the phenotype of the selected MPE. Clicking on the view button shows one global view of the MPE.

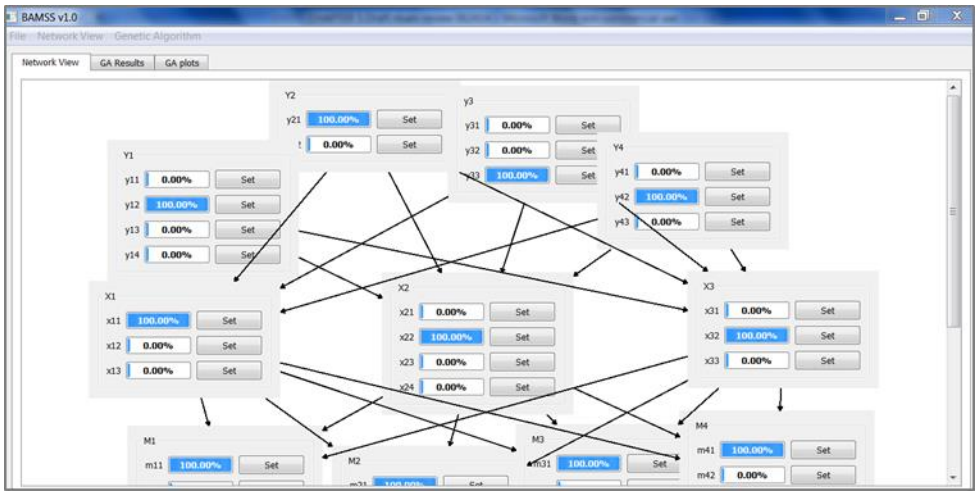

Figure 32. Network view of the phenotype of a selected MPE.

The BAMSS-GA GUI allows the user to plot and graphically evaluate the evolution of the fitness value of the selected solution(s) in each generation. Figure 33 shows the evolution of probabilities over all the generations for the best, the worst and the average solutions. The green line represents the best solutions while the red line represents the worst solutions. The average of

the two populations represents the convergence trend towards an optimal solution and is represented by the blue line. This is a graphical representation of how the algorithm search process refines the results pool over each generation and how fast it converges towards the optimal result.

The best solution follows a logarithmic growth curve, increasing rapidly for the first 10 generations before flat lining to a constant level. The maximum probability is reached at the 10th generation. The average solution asymptotically approaches the best solution, converging after 15 generations. The worst solution of the network is a non-monotonic with oscillations of significant amplitude especially after 10 generations. The oscillations of the fitness (probability) of the solutions in each generation indicate that the algorithm is sampling from a diverse population and this is a desirable feature for the model to achieve better results. The probability of the MPE is plotted on the y-axis while the iteration or generation number is plotted on the x-axis.

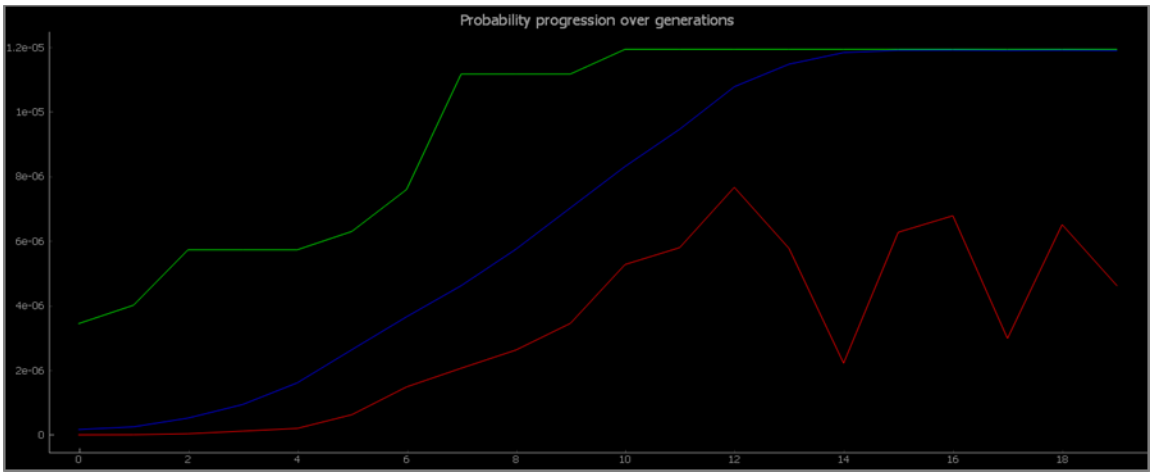

Figure 33. Evolution of fitness for the best, average and worst solutions of the *BAMSS COA Analysis* network for experiment 1.Green = best solution, Blue = average, Red = worst solution.

The effects of varying the GA parameters for the second and third simulations are shown in Figure 34. The most significant effect is the faster convergence to an optimal Network solution. The population diversity is increased due to an increase in the probability of *mutation* and hence, the convergence of the algorithm to an optimal solution is faster. The behavior of the worst individuals is also significantly improved with fewer oscillations due to the diverse sampling population. The probability of the MPE is plotted on the y-axis while the iteration or generation number is plotted on the x-axis.

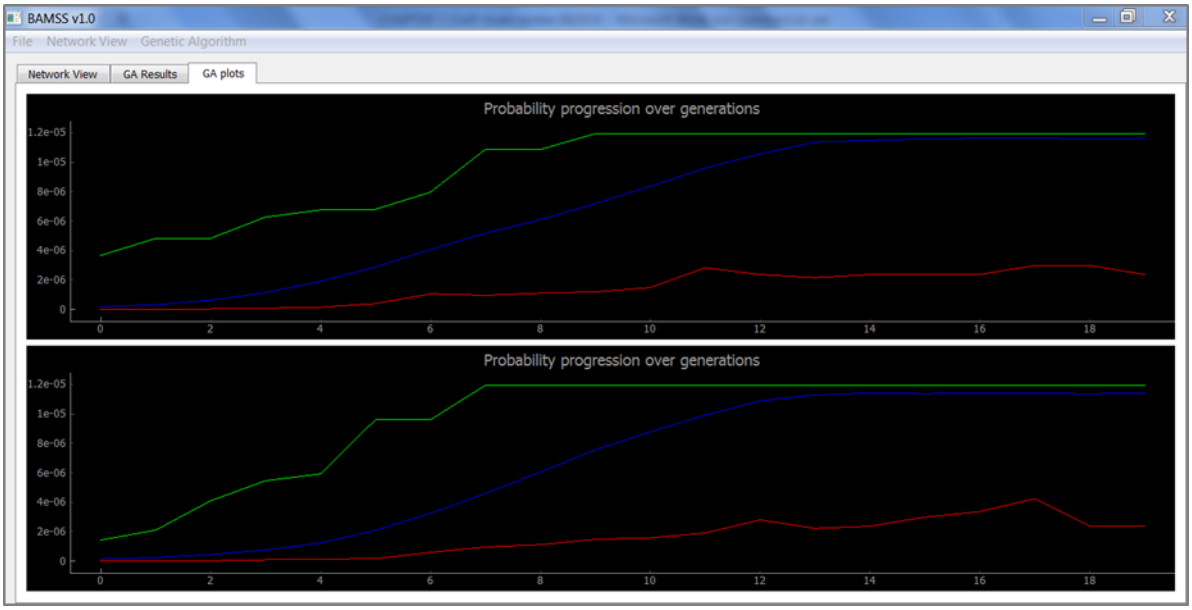

Figure 34. Effects of varying the GA parameters on the network solution probability for experiment 2(top) and experiment 3(bottom).Green = best solution, Blue = average solution, Red = worst solution.

Table 27 is a summary of the probability of the best, average, and worst network solutions obtained for each of the three trials. A result for only the first 10 generations are shown since convergence to the best solution occurs after about 10 generations. The genotype for the kMPEs is [02110110000000] which is decoded to the phenotype [$Y_1 = y_{12}$, $Y_2 = y_{21}$, $Y_3 = y_{33}$, $Y_4 = y_{42}$; $X_1 = x_{11}$, $X_2 = x_{22}$, $X_3 = x_{32}$; $M_1 = m_{11}$, $M_2 = m_{21}$, $M_3 = m_{31}$, $M_4 = m_{41}$; $T_1 = t_{11}$, $T_2 = t_{21}$, $T_3 = t_{31}$].

Table 27

Probability of MPE for the Simulation Experiments

Experiment 1				Experiment 2				Experiment 3			
P (MPE)				*P(MPE)*				*P(MPE)*			
Gen #	Best	Average	Worst	Gen #	Best	Average	Worst	Gen #	Best	Average	Worst
0	3.44E-06	1.03E-09	1.65E-07	0	2.25E-06	1.87E-09	1.83E-07	0	3.89E-06	3.76E-09	1.65E-07
1	4.01E-06	4.90E-09	2.48E-07	1	4.50E-06	3.20E-09	2.98E-07	1	3.89E-06	2.73E-09	2.59E-07
2	5.73E-06	3.40E-08	5.19E-07	2	4.50E-06	4.31E-08	5.91E-07	2	3.89E-06	3.23E-08	5.20E-07
3	5.73E-06	1.15E-07	9.39E-07	3	4.50E-06	9.19E-08	1.04E-06	3	4.00E-06	1.02E-07	9.42E-07
4	5.73E-06	2.00E-07	1.61E-06	4	1.02E-05	2.20E-07	1.69E-06	4	5.76E-06	1.49E-07	1.51E-06
5	6.30E-06	6.24E-07	2.64E-06	5	1.02E-05	2.65E-07	2.61E-06	5	9.81E-06	2.09E-07	2.29E-06
6	7.59E-06	1.48E-06	3.65E-06	6	1.02E-05	7.17E-07	3.75E-06	6	9.81E-06	3.92E-07	3.32E-06
7	1.12E-05	2.06E-06	4.62E-06	7	1.12E-05	8.38E-07	5.19E-06	7	9.81E-06	6.79E-07	4.45E-06
8	1.12E-05	2.62E-06	5.74E-06	8	1.12E-05	8.94E-07	6.50E-06	8	9.81E-06	1.51E-06	5.78E-06
9	1.12E-05	3.45E-06	7.03E-06	9	1.19E-05	2.23E-06	7.71E-06	9	1.19E-05	1.51E-06	6.90E-06
10	1.19E-05	5.27E-06	8.31E-06	10	1.19E-05	1.52E-06	8.89E-06	10	1.19E-05	1.23E-06	8.06E-06

Table 28 shows the comparison of performance gains for BAMSS-GA compared to BAMSS for the three experiments. Seven simulations were performed for each experiment and the MPE for each run selected. The corresponding genotype of each MPE is shown in the second column. For all the simulation runs, each variable of the network was set to a specific state which was held constant across all the trials. The probability of evidence for BAMSS (Bayesian Clustering Algorithm) and BAMSS-GA was then computed.

Table 28

Performance Comparison for BAMSS and BAMSS-GA

	Experiment 1		Experiment 2		Experiment 3	
P (*MPE)* BAMSS	MPE Genotype	P(*MPE)* BAMSS-GA	MPE Genotype	P (*MPE*) BAMSS-GA	MPE Genotype	P(*MPE*)) BAMSS-GA
1.508E-08	02110110000000	1.193E-05	02110110000000	1.193E-05	02120110000000	8.951E-06
8.639E-09	10000100000000	4.789E-05	10000100000000	4.789E-05	10000100300000	3.369E-05
7.999E-09	10000100000000	4.543E-05	10000100000000	4.543E-05	10000101000000	3.724E-05
7.251E-09	10002100200000	4.227E-05	10000100000000	4.693E-05	10002110000000	3.672E-05
7.504E-09	10000100000000	5.602E-05	10000100200000	5.038E-05	10000110000000	4.866E-05
5.823E-09	10002100300000	4.849E-05	10000100300000	5.385E-05	10000110300000	4.678E-05
8.446E-09	10000100300000	4.873E-05	10000100300000	4.874E-05	10000110000000	3.963E-05

The results of these simulations are displayed graphically in Figures 35-38.To make the charts readable, a logarithmic scale was used for the probability of the network solution denoted as P(*MPE*) or simply as P(*e*).

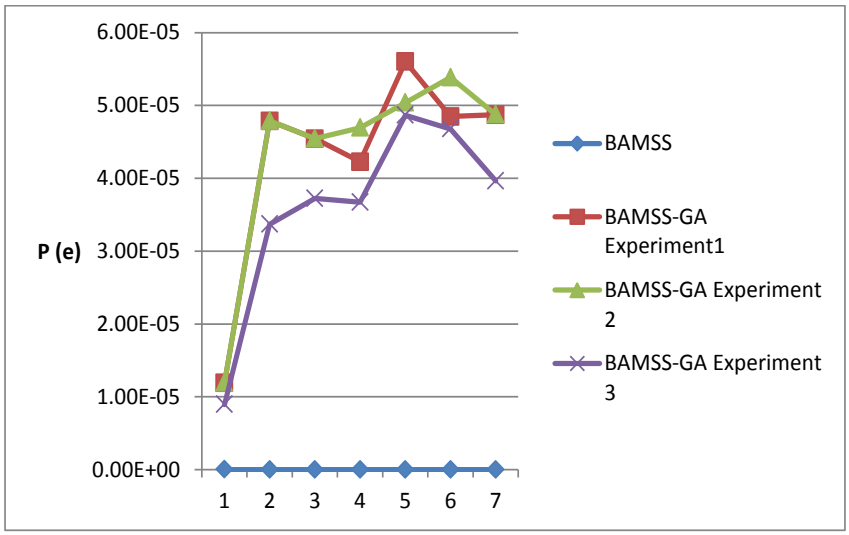

Figure 35. Comparison of performance gains for BAMSS-GA for Experiments 1, 2 and 3.

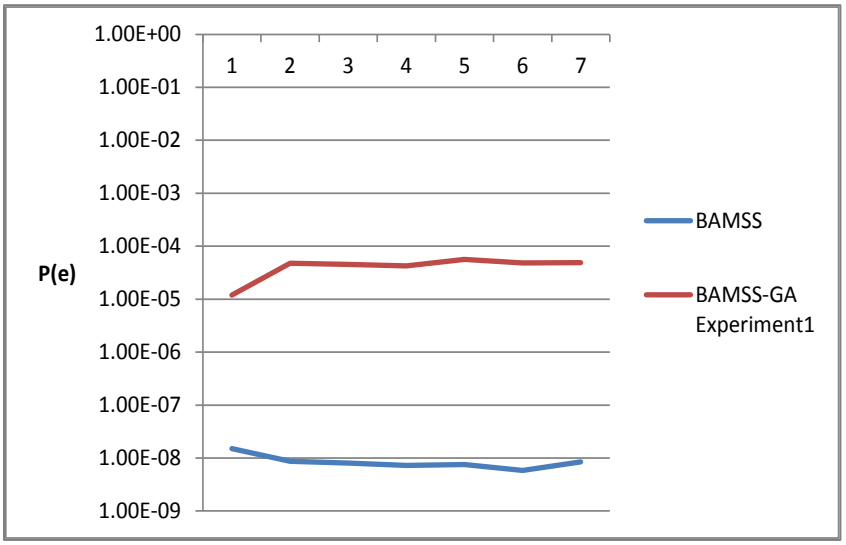

Figure 36. Performance gains for BAMSS-GA compared to BAMSS for Experiment 1.

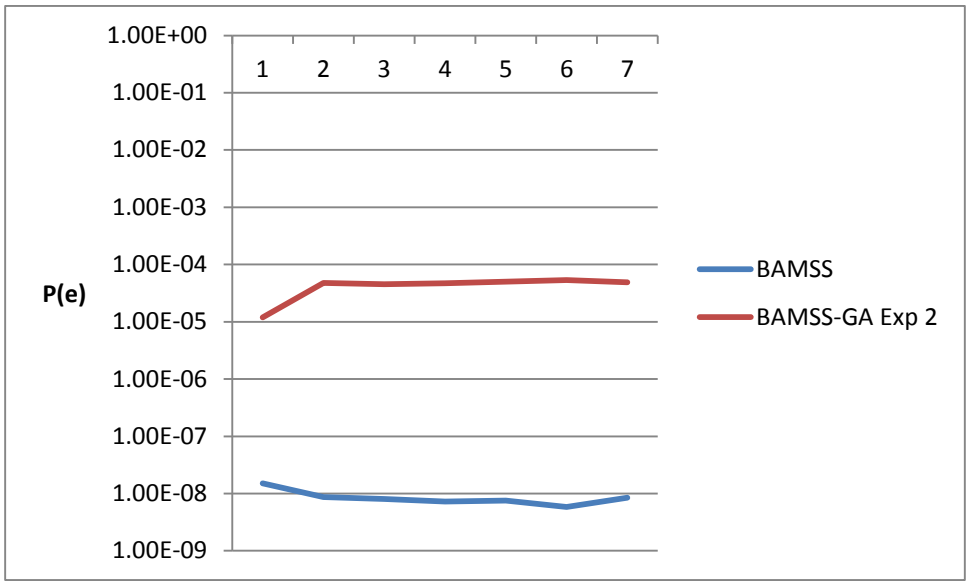

Figure 37. Performance gains for BAMSS-GA compared to BAMSS for experiment 2.

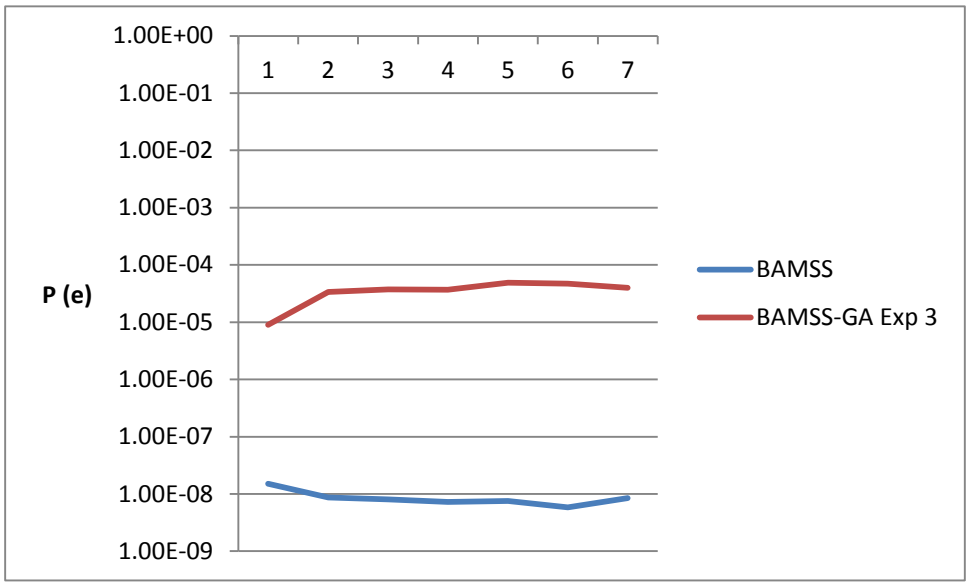

Figure 38. Performance gains for BAMSS-GA compared to BAMSS for experiment 3.

5.4 Discussion

The results shown in the preceding section show that the BAMSS-GA is able to find the *kMPEs* for the Network in a fast and an efficient manner. The probabilities presented in Table 27 represent the probabilities of obtaining Network solutions of that configuration. These

probabilities are also displayed in the first column of Figure 31. For each experiment, the probabilities of 10 Network solutions are presented along with the optimal solution. To each solution, there exists a specific genotype corresponding to the combination of variables that can produce the solution as displayed in the second column of Figure 31. The genotype for the kMPEs is [02110110000000] which is decoded to the phenotype [$Y_1 = y_{12}$, $Y_2 = y_{21}$, $Y_3 = y_{33}$, $Y_4 = y_{42}$; $X_1 = x_{11}$, $X_2 = x_{22}$, $X_3 = x_{32}$; $M_1 = m_{11}$, $M_2 = m_{21}$, $M_3 = m_{31}$, $M_4 = m_{41}$; $T_1 = t_{11}$, $T_2 = t_{21}$, $T_3 = t_{31}$]. From the phenotype, the extracted hypotheses for the MPE are $Y_1 = y_{12}$ (*Law and Order Breakdown*); $Y_2 = y_{21}$ *(Sectarian Governance Structures)*, $Y_3 = y_{33}$ *(Disruption of Civic and Governance Processes)* and $Y_4 = y_{42}$ *(Sectarian Violence)*.

A comparison of performance gains obtained by using BAMSS-GA is shown in Table 28. Using the Bayesian Clustering Algorithm (Chapter 4), each simulation can only return one probability of the Network solution. An advantage of using GA, as shown in Tables 27 and 28 is that each simulation returns more than one Network solution as well as the optimal Network solutions based on the user defined parameters. If the analyst is interested in 20 solutions with a fitness value of, say 70%, the only input needed is the parameter specification. The output results will contain 20 Network solutions with a 70% probability of occurring given the evidence as well as the probability and genotype of the optimal Network solution.

For COA analysis, the states of the variables for the three experimental configurations in the simulation were set as follows: The hypothesis variable Y_1 was set to state y_{13} (*Insurgent Control of the Population*).Similarly $Y_2 = y_{21}$ (*Sectarian governance structures*), $Y_3 = y_{32}$ (*Insurgent control of the security space*), and $Y_4 = y_{41}$ (*Nationalism*).The informational variables were set as follows: $X_1 = x_{11}$, $X_2 = x_{23}$, $X_3 = x_{32}$, $M_1 = m_{12}$,$M_2 = m_{23}$,$M_3 = m_{33}$,$M_4 = m_{42}$, $T_1 = t_{12}$, $T_2 = t_{23}$ and $T_3 = t_{32}$. For experiment 1, using BAMSS-GA, the probability of obtaining an MPE is

4.227E-05 with the genotype [10002100200000] corresponding to phenotypes: $Y_1 = y_{12}$, $Y_2 = y_{21}$, $Y_3 = y_{31}$, $Y_4 = y_{41}$; $X_1 = x_{13}$, $X_2 = x_{22}$, $X_3 = x_{31}$; $M_1 = m_{11}$, $M_2 = m_{24}$, $M_3 = m_{31}$, $M_4 = m_{41}$; $T_1 = t_{11}$, $T_2 = t_{21}$, $T_3 = t_{31}$.

For illustration purposes, assume that the following hypotheses are under consideration by the commander: $Y_1 = y_{13}$ (*Insurgent Control of the Population*), $Y_2 = y_{21}$ (*Sectarian Governance Structures*), $Y_3 = y_{32}$ (*Insurgent Control of the Security Space*) and $Y_4 = y_{41}$ (*Insurgent Nationalism*). From the simulation results, considering only the Y_1 hypothesis variable, the MPE is $Y_1 = y_{12}$ (*breakdown in law and order*) and not the initial hypothesis state y_{13} (*Insurgent Control of the Population*). The change in the hypothesis state is supported by explanatory variables $X_3|x_{32} \rightarrow x_{31}$ (*Unbounded Battlespace*), $M_1|m_{12} \rightarrow m_{11}$ (*Insurgent Security Target Engagement*). For experiment 2, the probability of the MPE is 4.693E-05 with a corresponding genotype, [10000100000000]. The informational variable changes from $X_1 = x_{13}$ to $X_1 = x_{11}$ meaning the most probable state of the Network is to be reached if we consider the insurgent political operational effect to be *Sectarian Identity* ($X_1 = x_{11}$) rather than the *Legitimacy of Jihad* ($X_1 = x_{13}$). Additionally the tactical effect changes from $T_3 = t_{32}$ (*Infrastructure Sabotage*) to $T_3 = t_{31}$ (*Arson*). The commander will therefore have to give more weight to this evidence variable for detail planning by, for example, increasing force levels in areas where critical infrastructure such as dams or power stations are located or deploying surplus units.

For experiment 3, the probability of the MPE is 3.672E-05 with a genotype, [10002110000000].The evidence variable $X_3 = x_{31}$ (*Unbounded Battlespace*) changes to $X_3 = x_{32}$ (*Techniques, Tactics and Procedures*). In this case a change in the counterinsurgent force tactics may be required to counteract the insurgents who operate with highly dispersed and

decentralized command and control structures. The commander may have to consider these changes in the Political Operational Effects to inform the select hypotheses.

Using the Bayesian Clustering Algorithm, the probability for getting an MPE with the Network evidence set as previously described is 7.251E-09. Note that the probability of obtaining the Network solution, P(MPE) decreases by an order of magnitude (10^3) due to the inherent limitations of the clustering algorithm. In general, from the *k*MPEs output from BAMSS-GA, the analyst can select an MPE for a COA analysis. When new evidence is introduced in the evidence variables of the network, the Bayesian Clustering Algorithm is then applied and the posterior belief distribution of the hypothesis variables or the target variables of interest is computed as discussed in Chapter 4.

5.5 Chapter Summary

This chapter described the optimization of abductive inference in BAMSS using a Genetic Algorithm. The problem of Abductive Inference was presented as one of finding the most probable explanation or the MPEs of a Bayesian Network. Three simulation runs were conducted, varying the GA parameters for each run. For the first experiment, the probability of crossover was set to 0.49 while the probability of mutation was set at 0.01. The probability of the best network solution (MPE) was 1.19E-0.5 for the genotype [02110110000000] with a corresponding phenotype [$Y_1 = y_{12}$, $Y_2 = y_{21}$, $Y_3 = y_{33}$, $Y_4 = y_{42}$; $X_1 = x_{11}$, $X_2 = x_{22}$, $X_3 = x_{32}$; $M_1 = m_{11}$, $M_2 = m_{21}$, $M_3 = m_{31}$, $M_4 = m_{41}$; $T_1 = t_{11}$, $T_2 = t_{21}$, $T_3 = t_{31}$]

For the second experiment, the parameters were varied with the probability of crossover = 0.4 and the probability of mutation = 0.1. By comparing the best results for each experiment in Table 27 using the P(MPE) or *P(e)* as the comparison metric, this experimental configuration yielded 30% better network solutions due to the population diversity introduced by the increase

in the probability of mutation. The third simulation experiment with *P*(*Crossover)* = 0.35 and *P*(*Mutation*) = 0.15 did not show much improvement in the quality of the solutions implying that the best parameter setting had been exceeded.

For COA analyses, the states of the variables for all the experimental configurations in the simulation were set as follows: The hypothesis variable Y_1 was set to state y_{13} (*Insurgent Control of the Population*).Similarly $Y_2 = y_{21}$ (*Sectarian governance structures*), $Y_3 = y_{32}$ (*Insurgent control of the security space*), and $Y_4 = y_{41}$ (*Nationalism*).The informational variables were set as follows: $X_1 = x_{11}$, $X_2 = x_{23}$, $X_3 = x_{32}$, $M_1 = m_{12}$, $M_2 = m_{23}$, $M_3 = m_{33}$, $M_4 = m_{42}$, $T_1 = t_{12}$, $T_2 = t_{23}$ and $T_3 = t_{32}$. Tables 29-31 give the summary and comparisons of the outcomes of the experiments. The most probable hypothesis and the explanatory variables are highlighted.

Table 29

Experiment 1: Probability of Crossover = 0.49, Probability of Mutation = 0.01, Number of Generations=20, k MPEs=20

Genotype Input	Hypothesis Input nodes	Input Informational Variables	Output Hypothesis nodes	Best Explanatory Variables	Network Efficiency	Comments
10100211221121	$Y_1 = y_{13}$ $Y_2 = y_{21}$ $Y_3 = y_{32}$ $Y_4 = y_{41}$	$X_1 = x_{11}$ $X_2 = x_{23}$ $X_3 = x_{32}$ $M_1 = m_{12}$ $M_2 = m_{23}$ $M_3 = m_{33}$ $M_4 = m_{42}$ $T_1 = t_{12}$, $T_2 = t_{23}$, $T_3 = t_{32}$	$Y_1 = y_{12}$ $Y_2 = y_{21}$ $Y_3 = y_{31}$ $Y_4 = y_{41}$	$X_1 = x_{11}$, $X_2 = x_{23}$, $X_3 = x_{31}$, $M_1 = m_{11}$, $M_2 = m_{24}$ $M_3 = m_{31}$ $M_4 = m_{41}$ $T_1 = t_{11}$, $T_2 = t_{21}$, $T_3 = t_{31}$	85% →17 out of 20 plausible network solutions better than BAMSS	Most probable hypothesis is *Breakdown in Law and Order*, y_{12} not *Insurgent Control of the Population*, y_{13}.

Table 30

Experiment 2: Probability of Crossover = 0.40, Probability of Mutation = 0.10, Number of Generations=20, k MPEs=20

Genotype Input	Hypothesis Input nodes	Input Informational Variables	Output Hypothesis nodes	Best Explanatory Variables	Network Efficiency	Comments
10100211221121	$Y_1 = y_{13}$ $Y_2 = y_{21}$ $Y_3 = y_{32}$ $Y_4 = y_{41}$	$X_1 = x_{11}$ $X_2 = x_{23}$ $X_3 = x_{32}$, $M_1 = m_{12}$ $M_2 = m_{23}$ $M_3 = m_{33}$ $M_4 = m_{42}$ $T_1 = t_{12}$ $T_2 = t_{23}$ $T_3 = t_{32}$	$Y_1 = y_{11}$ $Y_2 = y_{22}$ $Y_3 = y_{31}$ $Y_4 = y_{41}$	$X_1 = x_{13}$ $X_2 = x_{22}$ $X_3 = x_{31}$ $M_1 = m_{11}$ $M_2 = m_{21}$ $M_3 = m_{31}$ $M_4 = m_{41}$ $T_1 = t_{11}$ $T_2 = t_{21}$ $T_3 = t_{31}$	95%→ 19 out of 20 plausible network solutions better than BAMSS	$X_1 = x_{13}$ to $X_1 = x_{11}$: the insurgents are using *Sectarian Identity* ($X_1 = x_{11}$) rather than the *Legitimacy of Jihad* ($X_1 = x_{13}$) as the political operations effect.

Table 31

Experiment 3: Probability of Crossover = 0.35, Probability of Mutation = 0.15, Number of Generations=20, k MPEs=7

Genotype Input	Hypothesis Input nodes	Input Informational Variables	Output Hypothesis nodes	Best Explanatory Variables	Network Efficiency	Comments
10100211221121	$Y_1 = y_{13}$ $Y_2 = y_{21}$ $Y_3 = y_{32}$ $Y_4 = y_{41}$	$X_1 = x_{11}$ $X_2 = x_{23}$ $X_3 = x_{32}$ $M_1 = m_{12}$ $M_2 = m_{23}$ $M_3 = m_{33}$ $M_4 = m_{42}$ $T_1 = t_{12}$ $T_2 = t_{23}$ $T_3 = t_{32}$	$Y_1 = y_{11}$ $Y_2 = y_{22}$ $Y_3 = y_{31}$ $Y_4 = y_{41}$	$X_1 = x_{12}$ $X_2 = x_{22}$ $X_3 = x_{32}$ $M_1 = m_{11}$ $M_2 = m_{21}$ $M_3 = m_{31}$ $M_4 = m_{41}$ $T_1 = t_{11}$ $T_2 = t_{21}$ $T_3 = t_{31}$	70%→14 out of 20 plausible network solutions better than BAMSS	$X_3 = x_{31}$ *Unbounded Battlespace* changes to $X_3 = x_{32}$ *Techniques, Tactics and Procedures* . Probable COA is to consider changes in coalition TTPs

Comparison of performance gains for BAMSS-GA and BAMSS was performed using the same experimental setup. Using P(MPE) as the comparison metric, the results showed that Bayesian Network inference using BAMSS-GA produced better network solutions than BAMSS by an order of magnitude (10^3). The network view of the computed MPE gave a representation of the network nodes with evidence set to the state of the solution. The phenotype of this representation was a network with a global state of the computed posterior probabilities. When the network was loaded into BAMSS, the computed posterior probabilities became priors and prior conditionals. When new evidence was introduced into the network, the Bayesian Inference algorithm was applied and the updated posterior beliefs of the hypothesis variables or target variables of interest were computed.

CHAPTER 6

Observations, Conclusions and Future Research

6.1 Summary

Chapter one offers a general introduction to the research topic, the problem statement, the research goals and objectives, the challenges encountered in the research and the general contribution to the scientific body of knowledge. Chapter two reviews both the qualitative and analytical models of sensemaking. From the qualitative analyses, most researchers have focused on the aspect of cognition where the primary sensemaking task is to construct a meaningful mental representation of the problem space. Schema-driven representation, mental models, and other cognitive constructs dominate the process models of sensemaking that have been discussed. These models give an understanding of the meta-cognitive and cognitive acts that inform the sensemaking process and determine how they may be applied to understand and overcome the cognitive limitations of the human mind. The limitations of this approach lie primarily in the lack of a unifying paradigm of sensemaking. An additional challenge exists in knowing how to use information gained from these models to develop a unifying framework or provide standardized guidance for the development of better sensemaking support systems.

Research on sensemaking analytics is presented as a tool to support the sensemaking process. In this approach, sensemaking models are defined as computational cognitive models whose primary task is to enable processing of information to achieve an understanding of the problem space and facilitate an effective analysis process. Most of the models discussed have been developed for the fields of intelligence analysis, information foraging and knowledge management. The diversity of approaches advocated provides challenges in developing a unified sensemaking process. A critical look at the tools developed does point to one aspect: the gradual

shift from decision support tools to sensemaking support tools. Sensemaking support tools focus on augmenting the cognitive capability of the sense-maker during the whole process of sensemaking.

This research uses the tool-based approach for two reasons: First, advances in the field of Computational Intelligence have led to the development of powerful and efficient algorithms and methods that can be used to computationally simulate some processes in sensemaking. For example, it is possible to represent sensemaking models in software and cognitive architectures. The algorithms can simplify the process of sensemaking tasks in context. Second, through the use of computational techniques such as Bayesian Networks and Abductive Inference, both the qualitative and quantitative approaches can be combined to provide a better representation of a sensemaking process.

Chapter three discusses Bayesian Formalism for representing sensemaking information. The Bayesian Belief Network reflects a person's belief about the state of a variable in the real world through the use of joint probability distributions over the variables. Bayesian Networks are presented as normative cognitive models that support sensemaking under uncertainty. The networks are shown to support reasoning about evidence and actions not easily handled by other competing computational models. In a Bayesian Belief Network, inference is undertaken by abduction. This means that we infer from effects to the best explanation of those effects. This reflects the behavior of a sensemaking problem. A forward (top-down) inference was shown to support prospective sensemaking, while a backward (bottom-up) inference supported information fusion in retrospective sensemaking.

Chapter four discusses the development experiments and validations of the BAMSS model using a case study in asymmetric warfare. Vignettes representative of a sensemaking task

in the asymmetric warfare domain were developed and used for analyses. In the first vignette, the sensemaking task required an analyst to create a hypothesis variable $Y_1 = y_{12}$ where y_{12} represented *Law and Order Breakdown*. New evidence was then introduced in the node $M_1 = m_{11}$, where m_{11} was an indicator for the *Security Target Engagement* by varying the input data from 0.1 to 0.9. Results from seven simulation runs were then analyzed for the informational variables $X_1 = x_{11}$ (*Sectarian Identity*) and $T_3 = t_{32}$ (*Infrastructure Sabotage*).

Examining the evidence propagation in the first vignette, the probability of (*Law and Order Breakdown*) remained relatively stable at 40% with increasing evidence of adversary targeting of the counterinsurgent security personnel. The relative stability of the posterior belief distribution implied that the causal effect of this variable was limited hence does not carry much weight as a COA. The probability that the *Insurgent Security Target Engagement* as a mode of operation was influenced by *Sectarian Identity* ($X_1 = x_{11}$) decreased from 50% to 30% .This would imply that operations against security personnel could not be attributed to a particular group. In fact, focusing on the sectarian identity of the group could be detrimental to the course of action selection because of the negative correlation and this effect then, ought to be discarded. The probability of (*Infrastructure Sabotage*| *Insurgent Security Target Engagement*) increased from 20 to 40%. An increase in infrastructure sabotage was the most likely tactical effect of the increase in insurgent security target engagement probably due to the vacuum created by this particular military operational effect. This COA would require the commander to increase protection for critical infrastructure and security targets.

For the second vignette, the hypothesis for the sensemaking task was changed to $Y_2 = y_{22}$ (*Insurgent ideology*). Evidence was introduced in node $X_3 = x_{33}$ (*Intelligence Asymmetry*) and the posterior probabilities for informational variables $M_1 = m_{11}$ *(Security Target Engagement)* and T_2

= t_{21} (*Small Arms Attacks*) were computed. The probability of (*Insurgent Security Target Engagement*| *Intelligence Asymmetry*) decreased from 60 to 35% as evidence for intelligence asymmetry increased from 0.1 to 0.9. This implied that better intelligence by the insurgent group was not a direct influence on this mode of operation. The commander's COA could likely invest more resources in recruiting intelligence assets to counteract the asymmetry. Probability of (*Small Arms Attacks*| *Intelligence Asymmetry*) showed minor variability at 40% similar to the *P*(*Insurgent Ideology*|*intelligence asymmetry*) . The tactical effect *Small Arms Attacks* was not significantly influenced by the insurgent intelligence assets. Both these effects were however, inadmissible as courses of action.

In the last sensemaking vignette, we considered the hypothesis variable $Y_4 = y_{41}$, the insurgent concept of *Nationalism*. For the informational variables we set $X_2 = x_{22}$ (*Insurgent Modular Operations*) and $M_2 = m_{23}$ *(Civilian Shelters)*. New evidence was introduced into variable $T_3 = t_{32}$ (*Arson*). The probability of (*Insurgent Modular Operations*| *Arson*) decreased from 50 to 40% (approximately) with an increase in evidence of *Arson* as a tactical effect from 0.1 to 0.9. The probability of *Nationalism* increased from 30 to 40% while the *P*(*Civilian Shelters*| *Arson*) remained constant at 30%. The commanders' COA could be to consider the tactical effect as a reflection of nationalistic feelings and take appropriate measures in the PMESII spectrum to address this effect. *P*(*Insurgent Modular Operations*| *Arson*) and *P*(*Civilian Shelters*| *Arson*) were not admissible for COA analyses.

A sensitivity analysis was performed on the model output for the second sensemaking support demonstration using three simulation experiments. In the first experiment, target nodes representing *Tactical Effects* variable T_1 (t_{11}, t_{12}, *and* t_{13}) were selected. The probability of (*Law and Order* |*High Level Attrition Attacks*) did not show significant variation to changes in input

evidence from 0.1 to 0.9. *P*(*Civilian Suicide Bombing*) showed the highest posterior belief accrual peaking at 58% demonstrating that the new evidence on this variable could confirm the most likely aposteriori hypothesis ($Y_1 = y_{12}$). On average, *P*(*Remotely Detonated IEDs*|*Law and Order Breakdown*) was 10% while *P*(*Rocket Propelled Grenades*|*Law and Order Breakdown*) was 28%. In general, the commander could consider the variable *Civilian Suicide Bombing* for additional analysis since it exhibited the greatest variation in response to changes in the input variable.

In the second simulation, a sensitivity analysis was performed on variable T_2 (t_{21}, t_{22}, t_{23}), varying the input to node $Y_4 = y_{42}$ (*Sectarian Violence*). *P*(*Small Arms Attacks*| *Sectarian Violence*) recorded the highest aposteriori probability at 44%. A COA analysis by the commander required a closer examination of the differences between t_{22} (*Coercive Threats*, 30%) and t_{23} (*Convoy Ambushes*, 30%) which seemed to exhibit interaction effects. Lastly, sensitivity analysis was done for target nodes T_2=t_{23} (*Convoy Ambushes*), T_3=t_{31} (*Infrastructure sabotage*), and T_3= t_{32} (*Arson*). *Infrastructure Sabotage* recorded the highest variations and posterior belief at 75% as evidence in the input variable $Y_2 = y_{22}$ (*Insurgent Ideology*) was varied from 0.1 to 0.9. The high degree of sensitivity to the variation in input could prompt the commander to perform additional what-if analyses to identify more causal variables. Similarly, for *P*(*Convoy Ambush*| *Sectarian Violence*) and *P*(*Arson*| *Sectarian Violence*), both had an average aposteriori probability of 30% since they exhibited mutually exclusive behaviors.

Chapter five described an optimization of Abductive Inference in BAMSS using a Genetic Algorithm(GA) and simulation experiments to find the most probable explanations (MPEs). Three simulation runs were conducted, varying the GA parameters for each run. For the first experiment, the probability of crossover was set to 0.49 while the probability of mutation

was set at 0.01. The probability of the best network solution (MPE) was 1.19E-0.5 for the genotype [02110110000000] with a corresponding phenotype [$Y_1 = y_{12}$, $Y_2 = y_{21}$, $Y_3 = y_{33}$, $Y_4 = y_{42}$; $X_1 = x_{11}$, $X_2 = x_{22}$, $X_3 = x_{32}$; $M_1 = m_{11}$, $M_2 = m_{21}$, $M_3 = m_{31}$, $M_4 = m_{41}$; $T_1 = t_{11}$, $T_2 = t_{21}$, $T_3 = t_{31}$]

For the second experiment the parameters were varied with the probability of crossover = 0.4 and the probability of mutation = 0.1. By comparing the best results for each experiment in Table 27 using the P(MPE) as the comparison metric, this experimental configuration yielded 30% better network solutions due to the population diversity introduced by the increase in the probability of mutation. The third simulation experiment with the probability of crossover = 0.35 and the probability of mutation = 0.15 did not show much improvement in the quality of the solutions implying that the best parameter setting had been exceeded.

For COA analysis, the states of the variables for the three experimental configurations in the simulation were set as follows: The hypothesis variable Y_1 was set to state y_{13} (*Insurgent Control of the Population*). Similarly, $Y_2 = y_{21}$ (*Sectarian governance structures*), $Y_3 = y_{32}$ (*Insurgent control of the security space*), and $Y_4 = y_{41}$ (*Nationalism*). The informational variables were set as follows: $X_1 = x_{11}$, $X_2 = x_{23}$, $X_3 = x_{32}$, $M_1 = m_{12}$,$M_2 = m_{23}$,$M_3 = m_{33}$,$M_4 = m_{42}$, $T_1 = t_{12}$, $T_2 = t_{23}$ and $T_3 = t_{32}$. For experiment 1, using the BAMSS-GA, the probability of obtaining an MPE was 4.227E-05 with the genotype [10002100200000] corresponding to phenotypes: $Y_1 = y_{12}$, $Y_2 = y_{21}$, $Y_3 = y_{31}$, $Y_4 = y_{41}$; $X_1 = x_{13}$, $X_2 = x_{22}$, $X_3 = x_{31}$; $M_1 = m_{11}$, $M_2 = m_{24}$, $M_3 = m_{31}$, $M_4 = m_{41}$; $T_1 = t_{11}$, $T_2 = t_{21}$, $T_3 = t_{31}$.

For illustration purposes, assume that the following hypotheses are under consideration by the commander: $Y_1 = y_{13}$ (*Insurgent Control of the Population*), $Y_2 = y_{21}$ (*Sectarian Governance Structures*), $Y_3 = y_{32}$ (*Insurgent Control of the Security Space*) and $Y_4 = y_{41}$ (*Insurgent Nationalism*). From the simulation results, considering only the Y_1 hypothesis

variable, the MPE supports $Y_1 = y_{12}$ (*breakdown in law and order*) and not the initial hypothesis state y_{13} (*insurgent control of the population*). The change in the hypothesis state is supported by explanatory variables $X_3|x_{32} \rightarrow x_{31}$ (*Unbounded Battlespace*), $M_1|m_{12} \rightarrow m_{11}$ (*Insurgent Security Target Engagement*).

For experiment 2, the probability of the MPE is 4.693E-05 with a corresponding genotype, [10000100000000]. The informational variable changes from $X_1 = x_{13}$ to $X_1 = x_{11}$ meaning the most probable state of the network is to be reached if we consider the insurgent political operational effect as using *Sectarian Identity* ($X_1 = x_{11}$) rather than the *Legitimacy of Jihad* ($X_1 = x_{13}$). Additionally the tactical effect changes from $T_3 = t_{32}$ (*Infrastructure Sabotage*) to $T_3 = t_{31}$ (*Arson*). The commander will therefore have to give more weight to this evidence variable for detail planning in the form of perhaps increasing force levels in areas where critical infrastructure such as dams or power stations are located or deploying surplus units. For the third experiment, the probability of the MPE is 3.672E-05 with a genotype, [10002110000000]. The evidence variable $X_3 = x_{31}$ (*Unbounded Battlespace*) changes to $X_3 = x_{32}$ (*Techniques, Tactics and Procedures*). In this case a change in the counterinsurgent force tactics may be required to counteract the insurgents who operate with highly dispersed and decentralized command and control structures. The commander then, has to consider these changes in the *Political Operational Effects* to inform the select hypotheses.

Comparisons of performance gains for BAMSS-GA as compared to BAMSS were performed using the same experimental setup. Using P(MPE) as the comparison metric, the results showed that Bayesian Network Inference using BAMSS-GA produced better network solutions than BAMSS by an order of magnitude (10^3). A direct comparison with BAMSS was done using network efficiency as the metric. In this case, network efficiency refers to the

"throughput" or the ability of the model to generate plausible network solutions under the influence of various variables. For the first experiment, a network efficiency of 85% was achieved with BAMSS-GA. When the probability of crossover and mutation were varied for the second experiment, a network efficiency of 95% was realized. Additional variation in the GA parameters resulted in a network efficiency of 70%.

As per the experimental results, this means that the best configuration for BAMSS-GA is achieved when the probability of crossover is set to 40% and the probability of mutation is set at 10%. The network view of the computed MPE gives a representation of the network nodes with evidence set to the state of the solution. The phenotype of this representation is a network with a global state of the computed posterior probabilities. When new evidence is introduced into the network, the Bayesian Inference Algorithm is applied and the updated posterior beliefs of the hypothesis variables or target variables of interest are computed.

6.2 Observations and Conclusions

Belief Updating and Abductive Inference have been demonstrated using a BAMSS prototype, a sensemaking support tool. Two algorithms were implemented for BAMSS, the Bayesian Clustering Algorithm for Bayesian Abductive Inference and the Genetic Algorithm to optimize Abductive Inference in the model. Experimental simulation was used to test BAMSS and BAMSS-GA using sensemaking vignettes from an asymmetrical battlespace domain. A summary comparison of the major performance parameters for BAMSS and BAMSS-GA is presented below.

a) Problem Representation: The clustering algorithm used in BAMSS takes direct probability values as input without any need for extra data massaging. Some effort is needed to develop the network topology and populate the conditional probability tables with prior probabilities

for the parent variables and prior conditionals for the children variables. BAMSS-GA requires the input data to be encoded in a format that is compatible with GA operators. This requires additional computational resources to massage the data into GA format before it can be used as input to the BAMSS model.

b) Computational complexity: BAMSS uses a clustering algorithm, an exact search algorithm to perform inference in a Bayesian Network. For simple networks, the algorithm does not consume much computing resources. However, its search becomes limited as the network grows and more computation time is required. As the network grows, the clustering algorithm defaults to the use of hierarchical search through a top-down processing to reveal structures of interest at different levels in its divisive hierarchical clustering process. Divisive clustering, however, does not produce an optimal solution. Additionally, as the network complexity increases, inference using the clustering algorithm becomes intractable, exponentially increasing resource utilization. The space complexity is $O(n^2)$ because of the space required for adjacency matrix (where they are *n* items to cluster). The time complexity is $O(kn^2)$ because of there is one iteration for each level in the dendogram hence the matrix (or subset of it) must be accessed multiple times. BAMSS-GA uses a Genetic Algorithm to perform inference. GA has a parallel search capability which leads to a fast and efficient convergence to optimal network solution. Additionally, GAs search from a population of points and use a coding of the parameter sets as compared to the parameters themselves. GA can handle networks of varying complexity without significant resource utilization.

c) Quality of network solutions: BAMSS-GA can be configured to output *k* network solutions or *kMPEs* for each simulation run. Additionally, BAMSS-GA output can be configured to display the best (optimal), average and worst solutions. Without additional significant

computation, the output of BAMSS cannot be determined to be optimal on any input. Comparison of performance gains for BAMSS-GA as compared to BAMSS using the probability of MPE as the comparison metric showed that inference using BAMSS-GA produced better network solutions by an order of magnitude (10^3).

In order to obtain better solutions for BAMSS, two issues have to be considered: Foremost, an algorithm for CPT elicitation and computation should be incorporated. A CPT elicitation requires a considerable input time from the user and if not done right, can lead to outputs with spurious results. Algorithms with the capacity to filter inadmissible and/or conflicting CPT expressions have been developed. Inadmissible expressions often result into incompatible hypotheses or the wrong chains of evidence propagations through the network being output to the user. Secondly, the use of hybrid exact search algorithms to replace the clustering algorithm is found to speed up computation and output better and accurate results. Hybrid algorithms will produce better results than those produced by the clustering algorithm and in the case of some networks will produce results that are an order of magnitude more precise.

Although the asymmetric battlespace domain has been used for network development simulation experimentation, BAMSS is a sensemaking support tool and can used for any problem domain where causal reasoning and Abductive Inference is desired. With appropriately defined networks, BAMSS can be used for diagnostic assistance in the medical field, fault detection and isolation in engineering, as well as problem solving and data mining in education. The Open Source software used in its prototype development creates opportunities for further tailored development.

BAMSS is a standalone application, currently not hosted on the web server. To run the tool, the software listed in Table 2 has to be installed and run on the client machine. However,

the executable BAMSS files are easily portable and are readily available to the user. The only component of the BAMSS accessible on the web is GeNIe which is used for network development as described in Chapter 4.

This research represents a successful step in developing a proof of concept sensemaking support system that combines the qualitative and quantitative approaches of sensemaking with asymmetric battlespace as the problem domain. The use of Genetic Algorithms for sensemaking support has not been widely explored. We have demonstrated through experimental simulations that the use of GA for Abductive Inference can produce better results. This technique is useful for computational search for changes in a network due to belief revisions.

6.3 Lessons Learned and Recommendations for Future Research in BAMSS

The BAMSS developed in this research is a proof of concept in computational sensemaking, especially in extracting conditional evidences that support a set of hypotheses. Prior probabilities and prior conditionals for the *BAMSS COA Analysis* network were obtained from existing and historical databases of asymmetric wars in the Middle East. No empirical validation was performed. Additionally, empirical research needs to be done to test the model with real world data and military expert assessment. The experimental participants need to be given representative scenarios, be presented with evidence, and then, select a COA without the use of BAMSS. In the next iteration, the same participants should be required to use the tool, compare the COA selection in terms of accuracy (with or without the tool) and time needed to make the correct inference, and select a COA.

With regards to the BAMSS future development, a lot of software development work still remains to be done in order to seamlessly integrate the GA and the Bayesian Algorithm. The most important and immediate tasks to be accomplished are:

i) Since BAMSS requires a user to define the Belief Network, an additional task is to develop the Network module as a standalone application in order to remove the requirement for expert knowledge needed develop the N.etwork structure.

ii) A dedicated data parsing and formatting subroutine needs to be developed within the model to convert the output (posterior) probabilities into a format that is suitable for genetic algorithm application. The challenge is in developing automatic encoding functions to convert the Bayesian output (phenotype) to GA input (genotype). This will significantly increase the BAMSS functionality.

iii) A GUI front end is needed to support BAMSS. This can include the development of user manuals, an interactive help menu, and a function to enable the user to create new data fields.

iv) A further significant enhancement would be to add functionality to BAMSS so that it can perform sensitivity analysis automatically to reduce the manual COA selection from kMPEs

A web version of BAMSS that operates in a client-server model will enhance distributed access for multiple sensemakers who are distributively co-located or geographically dispersed.

References

Antonisse, J. (1989).A new interpretation of Schema notation that overturns the binary encoding constraint, in: J.D. Schaffer (Ed.), *Proceedings of the Third International Conference on Genetic Algorithms*, Morgan Kaufmann, Los Altos, CA.

Bar-Yam, Y. (2004). Multiscale variety in complex systems. *Complexity* 9, 4 (2004), 37–45.

Bell, B., Santos, E., Jr., & Brown, S. (2002). Making Adversary Decision Modeling Tractable with Intent Inference and Information Fusion, *In Proceedings of the 11th Conference on Computer Generated Forces and Behavioral Representation*.

Belton, V., & Stewart, T.J. (2002). *Multiple Criteria Decision Analysis: an Integrated Approach*. Boston, Kluwer Academic Press

Bhatnagar, R., & Kanal, L.N. (1993). Structural and Probabilistic Knowledge for Abductive Reasoning, in *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 15, number 3.

Bhattacharyya, S., & Koehler, G.J. (1994). An analysis of non-binary genetic algorithms with cardinality 2^v, *Complex Systems* 8, 227–256.

Bodnar, J.W. (2005). Making Sense of Massive Data by Hypothesis Testing. *In proceedings of the International Conference on Intelligence Analysis*, McLean, Va.

Boyd, J.R. (1987). *A Discourse on Winning and Losing*. Maxwell AFB: Air Defense University

Breton, R., & Rousseau, R. (2005). The C-OODA: A Cognitive Version of the OODA Loop to Represent C^2 Activities. In *Proceedings of the Tenth International Command and Control Research and Technology Symposium*, McLean, VA.

Buckingham-Shum, S., & Selvin, A.M. (1999). Collaborative Sense-Making in Design Involving Stakeholders via Representational Morphing. *Technical Report KMITR- 74*. Knowledge Media Institute: The Open University, UK

Card, S. (2004). From information visualization to sensemaking: Connecting the mind's eye to the mind's muscle .*Proceedings of the IEEE Symposium on Information Visualization, INFO VIS 2004*, p xii.

Chi, E. H., & Card, S. K. (1999).Sensemaking of evolving Web sites using visualization spreadsheets. *Proceedings 1999 IEEE Symposium on Information Visualization*; October 24-29, 1999; San Francisco, CA. Los Alamitos CA: IEEE Computer Society.

Cluxton, D., & Eick, S.G. (2005). DECIDE - A Hypothesis Visualization Tool. *In proceedings of the International Conference on Intelligence Analysis*, McLean, Va.

Conklin, J., & Begeman M. (1988). gIBIS: A hypertext tool for exploratory policy discussion. *ACM Transactions on Office Information Systems*, Vol. 6, No. 4. pp. 303-331

Das, B. (1999). Representing uncertainties using Bayesian networks. *Technical Report DSTO-TR-0918, Defence Science and Technology Organisation*, Salisbury, Australia.

Das, B. (2006). *Generating Conditional Probabilities for Bayesian Networks: Easing the Knowledge Acquisition Problem*, http://arxiv.org/abs/cs.AI/0411034 , Accessed in December 2013.

Davis, L. (1991). *Handbook of Genetic Algorithms*, Van Nostrand Reinhold, New York.

De Campos, L.M., Gamez, J.A., & Moral, S. (1999). Partial abductive inference in Bayesian belief networks using a genetic algorithm. *Pattern Recognition Letters, 20:1211–1217*.

De Campos, L. M., Gamez, J. A., & Moral, S. (2002). Partial abductive inference in Bayesian belief networks: an evolutionary computation approach by using problem-specific genetic operators. *IEEE Transactions on Evolutionary Computation. 6*, 2 (April), 105–131.

Díetz, F. J. (1993). Parameter adjustment in Bayes networks. The generalized noisy OR-gate. *Proceedings of the 9th Conference on Uncertainty in AI*, Washington DC, USA, pp. 99-105.

Eggleston, R.G., Bearavolu, R., & Mostashfi, A. (2005). Sensemaking Support Environment: A Thinking Aid for All-Source Intelligence Analysis Work. *In proceedings of the International Conference on Intelligence Analysis*, McLean, Va.

Eiter, T., & Gottlob, G. (1995). The complexity of logic based abduction. *Journal of ACM* 42(1):3–42.

Endsley, M. R. (1995). Situation awareness and the cognitive management of complex systems. *Human Factors Special Issue* 37(1): 85-104.

Evans, A., Graham, S., Jones, E.K., Pioch, N., Prendergast, M.& White, C.M. (2003) Strategy Development for Effects-Based Planning, *Military Operations Research Society official website*, http://www.mors.org/meetings/ebo/ebo_read.htm, last accessed December 2013.

Falzon, L., & Priest, J. (2004). The Center of Gravity Network Effects Tool: Probabilistic modeling for operational planning. Australia: *Defense Science and Technology Organization*. Pp. 1-45.

Feldman, M., & March, J.G. (1988). *Information in organizations as signal and symbol*. J.G. March (eds.). *Decision and Organizations*. Oxford, Cambridge: Basil Blackwell. 409-428

French, S. (2013). Cynefin, statistics and decision analysis. *Journal of the Operational Research Society*, 64(4), 547-561.

Furnas, G.W., Qu, Y., & Sharma, N.(2003). *CoSen* – Supporting Sensemaking across Different Scales of Social Aggregation. In *CHI '03 Extended Abstracts on Human Factors in Computing Systems.* CD, 906-907.

Gelsema, E.S. (1995).Abductive reasoning in Bayesian belief networks using a genetic algorithm. In *Pattern Recognition Letters 16*,865-871.

Goldberg, D.E. (1989). *Genetic Algorithms in Search, Optimization and Machine Learning*. Addison-Wesley, Reading, MA.

Good, L., Shrager, J., Stefik, M., Pirolli, P., & Card, S., (2004). *ACH0: A tool for analyzing competing hypotheses*. Technical description for Version 1.0. Palo Alto, CA: Palo Alto Research Center.

Gundry, J., & Metes, G. (1996). *Team Knowledge Management: A Computer-Mediated Approach*, Virtual Learning Systems Inc., Manchester NH, USA, December

Heckerman, D. (1997). Bayesian networks for data mining. *Data Mining and Knowledge Discovery* 1.pp 79-119.

Huber, G. P. (1991). Organizational learning: The contributing processes and literatures. *Organizational Science* 2(1) 88-115

Jensen, F.V., Lauritzen, S.L., & Olesen, K.G. (1990). Bayesian Updating in Causal Probabilistic Networks by Local Computations. *Computational Statistics Quarterly 4*: 269-282.

Johansson, F., & Falkman, G. (2008). A Bayesian network approach to threat evaluation with application to an air defense scenario. *In Proceedings of the 11th International Conference on Information Fusion*.

Jøsang, A. (2008). Abductive Reasoning with Uncertainty. *Proceedings of the International Conference on Information Processing and Management of Uncertainty (IPMU 2008*). Malaga, pp.9-16.

Kilcullen, LTCOL D. (2004). Complex Warfighting (*Draft Developing Concept*), Commonwealth of Australia.

Klein, G., Long, W. G., Hutton, R. B., & Shafer, J. (2004). *Battlesense: An innovative sensemaking-centered design approach for combat systems* (Final report prepared under contract # N00178-04-C-3017 for Naval Surface Warfare Center, Dahlgren, VA). Fairborn, Ohio: Klein Associates Inc.

Klein, G., Phillips, J. K., Rall, E., & Peluso, D. A. (2006). A data/frame theory of sensemaking. In R. R. Hoffman (Ed.), *Expertise out of context: Proceedings of the 6th International Conference on Naturalistic Decision Making*. Mahwah, NJ: Lawrence Erlbaum & Associates.

Konolige, K. (1992). Abduction versus closure in causal theories. *Artificial Intelligence Vol 53*, 255-272.

Kurtz, C. F., & Snowden, D.J. (2003). The new dynamics of strategy: Sensemaking in a complex and complicated world. *IBM Systems Journal* 42 (3).

Lacave, C., & Diez, F.J. (2002). A review of explanation methods for Bayesian networks. *Knowledge Engineering Review*, 17:107-127.

Larranaga, P., Karshenas, H., Bielza, C., & Santana, R. (2013). A review on evolutionary algorithms in Bayesian network learning and inference tasks. *Information Sciences*, vol. 233, pp. 109–125.

Lauritzen, S. L., & Spiegelhalter, D.J. (1988). Local computations with probabilities on graphical structures and their application to expert systems. *Journal of the Royal Statistical Society, Series B B 50* (2), 157–224.

Lave, J., & Wenger, E. (1991). *Situated learning: Legitimate peripheral participation.* Cambridge, UK: Cambridge University Press

Lebiere, C., Pirolli, P., Thomson, R., Paik, J., Rutledge-Taylor, M., Staszewski, J., & Anderson, J., (2013). A Functional Model of Sensemaking in a Neurocognitive Architecture. *Computational Intelligence and Neuroscience*; Special Issue on Neurocognitive Models of Sense Making

Leedom, D. K. (2004). *The Analytic Representation of Sensemaking and Knowledge Management within a Military C2 Organization*. Evidence Based Research, Inc., Vienna, Virginia.

Leedom, D.K., & Eggleston, R.G. (2005). The simulation of sensemaking and knowledge management within a joint effects-based planning system. *Proceedings of the Tenth International Command & Control Research & Technology Symposium* (CD ROM), McLean, VA.

Leedom, D.K. (2005). Our evolving definition of knowledge: Implications for C2ISR system performance assessment. *Proceedings for 10th International Command & Control Research and Technology Symposium.* McLean, VA.

Li, X., Liu, X., Dong, Z., & Li, K. (2010, July). Toward an agent-based model of tactical engagement. In *Advanced Management Science (ICAMS), 2010 IEEE International Conference on* (Vol. 3, pp. 218-223).

Lin, R., Galper, A., & Shachter, R. (1990). Abductive inference using probabilistic networks: Randomized search techniques. *Technical Report KSL-90-73,* Knowledge Systems Laboratory, Stanford.

Louis, M. R. (1980). Surprise and sensemaking: What newcomers experience in entering unfamiliar organizational settings. *Administrative Science Quarterly*, 25, 225-251.

Malhotra, Y. (2001). Expert systems for knowledge management: Crossing the chasm between information processing and sense making. *Expert Systems with Applications, 20, 7-16.*

McLaughlin, J., & Paté-Cornell, E. (2005). A Bayesian Approach to Iraq's Nuclear Weapon Program Intelligence: A Hypothetical Illustration. *Proceedings of the International Conference on Intelligence Analysis*. McLean, Virginia.

Mengshoel, O.J. (1999). *Efficient Bayesian Network Inference: Genetic Algorithms, Stochastic Local Search, and Abstraction*. PhD dissertation, Dept. of Computer Science, Univ. of Illinois at Urbana-Champaign.

Mengshoel, O.J., & Wilkins, D.C. (1998). Genetic algorithms for belief network inference: The role of scaling and niching. *Evolutionary Programming VII, Vol 1447*. Springer, pp 547-556.

Metz, S. (2003). Insurgency and Counterinsurgency in Iraq. *The Washington Quarterly*, 27:1, 25-36.

Milligan, J. R., & Ahmed, N.O. (2005). Decision-support Infosphere Services for Collaborative Operations and Virtual Environmental Requirements (DISCOVER). In *Proceedings of the Tenth International Command and Control Research and Technology Symposium*, McLean, VA.

Morrison, C. T., & Cohen, P.R. (2005). COLAB: *A Laboratory Environment for Studying Analyst Sensemaking and Collaboration*. Center for Research on Unexpected Events, USC Information Sciences Institute, Marina del Rey, California.

Munya, P., Trevino, M., & Ntuen, C. (2005).Design Principles for an automated Sensemaking Support System. *In the Proceedings of the IIE Annual Conference*. Atlanta, GA.

Munya, P., & Ntuen, C.A. (2007). Adaptive Information Fusion in Asymmetric Sensemaking Environment. In *Proceedings of the 12th International Command and Control Research and Technology Symposium*. Newport, RI.

Neapolitan, R.E. (2004). Learning Bayesian Networks. *Artificial Intelligence*. Prentice Hall, NJ

Nosek, J.T. (2005). Collaborative sensemaking support: progressing from portals and tools to collaboration envelopes™. *International Journal of e-Collaboration*, Vol 1.

Ntuen, C. (2006).Cognitive Constructs and the Sensemaking Process. In *Proceedings of the 2006 International Command and Control Research and Technology Symposium,* Cambridge, UK.

Ntuen, C.A (2008). The process of sensemaking in complex human endeavor. Proc. ICCRTS, Seattle, WA, June 17-19.

Ntuen, C. A. (2009). *Sensemaking as a naturalistic knowledge discovery tool.* Proceedings of NDM9, the 9th International Conference on Naturalistic Decision Making, London, UK.

Ntuen, C. A., Park, E. H., & Gwang-Myung, K. (2013). Designing an Information Visualization Tool for Sensemaking. *International Journal of Human-Computer Interaction*, Vol. 26(2), pp. 189 – 205.

Onisko, A. (2002). *Probabilistic Causal Models in Medicine: Applications to Diagnosis of Liver Disorders*, PhD Dissertation. Polish Academy of Science.

Onisko, A., Druzdzel, M. J., & Wasyluk, H. (2000).Learning Bayesian Network Parameters from Small Data Sets: Application of Noisy-OR Gates. Working Notes of the *Workshop on Bayesian and Causal Networks: From Inference to Data Mining, 12th European Conference on Artificial Intelligence* (ECAI-2000), Berlin, Germany.

Paté-Cornell, E. (2002). Fusion of Intelligence Information: a Bayesian Approach. *Risk Analysis* Vol.22, No. 3: 445-454.

Pearl, J. (1988). *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. Representation and Reasoning Series (2nd printing ed.). San Francisco, California: Morgan Kaufmann. ISBN 0-934613-73-7.

Peirce, C.S. (1877). *The Thought of C.S. Pierce*. Book by Thomas A. Goudge; University of Toronto Press.

Peng, Y., & Reggia, J.A. (1990). *Abductive Inference Models for Diagnostic Problem-Solving*. New York: Springer Verlag.

Pfeffer, A. (2000). Probabilistic Reasoning for Complex Systems. *PhD thesis*, Department of Computer Science, Stanford Univ.

Pirolli, P. & Card, S. (2005). The sensemaking process and leverage points for analyst technology as identified through cognitive task analysis. In *Proc. of the Inter. Conf. on Intelligence Analysis*.

Pirolli, P., & Card, S. K. (1999). Information Foraging. *Psychological Review, 106, 643-675*.

Pradhan, M., Provan, G. M., Middleton, B., & Henrion, M. (1994). Knowledge engineering for large belief networks. *Uncertainty in Artificial Intelligence: Proceedings of the Tenth Conference*, Seattle, WA, pp. 484–490.

Prakken, H. (2004). Analyzing reasoning about evidence with formal models of argumentation. *Law, Probability and Risk Vol 3*, 33-50.

Qu, Y. (2003). A sensemaking-supporting information gathering system. In *CHI '03 Extended Abstracts on Human Factors in Computing Systems*, Ft. Lauderdale, Florida, USA. ACM Press, New York, NY, 906-907.

Ring, P.S, & Rands, G.P. (1989). Sensemaking, understanding, and committing: Emergent interpersonal transaction processes in the evolution of 3M's microgravity research program. *Research in the management of innovation: The Minnesota studies*. A. H. Van de Ven, H. Angle and M. S. Poole (eds.), 337-366. New York: Ballinger/Harper.

Rojas-Guzman, C., & Kramer, M.A.(1993). GALGO: A Genetic ALGOrithm decision support tool for complex uncertain systems modeled with Bayesian belief networks. In *Proceedings* of *the Ninth Conference on Uncertainty in Artificial Intelligence,* pages 368-375, Washington, D.C.

Rojas-Guzman, C., & Kramer, M.A.(1996). An evolutionary computing approach to probabilistic reasoning on Bayesian networks. *Evolutionary Computation*, 4(1):57-85.

Rura-Polley, T., Hawryszkiewycz, I.T., & Baker, E. (2000). Facilitating sensemaking in knowledge integration within geographically dispersed cross-functional teams. *Challenges of Information Technology Management in the 21st Century. 2000 Information Resources Management Association International Conference*, p 1131-4

Russell, D. M., Stefik, M. J., Pirolli, P., & Card, S. K.(1993). The cost structure of sensemaking, *Proceedings of the SIGCHI conference on Human factors in computing systems*, p.269-276, April 24-29, 1993, Amsterdam, The Netherlands.

Russell, D.M., Slaney, M., Qu, Y., & Houston, M. (2005). A Cost Structure Analysis of Manual and Computer-supported Sensemaking Behavior. In *Proceedings of Intelligence Analysis*.

Russell, D. M. (2003). Learning to see, seeing to learn: Visual aspects of sensemaking. *Proceedings of SPIE - The International Society for Optical Engineering*, Vol 5007

Russell, D.M., & Slaney, M. (2004). Measuring the Tools and Behaviors of Sensemaking. Submitted to *CHI 2004.*

Russell, S.J., & Norvig, P. (2003). *Artificial Intelligence: A Modern Approach (2nd ed.)*, Upper Saddle River, New Jersey: Prentice Hall, ISBN 0-13-790395-2.

Ryan, A. (2008). About the Bears and the Bees: Adaptive Responses to Asymmetric Warfare. DSTO, Australia. *Interjournal*.

Sackman. S. (1991). *Cultural Knowledge in Organizations: Exploring the Collective Mind* Newbury Park, CA: Sage.

Santos, E., Jr. (2003). A cognitive architecture for adversary intent inferencing: Knowledge structure and computation. *Proceedings of the SPIE 17th Annual International Symposium on Aerospace/Defense Sensing and Controls*: *AeroSense 2003*, 182–193.

Santos, E., Jr., Shimony, S.E., & Williams, E. (1996). Sample and accumulate algorithms for belief updating in Bayes networks. In *Proceedings of the Twelfth Annual Conference on Uncertainty in Artificial Intelligence (UAI-96)*,pp 477-484, Portland, Oregon.

Sereno, B., Shum, S. B., & Motta, E. (2004*). ClaimSpotter: an Environment to Support Sensemaking with Knowledge Triples*. Knowledge Media Institute, The Open University, Milton Keynes, UK**.**

Shattuck, L.G., & Miller, N.L. (2004). A process tracing approach to the investigation of situated cognition. *Proceedings of the Human Factors and Ergonomics Society's 48th Annual Meeting*, New Orleans, LA.

Shimony, S.E. (1994). Finding MAPs for belief networks in NP-hard. *Artificial Intelligence 68 (2*), 399–410.

Starbuck, W., & Milliken, F. (1988). Executive perceptual filters: What they notice and how they make sense. In D. Hambrick (ed.) *The executive effect: Concepts and methods for studying top managers*: 35-65. Greenwich, CT: JAI Press

Sticha, P., Buede, D., & Rees, R. (2005). APOLLO: An Analytical Tool for Predicting a Subject's Decision-making. *Proceedings of the International Conference on Intelligence Analysis*. McLean, Virginia.

Su, X., Bai, P., Du, F., & Feng, Y. (2011). Application of Bayesian networks in situation assessment. In *Proceedings of ICICIS*, Part I (R. Chen, Editor). Berlin, Germany: Springer-Verlag, 643-648.

Suzic, R. (2003). Representation and recognition of uncertain enemy policies using statistical models. *In Proc. of the NATO RTO Symposium on Military Data and Information Fusion*, Prague, Czech Republic.

Thomas, J. B., Clark, S. M. & Gioia, D. A. (1993). Strategic Sensemaking and Organizational Performance: Linkages among Scanning, Interpretation, Action, and Outcomes. *Academy of Management Journal* 36 (2) 239-270.

Thoms, G.A., (2003). Situation awareness - a commander's view. In *Proceedings of the Sixth Inter- national Symposium on Information Fusion (Fusion 2003),* Cairns, Queensland, Australia.

Van Creveld, M. (1985). *Command in War*, Cambridge: Harvard University Press, 1985.

Weick, K. E. (1995). *Sensemaking in organizations*. Thousand Oaks, CA: Sage.

Welch, R.L. (1996). Real time estimation of Bayesian networks. In *Proceedings* of *the Twelfth Annual Conference on Uncertainty in Artificial Intelligence (UAI-96),*pp. 533-544.Morgan Kaufmann.

Wiig, K.M. (2003). A knowledge model for situation-handling. *Journal of Knowledge Management*, Vol 7, (5) .

Woodberry, O., Nicholson, A. E., Korb, K. B., & Pollino, C.A. (2004). Parameterizing Bayesian networks. In *Proceedings of the 17th Australian Joint Conference on Artificial intelligence*, Cairns, Australia, pp. 1101-1107.

Zagorecki, A., & Druzdzel, M. (2006). Probabilistic Independence of Causal Influences, in *Proceedings of the Third European Workshop on Probabilistic Graphical Models (PGM'06)*, Prague, Czech Republic, pp. 325-332.

Zagorecki, A., Voortman, M., & Druzdzel, M. J. (2006). Decomposing Local Probability Distributions in Bayesian Networks for Improved Inference and Parameter Learning. In *Proceedings of the 19th International Florida Artificial Intelligence Research Society Conference (FLAIRS 2006)*, Melbourne Beach, FL, pages 860-865.

Zhaoyu, L., & D'Ambrosio, B. (1993). An Efficient Approach for Finding the MPE in Belief Networks. In Heckerman, D., and Mamdani, A. (Eds.): *Uncertainty in Artificial Intelligence; Proceedings of the Ninth Conference*, Morgan Kaufmann, San Matteo, California.

Appendix A: Description of Insurgent Asymmetric Battlespace Variables

Node Name	Definition	States (Indicators)
Y_1	Resistance and liberation from foreign occupation.	y_{11}: Resistance and liberation- liberate the country or region from the militarily stronger occupation force by engaging in asymmetric warfare
		y_{12}: Law and order breakdown-Disruption of counterinsurgent control of the local security situation by limiting their ability for military maneuvers and restricting interaction with the population in stability and support operations.
		y_{13}: Control of the population- Discouraging the local population from cooperating with the counterinsurgents through instability, chaos, conflict and fear.
		y_{14}: Excessive force projection- provoking excessive raids by the counterinsurgent forces and use the second order effects of that action as a strategy for resistance
Y_2	Establishment of political infrastructure to legitimize the insurgency	y_{21}: Sectarian governance structures
		y_{22}: Fundamentalist insurgent ideology based on radical tenets
Y_3	Control of the political space by the insurgent force	y_{31}: Political opposition to the ruling regime
		y_{32}: Control of the security space
		y_{33}: Disruption of civic and governance processes
Y_4	Promotion of fundamentalist ideologies	y_{41}: Nationalism
		y_{42}: Sectarian and inter-faith conflicts by insurgent groups
		y_{43}: The conceptual Islamic state (Caliphate).
X_1	Ethnic and sectarian supremacy by the insurgent force	x_{11}: Sectarian identity and influence on insurgent mode of operation
		x_{12}: Use of fundamentalist ideologies such as *Salafism* as a motivating factor for some forms of battlespace operations
		x_{13}: Legitimacy of the Jihad-jihad used in the context of armed struggle against non-believers.
X_2	Disruption of the ability to carry out nation building and stability operations by the counterinsurgent forces	x_{21}: Local environment and feedback mechanisms
		x_{22}: Operational modularity-modular operations make it difficult for the rigid counterinsurgent Techniques, Tactics and Procedures

		x_{23}:Threat forces, criminal elements and part time forces
		x_{24}: Direct attacks on counterinsurgent forces to influence the perception of the population regarding capability
X_3	Exploiting the vulnerabilities in the counterinsurgent force structure	x_{31}: Unbounded battlespace- the forward edge of the battlespace is unbounded introducing a complexity that supports the insurgents asymmetrical tactics
		x_{32}:Techniques, tactics and procedures- coherent but highly dispersed and decentralized command and control structures
		x_{33}: Intelligence asymmetry- evolving new tactics that strain or defeat the counterinsurgent Intelligence, Surveillance and Reconnaissance (IS&R) assets.
M_1	Targeted assassinations and attacks on counterinsurgent forces and institutions	m_{11}: Security target engagement-attacks on military and security leaders considered hard targets.
		m_{12}: Political target engagement-attacks on government officials, political party leaders and religious leaders.
		m_{13}: Symbolic target engagement-Attacking symbolic or iconic targets that represent the best opportunities to achieve a desired reaction in the psychological target
M_2	Promotion of sectarian and religious violence	m_{21}: Civil war- Instability due to the second order effects of the sectarian and religious conflict
		m_{22}: Sanctuary cities- areas where the local population is sympathetic to and supportive of the insurgent objectives
		m_{23}: Civilian shelters- Insurgents shelter in mosques, shrines, and other high value targets as well as targets with high cultural impact.
		m_{24}: Information operations-use of mass media and internet to disseminate information quickly and polarize public opinion.
M_3	Undermining the formation of legitimate government structures	m_{31}: Armed militias- formation of militias by the insurgent groups tasked with the responsibility to provide protection to the population and ensure law and order in the regions controlled by insurgents

		m_{32}: Propaganda warfare- The process of democratization and nation building is portrayed as a project of the occupying force and its implementation as the root cause of violence
		m_{33}: Criminal networks- emergence of ungovernable areas outside the central government's control, smuggling networks, or tribal or sectarian based militias
M_4	Insurgent force projection of military capability	m_{41}: Counter maneuver- employing unconventional means and methods to prolonging the conflict through a low level war of attrition
		m_{42}: Foreign fighters- Linking national insurgencies a wider global conflict, pitting nation states against transnational insurgent-terrorist networks.
		m_{43}: Force structure- insurgent groups decentralize and compartmentalize to avoid presenting an easy massive strike target to the counterinsurgents.
		m_{44}: Informal networks- networks of informers and sources act as reliable sources of actionable intelligence on counterinsurgent maneuvers, targets and locations.
T_1	High level attrition attacks by Insurgents	t_{11}: Civilian suicide bombing- A high priority targeted action within the military structure of a number of organized insurgent groups.
		t_{12}: Remotely detonated IED- The massive casualty rate of this tactic makes it highly popular among insurgent groups.
		t_{13}: Rocket propelled grenades: non- line of sight munitions give insurgents the ability to attack undetected, a wide target selection and limited engagement with counterinsurgent force
T_2	Low level attrition attacks by insurgents	t_{21}: Small arms attacks- A combination of low intensity kinetic effects, kidnappings and executions, usually of high value targets
		t_{22}: Coercive threats- Threats against the population seen as cooperating with the counterinsurgent force.
		t_{23}: Convoy ambushes- guerilla type ambush and disperse attacks on soft units such as lightly armed logistics and personnel

		transport units
T_3	Critical infrastructure attacks by insurgents	t_{31}: Infrastructure sabotage- Sabotage of critical infrastructure to paralyze the operations of the government and disrupt counterinsurgent SASO operations.
		t_{32}: Arson- Burning of houses in residential neighborhoods in a form of "cleansing" operation. A tactic widely used especially in the Iraqi Insurgency

Appendix B: Correlation Analysis of the Posterior Distributions for the Variables of Figure 19

The SAS System

The CORR Procedure

4 Variables: m11 y11 x11 t32

Simple Statistics

Variable	N	Mean	Std Dev	Sum	Minimum	Maximum	Label
m11	7	0.51429	0.30237	3.60000	0.10000	0.90000	m11
y11	7	0.20143	0.00900	1.41000	0.19000	0.21000	y11
x11	7	0.42714	0.02928	2.99000	0.38000	0.46000	x11
t32	7	0.30429	0.00535	2.13000	0.30000	0.31000	t32

Pearson Correlation Coefficients, N = 7
Prob > |r| under H0: Rho=0

	m11	**y11**	**x11**	**t32**
m11	1.00000	0.97144	0.98438	0.88388
m11		0.0003	<.0001	0.0083
y11	0.97144	1.00000	0.96715	0.89113
y11	0.0003		0.0004	0.0071
x11	0.98438	0.96715	1.00000	0.83680
x11	<.0001	0.0004		0.0189
t32	0.88388	0.89113	0.83680	1.00000
t32	0.0083	0.0071	0.0189	

Appendix C: Correlation Analysis of the Posterior Distributions for the Variables of Figure 20

The SAS System

The CORR Procedure

4 Variables: x33 y22 m11 t21

Simple Statistics

Variable	N	Mean	Std Dev	Sum	Minimum	Maximum	Label
x33	7	0.51429	0.30237	3.60000	0.10000	0.90000	x33
y22	7	0.39857	0.00378	2.79000	0.39000	0.40000	y22
m11	7	0.45286	0.09394	3.17000	0.35000	0.60000	m11
t21	7	0.40429	0.00787	2.83000	0.39000	0.41000	t21

Pearson Correlation Coefficients, N = 7
Prob > |r| under H0: Rho=0

	x33	**y22**	**m11**	**t21**
x33	1.00000	-0.56250	-0.98748	-0.87070
x33		0.1887	<.0001	0.0108
y22	-0.56250	1.00000	0.48284	0.80064
y22	0.1887		0.2724	0.0305
m11	-0.98748	0.48284	1.00000	0.79249
m11	<.0001	0.2724		0.0336
t21	-0.87070	0.80064	0.79249	1.00000
t21	0.0108	0.0305	0.0336	

Appendix D: Correlation Analysis of the Posterior Distributions for the Variables of Figure 21

The SAS System

The CORR Procedure

4 Variables: t32 x22 y41 m23

Simple Statistics

Variable	N	Mean	Std Dev	Sum	Minimum	Maximum	Label
t32	7	0.51429	0.30237	3.60000	0.10000	0.90000	t32
x22	7	0.39714	0.00756	2.78000	0.39000	0.41000	x22
y41	7	0.30000	0	2.10000	0.30000	0.30000	y41
m23	7	0.27000	0.00577	1.89000	0.26000	0.28000	m23

Pearson Correlation Coefficients, N = 7
Prob > |r| under H0: Rho=0

	t32	x22	y41	m23
t32	1.00000	-0.92708	.	0.76376
t32		0.0027	.	0.0457
x22	-0.92708	1.00000	.	-0.76376
x22	0.0027		.	0.0457
y41	.	.	.	.
y41	.	.	.	.
m23	0.76376	-0.76376	.	1.00000
m23	0.0457	0.0457	.	