A BAYESIAN ABDUCTION MODEL FOR EXTRACTING THE MOST PROBABLE EVIDENCE TO SUPPORT SENSEMAKING

Paul Munya[1]and Celestine A. Ntuen[2] , Eui H. Park[2] and Jung H. Kim[3]

[1] Army Research Laboratory, Warren, Michigan, USA
[2]Department of Industrial & Systems Engineering,
[3]Department of Computer Science & Engineering,
North Carolina A &T State University, North Carolina, USA

ABSTRACT

In this paper, we discuss the development of a Bayesian Abduction Model of Sensemaking Support (BAMSS) as a tool for information fusion to support prospective sensemaking. Currently, BAMSS can identify the Most Probable Explanation from a Bayesian Belief Network (BBN) and extract the prevalent conditional probability values to help the sensemaking analysts to understand the cause-effect of the adversary information. Actual vignettes from databases of modern insurgencies and asymmetry warfare are used to validate the performance of BAMSS. BAMSS computes the posterior probability of the network edges and performs information fusion using a clustering algorithm. In the model, the friendly force commander uses the adversary information to prospectively make sense of the enemy's intent. Sensitivity analyses were used to confirm the robustness of BAMSS in generating the Most Probable Explanations from a BBN through abductive inference. The simulation results demonstrate the utility of BAMSS as a computational tool to support sense making.

KEYWORDS

Abduction inference, Bayesian Belief Networks, Most Probable Explanation (MPE), Information fusion

1. INTRODUCTION

A great deal of research is currently being conducted in the fields of information fusion and data fusion. The impetus for this research is the growing need for a system or systems capable of integrating many pieces and forms of information and providing a coherent interpretable output. Real world situations are often characterized by a large number of complex and uncertain events. These events generate uncertain information at different levels of abstraction linked together only by cause and effect. The challenge is how to effectively and efficiently represent, fuse and interpret such information to provide a useful output. To address this challenge, we consider the use of the cognitive process of sensemaking to support information fusion in such dynamic and uncertain situations. We know, apriori, that information from the senses is always fused and analyzed to develop a mental model or "common picture" that informs our daily decision making process and increases our chances of survival. To emulate this ability, we analyze the problem of multisensory data and information fusion as a sensemaking problem. We do this by decomposing the sensemaking process into its cognitive primitives of synthesis, reasoning and inference and reconstructing each primitive using computational methods.

Sensemaking involves putting stimuli into some kind of framework [1]. Sensemaking is also viewed as a thinking process that uses retrospective accounts to explain surprises [2] a reciprocal interaction of information seeking, meaning ascription and action [3] and an interpretive process

DOI : 10.5121/ijaia.2015.6101

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" [4]. In [5] sensemaking is defined as "a process in which individuals develop cognitive maps of their environments".

In the military domain, sensemaking has been studied as a multidimensional process of developing an operational understanding and awareness within a complex and evolving task domain [6], [7], [8]. In asymmetric warfare for example, the adversaries evolve with different kinds of motivations and tactics. This introduces a level of complexity into the battle space information management that requires a military strategist to adopt new and novel ways of information handling and analysis. For instance, the commander must make sense of the evolving information through convoluted processes of hypotheses formulations, evidence collection and associations to the hypotheses, and gaining an understanding of the situation. As noted in [9], the commander must draw inferences from uncertain data, identify appropriate sequences of objectives and optimally assign resources to ensure their attainment. Making sense of dynamic multivariate information in order to establish a reasonable justifiable belief about the adversary's intent is the core of the sense making process [10].

Sensemaking of battlefield information is difficult for the following reasons: a) As asymmetric information, it is generally characterized by equivocation, different types of uncertainties, ambiguities, surprises, emerging and evolving features, and complexity; b) There is a problem of scale due to the military command hierarchy. The spiral nature of information transactions, processes, and feedback makes any closed-form analytical model difficult to apply in the sensemaking process and c) There is currently a lack of cognitive architectures that support the ability to integrate information for real-time sensemaking. Given the above challenges, this paper develops a Bayesian Abduction Model for Sensemaking Support (BAMSS). The BAMSS uses a classical Bayesian information fusion with cluster analytic algorithm to extract probable evidence from an adversary network. By populating the adversary network with the initial probability of evidence, the algorithm in BAMSS computes the posterior probabilities which represent the informational variables supporting specific sets of hypotheses in the network. The BAMSS is used to find a unique Most Probable Explanation (MPE) supporting a set of hypotheses.

2. BAYESIAN NETWORKS

A Bayesian network (BN) is a graphical model that encodes probabilistic relationships among variables within a context of interest. Variations of Bayesian networks developed in [11] have been used in many disciplines such as in medical diagnosis [12] and sensor data fusion [13] Dynamic Bayesian networks which are time dependent, have been used for military plan recognition [14], tactical engagement planning [15], prediction of enemy tactical intents [16], representing knowledge about the enemy beliefs [17], and updating uncertainties about changes in battlefield information [18]. In [19] BNs were used to develop an adversary model that captures goals, intentions, biases, beliefs and perceptions based on social cognition constructs.

Computer modeling and simulation of Bayesian networks has become robust and flexible in application to decision support systems. The models developed have some important roles to play in sensemaking. Examples include the framework for computational adversarial modeling and information systems [20], Center of Gravity Network Effects Tool (COGNET) [21], a dynamic Bayesian net for causal relationship between lower-level friendly tasks and higher-level effects on adversary systems [22] and tactical situation analysis [23]. In [24] Bayesian techniques were used to provide an analytical illustration of Iraq's nuclear program intelligence.

These researchers have focused mainly on the normative-deductive approach to decision making using Bayesian formalism. However, normative-deductive inference is more suitable to deterministic algorithms and fails to make efficient use of the expressive power of Bayesian networks. Deterministic algorithms do not perform optimally in complex and uncertain information environments such as the asymmetric battlefield.

The structure of this paper is as follows: Section 3 will describe Bayesian modeling and abductive inference applied in developing the framework for a computational sensemaking model as well as the prototype model development. Section 4 describes the experimental analysis of the model using vignettes that represent sensemaking tasks in asymmetric warfare domain. We discuss the experimental simulation results and the validation of the model in Section 5 and conclusions and opportunities for further research in the last section.

3. BAYESIAN BELIEF NETWORKS AND ABDUCTIVE INFERENCE

A Bayesian Belief Network (BBN) also referred to as a probabilistic 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 [11]. 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 [25]. 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

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

Where Π_{Xi} represents the parent variables of X_i.

An advantage of a 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 [26]; this is the core of a BN analysis.

Abduction in belief networks refers to inference from effects to the best explanations of the effects [27]. Based on the assumption that there is a causal model, an explanation is a configuration of the unobserved variables. The inference process is aimed at obtaining the MPE or the kMPEs, where k represents the selected best hypotheses in the network confirmed by the respective network pathways. In general, the variables that take the value “present” or “positive” in the MPE are considered the causes that explain the evidence. The 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 extracted from symptoms, signs, and test results.

Abduction intends to find the MPE with the configuration $\boldsymbol{w}$ having the maximum a-posteriori probability $P(\boldsymbol{w}|\boldsymbol{e})$,where $\boldsymbol{e}$is the available evidence. When $\boldsymbol{W}$ includes all the unobserved variables, the process is known as total abduction; else, it is partial abduction. In general, given an observation $\boldsymbol{o}$**,** a hypothesis $\boldsymbol{h}$ and the knowledge that $\boldsymbol{h}$ causes $\boldsymbol{o}$, it is an abduction to hypothesize that $\boldsymbol{h}$ occurred. Abduction tries to synthesize a composite hypothesis explaining the entire observation from elementary hypotheses [28].

We define Bayesian abductive inference for two instances of sensemaking: prospective (or predictive) sensemaking and retrospective sensemaking. For a prospective sensemaking we define a model of recursive Bayesian learning with data updates using the established procedure in [11]. Let H denote a hypothesis, $d = d_1, d_2,..d_n$ denote a sequence of data observed in the past, and d

denote a new datum. A method to calculate the belief in $H,P(H|d_n, d)$ is 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 $d_n+1=\{d_n,d\}$. Once $P(H|d_n)$ is computed, the past data is discarded and the posterior is computed as

$$P(H \mid d_n, d) = P(H \mid d_n)\frac{P(d \mid d_n, H)}{P(d \mid d_n)} \tag{2}$$

Comparing equations (1) and (2), 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 beliefs; it completely summarizes the past experience. The updating needs 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.

For retrospective sensemaking, let H represent a set of hypotheses H_i, each of which is equally likely. Let D_k represent a multi-valued evidence variable or datum - that is, the datum consists of k possible values each of which may or may not support the hypotheses. We can modify the model in [11] 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 $M_{kij} = P(d_{kj}|H_i)$. Then,

$$P(H_i \mid d_1,...,d_N) = \alpha P(H_i)[\prod_{k=1}^{N} P(d_k \mid H_i)] \tag{3}$$

Where α is the weighted value that scales the probability function on the left of equation 3 so that the total probability in the observation space is equal to one.

In sensemaking analytics, belief updating per equations (2) and (3) 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 could be fairly certain that this is a civil unrest and avoid sending in a suppressive force. If in the next instance a routine patrol in the same area of unrest comes under sustained fire, then the probability of civil unrest is lowered and his belief is updated. The hypothesis "insurgent attack" gets more support and the probability density function over the hypothesis space changes.

3.1. INFERENCE ALGORITHM IN BAMSS

Bayesian inference is a technique of inference in which Bayes' rule is used to update the probability estimate for a hypothesis as additional evidence is acquired. Usually, a posterior probability is inferred given the observation of new data or evidence. In BAMSS, a naïve clustering technique is used to support the inference through a multiple-value classification method [29].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. A message parsing propagation is done over the clique tree. By transmitting information between the variables in the local clique rather than the full joint probability, an efficient inference algorithm is realized. The choice of the algorithm is based on the requirements for exact and efficient solution using BAMSS. These requirements are discussed in [29] for a hierarchical Bayesian network and consist of:

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 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 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 BAMSS algorithm is a hierarchical, top-down process. It starts by randomly selecting a set of hypotheses nodes as the initial state variables. The current state consists of the parent nodes. The posterior probabilities of all the children nodes conditional on the set of parent nodes are then computed. 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. The evidence variables are informational variables since they reveal information about hypothesis variables. The process of information fusion in the BBN is accomplished by clustering the variables based on robust statistical properties such as distance metric or standard deviations from normed means. The pseudo code for BAMSS inference algorithm is shown in Figure 1.

```
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 1.Bayesian inference algorithm for BAMSS

3.2. SOFTWARE REQUIREMENTS FOR BAMSS IMPLEMENTATION

The BAMSS environment uses Open Source software which is freely available under the General Public License. It consists of three modules: a network module, a computational module and a graphical user interface (GUI). The modular architecture and the open source implementation ensure that the model can be modified with additional modules developed to address new challenges. The network module uses the existing GeNIe (graphical network interface) library from the Decision Systems Laboratory of the University of Pittsburgh [30]. GeNIe allows the user to develop a Bayesian network representation of the problem domain. The computational model takes the input data from the network and performs belief updating and abductive inference using the cluster algorithm described in [29]. The GUI helps to integrate 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 hypothesis variables or the target variables. The GUI for the computational module is a standalone application to be hosted on the client PC and runs on a Windows or Linux Operating System.

The representation of information flow in the BAMSS model is shown in Figure 2. Initially, a user defined domain specific BBN is created and loaded into the model from file or any other linked database. The problem definition is undertaken in the network module during the development of the Belief Network.

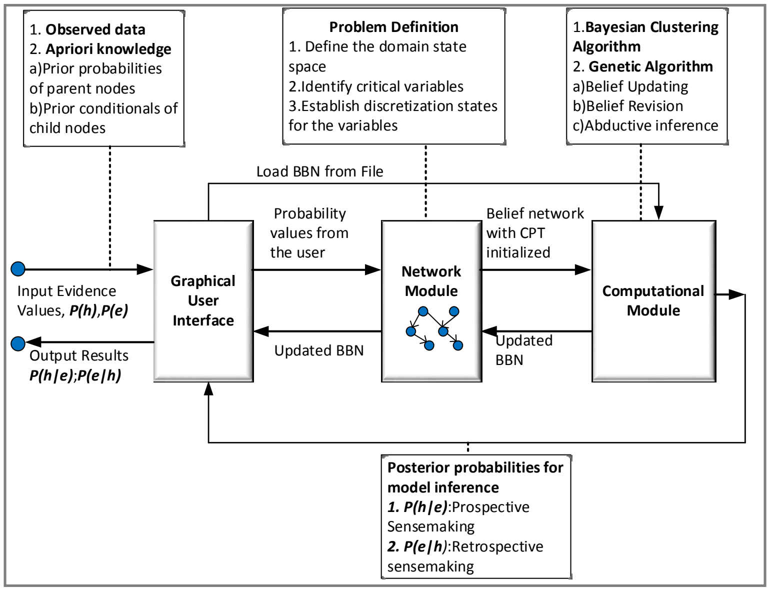

1. Observed data
2. Apriori knowledge
a)Prior probabilities of parent nodes
b)Prior conditionals of child nodes
Problem Definition
1. Define the domain state space
2.Identify critical variables
3.Establish discretization states for the variables
1.Bayesian Clustering Algorithm
2. Genetic Algorithm
a)Belief Updating
b)Belief Revision
c)Abductive inference
Load BBN from File
Probability values from the user
Belief network with CPT initialized
Input Evidence Values, P(h),P(e)
Graphical User Interface
Network Module
Computational Module
Output Results P(h|e);P(e|h)
Updated BBN
Updated BBN
Posterior probabilities for model inference
1. P(h|e):Prospective Sensemaking
2. P(e|h):Retrospective sensemaking

Figure 2.Information flow architecture in BAMSS

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 user defines the hypothesis variables, the evidence variables and the target variables of interest using the created network. A fully defined BBN with a conditional probability distribution values is then loaded into the model through the GUI data acquisition function. Once 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 conditional probability tables (CPTs) is then loaded into the computational module.

The computational module is responsible for making inference. The inference engine model performs the tasks of network belief updating, belief revision and the abductive inference. The results of the computations are received as output by the user for visualization through the GUI and comprise of a text 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. The computed updated beliefs form the prior probabilities for the network when the new evidence is introduced.

Figure 3 shows the system software architecture and components of BAMSS. The Structural Modeling, Inference and Learning Engine (SMILE) library of C++ classes [30] 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.

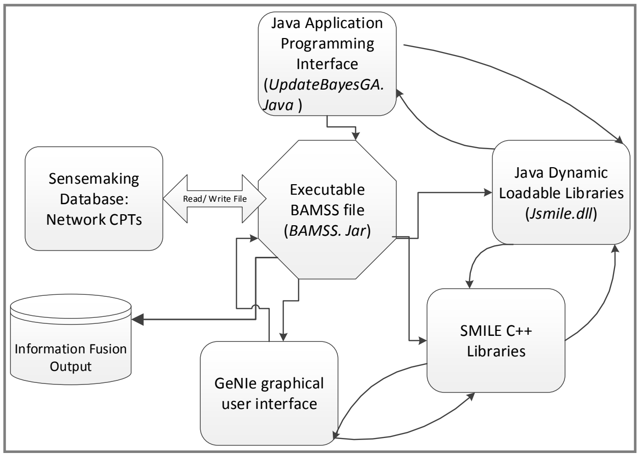

Java Application Programming Interface (UpdateBayesGA. Java)
Sensemaking Database: Network CPTs
Read/ Write File
Executable BAMSS file (BAMSS. Jar)
Java Dynamic Loadable Libraries (Jsmile.dll)
Information Fusion Output
SMILE C++ Libraries
GeNIe graphical user interface

Figure 3:BAMSS software architecture and components

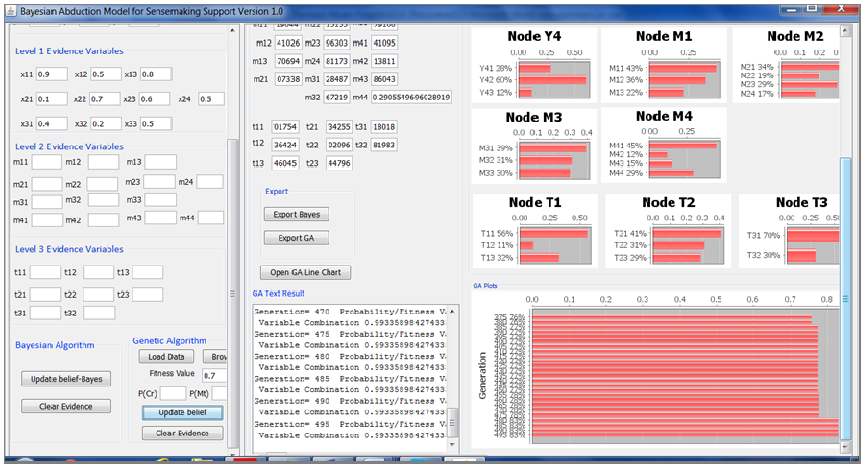
The executable *BAMSS.jar* is called by the user through a simple GUI command line. The *.dll* file interacts with the executable file in a read/write mode as shown in Figure 3. The network module is created through the GeNIe graphical user interface. GeNIe is accessed through a web browser on the client 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.

The BAMSS interface 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 is a repository of conditional probability tables that represent the knowledge base of 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.

3.3.BAMSS GRAPHICAL USER INTERFACE

Figure 4 shows a screen capture of the GUI for the BAMSS model. In the first operation, the domain specific BBN from a file residing on the client computer is loaded into the module.



x11 0.9 x12 0.5 x13 0.8
x21 0.1 x22 0.7 x23 0.6 x24 0.5
x31 0.4 x32 0.2 x33 0.5

m11 m12 m13
m21 m22 m23 m24
m31 m32 m33
m41 m42 m43 m44

t11 t12 t13
t21 t22 t23
t31 t32

Fitness Value 0.7
P(Cr) P(Mt)

m12 41026 m23 96303 m41 41095
m13 70694 m24 81173 m42 13811
m21 07338 m31 28487 m43 86043
m32 67219 m44 0.2905549696028919

t11 01754 t21 34255 t31 18018
t12 36424 t22 02096 t32 81983
t13 46045 t23 44796

```
Generation= 470  Probability/Fitness V.
 Variable Combination 0.99335898427433
Generation= 475  Probability/Fitness V.
 Variable Combination 0.99335898427433
Generation= 480  Probability/Fitness V.
 Variable Combination 0.99335898427433
Generation= 485  Probability/Fitness V.
 Variable Combination 0.99335898427433
Generation= 490  Probability/Fitness V.
 Variable Combination 0.99335898427433
Generation= 495  Probability/Fitness V.
 Variable Combination 0.99335898427433
```

Y41 28% Y42 60% Y43 12%
M11 43% M12 36% M13 22%
M21 34% M22 19% M23 29% M24 17%
M31 39% M32 31% M33 30%
M41 45% M42 12% M43 15% M44 29%
T11 56% T12 11% T13 32%
T21 41% T22 31% T23 29%
T31 70% T32 30%

Figure 4: A screen capture of the BAMSS graphical user interface

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 is 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 1 containing fields for hypothesis variables, followed by fields for Level 2 evidence variables, Level 3 evidence variables and so on. The user can input the evidence for a single variable or can select multiple variables on different levels.

To perform a 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 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 Genetic Algorithm is reserved for another analysis under investigation to optimize BAMSS inference search space [31]. The second and third quadrants show the results of the belief updating process for the selected algorithm both textually and graphically. 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. EXPERIMENTAL ANALYSIS

4.1. DATA ACQUISITION

The data used for BAMSS validation were sampled from two open public domain sources: a) The RAND Database of Worldwide (RDWTI), available at http://www.rand.org(web accessed on 12/16/2013). The RDWTI is a compilation of data from 1968 through 2009 and is free and publically accessible for research and analysis and b) 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). GTD provides the apriori data for the belief network. Information from the databases was based on the proportion (percentage) of occurrences. Where appropriately defined, these data provided the initial prior probabilities. The data contain information on the most recent conflicts on 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). Table 1 gives some sample data.

Table 1. 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 %
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 %
Hijacking	2	0.02 %
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 %

4.2. BAYESIAN NETWORK DEVELOPMENT

The network development follows the top-down military information hierarchy defined at four levels: strategic effect-, political operational-, military operational- and tactical- levels, respectively. Figure 5 is used to show the network topology. The network is based on the friendly force commander's perception of the adversary intent.

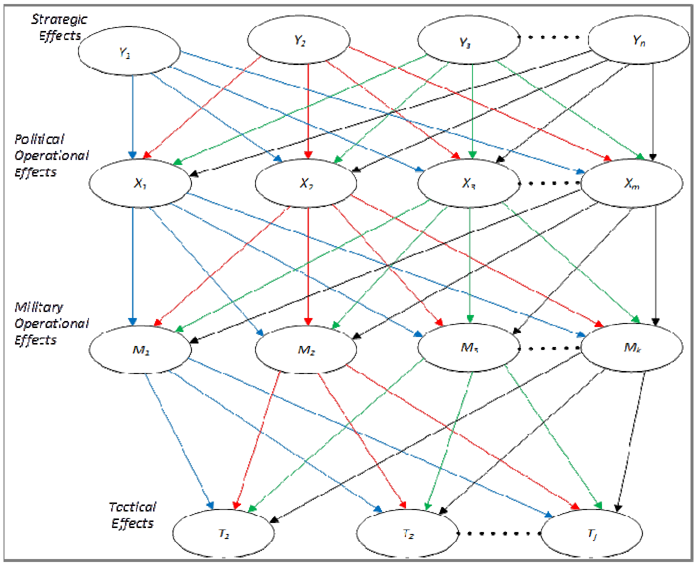


Figure 5. A Bayesian network topology representation of the adversary intent

The first level variables are for Strategic Effects. These are a set of 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 inform the commander of the adversary's strategies and are key to effective courses of action (COA) planning. The variable set is $\boldsymbol{Y}= \{Y_1, Y_2,\ldots Y_n\}$. Strategic effects are directly influenced by Political Operational Effects defined at Level 2. The variable set is $\boldsymbol{X} = \{X_1, X_{2,}\ldots X_m\}$ which represent evidence variables for $\boldsymbol{Y}$; $\boldsymbol{Y}$ is the set of parent nodes and $\boldsymbol{X}$ is the set of children nodes. These are informational variables that represent the Political, Military, Economic, Social, Information and Infrastructural (PMESII) state variables of the battlespace.

Level 3 is the Military Operational Effects. These are the informational variables that the adversary will exploit to destabilize the PMESII factors and is represented by $\boldsymbol{M}= \{M_1, M_2,\ldots M_p\}$.The vector M has a set of nodes whose parents are from $\boldsymbol{X}$ nodes. The friendly force commanders and their staffs would need to analyze these effects to correctly infer the desired end state of adversary. At this level, the adversary aims are to generate and exploit fine scale complexity and will seek to prevent the counterinsurgents from acting at the scale they are organized for [32].Level 4 is the Tactical effects which are evidence variables with direct causal linkages to the $\boldsymbol{M}$ nodes. These effects represent actions taken by the insurgents to influence certain outcomes in the battlespace. Depending on the choice of targets, the range of Tactical

Effects may be quite extensive and diverse. Most of these effects are kinetic and their strategic outcome is usually second order, not necessarily a direct one. These target variables are denoted as $\boldsymbol{T} = \{T_1, T_2,\ldots,T_r\}$.

Figure 6 shows the Bayesian network equivalent of Figure 5 with the real factors and nomenclatures used by the military. Here we have: $\boldsymbol{Y} = \{Y_1, Y_2, Y_3, Y_4\}$, $\boldsymbol{X} = \{X_1, X_2, X_3\}$,$\boldsymbol{M} = \{M_1, M_2, M_3, M_4\}$, and $\boldsymbol{T} = \{T_1, T_2, T_3\}$. This gives a network of size 4*3*4*3 =144 arrangements. Note that the size increases depending on the indicator variables of each node in the network. The variables in the network are discretized into nonnumeric sub factors so as to use the exact search algorithm implemented in BAMSS. The discretization is based on factors from the expert judgment. The states of each node in the network are subfactors representing all the possible indicators each variable can take within the domain state space. With the network topology defined and all the variables discretized, its parameters can be fully specified. Network parameterization was accomplished 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.

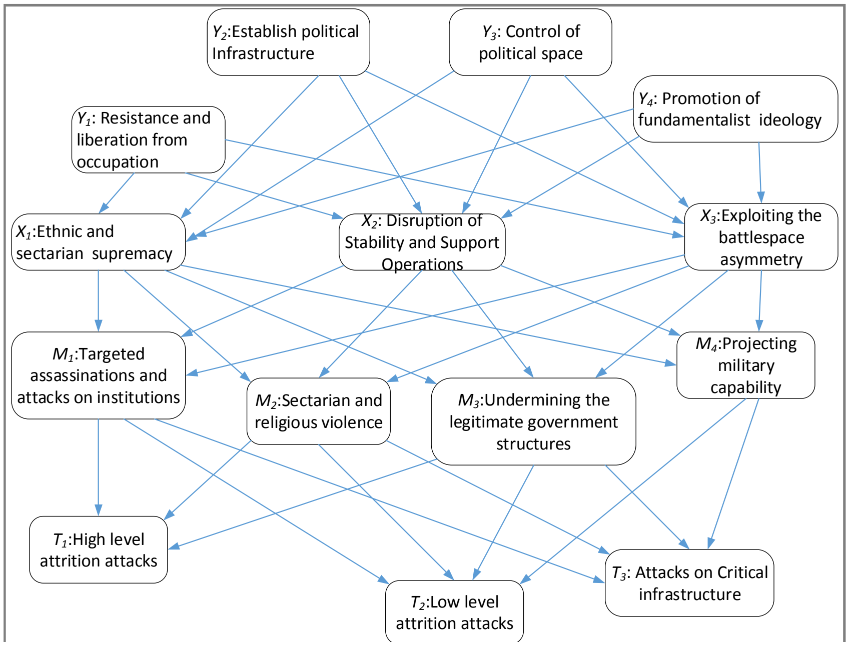
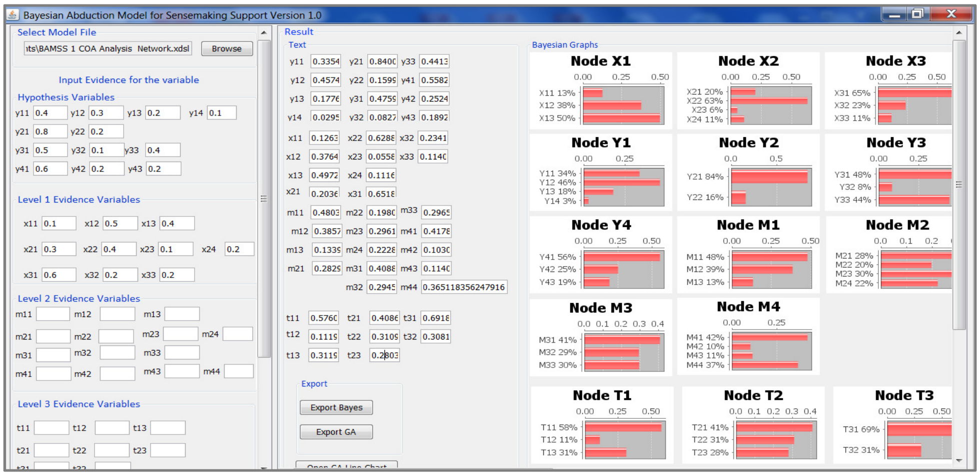

Y_2:Establish political Infrastructure
Y_3: Control of political space
Y_4: Promotion of fundamentalist ideology
Y_1: Resistance and liberation from occupation
X_1:Ethnic and sectarian supremacy
X_2: Disruption of Stability and Support Operations
X_3:Exploiting the battlespace asymmetry
M_1:Targeted assassinations and attacks on institutions
M_4:Projecting military capability
M_2:Sectarian and religious violence
M_3:Undermining the legitimate government structures
T_1:High level attrition attacks
T_3: Attacks on Critical infrastructure
T_2:Low level attrition attacks

Figure 6: A BAMSS network with decision variables

4.3. The simulation experiments

Simulation experiments were conducted using the sample historical data discussed earlier and summarized in Table 1. The data were presented to the BAMSS model using the GUI below in Figure 7. A node in the network was randomly selected and used as an input node for new evidence introduced into the model. With the input evidence varied 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.

Belief update was undertaken after CPT computation and the resultant posterior probabilities for all the nodes were displayed. Figure 7 shows this in a forward inference scheme. The output displayed on the right side of the GUI is both graphical and textual. For instance, given the hypotheses set $\boldsymbol{Y} = \{Y_1, Y_2, Y_3, Y_4\}$, 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.



Bayesian Abduction Model for Sensemaking Support Version 1.0

Select Model File

its\BAMSS 1 COA Analysis Network.xdsl

Input Evidence for the variable

Hypothesis Variables

y11 0.4 y12 0.3 y13 0.2 y14 0.1
y21 0.8 y22 0.2
y31 0.5 y32 0.1 y33 0.4
y41 0.6 y42 0.2 y43 0.2

Level 1 Evidence Variables

x11 0.1 x12 0.5 x13 0.4
x21 0.3 x22 0.4 x23 0.1 x24 0.2
x31 0.6 x32 0.2 x33 0.2

Level 2 Evidence Variables

m11 m12 m13
m21 m22 m23 m24
m31 m32 m33
m41 m42 m43 m44

Level 3 Evidence Variables

t11 t12 t13
t21 t22 t23

Result

Text

y11 0.3354 y21 0.840(y33 0.441
y12 0.4574 y22 0.1599 y41 0.5582
y13 0.1776 y31 0.4759 y42 0.2524
y14 0.0295 y32 0.0827 y43 0.1892
x11 0.1263 x22 0.6288 x32 0.2341
x12 0.3764 x23 0.0558 x33 0.1140
x13 0.4972 x24 0.1116
x21 0.2036 x31 0.6518
m11 0.4803 m22 0.1980 m33 0.2965
m12 0.3857 m23 0.2961 m41 0.4178
m13 0.1339 m24 0.2228 m42 0.1030
m21 0.2829 m31 0.4088 m43 0.1140
m32 0.2945 m44 0.365118356247916
t11 0.5760 t21 0.4086 t31 0.6918
t12 0.1119 t22 0.3109 t32 0.3081
t13 0.3119 t23 0.2803

Export

Bayesian Graphs

Figure 7.Belief updating (posterior probabilities) of the nodes in the network after new evidence is introduced

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 ($y_{41} = 0.6$, $y_{42} = 0.2$, $y_{43} = 0.2$) are similarly defined.

Next, we input the evidence values for Level 1 evidence variables, the Political OperationalEffectsX_1, $X_2$and X_3. This is evidence that is obtainable by direct observation of battlefield conditions or by analyzing sensor data and other information from various sources as summarized in Table 1. For example, 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 $X_1 = x_{13} = 0.4$. For illustration purposes, the following assumptions can be further made: 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 Levels 2 and 3.

5. Experimental results and model validation

5.1. Conditional posterior distributions

The right hand side of Figure 7 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 are: 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, the posterior probabilities are: y_{21}= 0.840, 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 Level 2 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 Level 3 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].The posterior distribution results for the Level 4 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. The posterior probability of each state of variable (textual result) is displayed by a bar chart under the variable node in Figure 7.

5.2. Parent and child node analysis

The posterior distribution for the selected network variables based on cause-effect (parent-child) relationships are shown in Tables 2-4 and the results are plotted against the probability of evidence of selected input variables (Figures 8-10).

Table 2: Belief Update in 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 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 *Security Target Engagement*. Figure 8 shows the posterior probability distribution of nodes after seven simulation runs.

By examining the evidence propagation in the first vignette, 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 implies that the causal effect of this variable is limited hence does not carry much weight as a course of action. The probability that the *Insurgent security Target Engagement* as a mode of operation is influenced by *Sectarian Identity* ($X_1 = x_{11}$) decreased from 50% to 30%. This implies that operations against security personnel cannot be attributed to a particular group. In fact focusing on the sectarian identity of the group is detrimental to the course of action selection because of the correlation factor (r =0.984) and this effect could be discarded. Probability of (*Infrastructure Sabotage*| *Insurgent Security Target Engagement*) increased from 20% to 40%. An increase in infrastructure sabotage could be regarded as 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 could require the commander to increase protection for critical infrastructure and security targets.

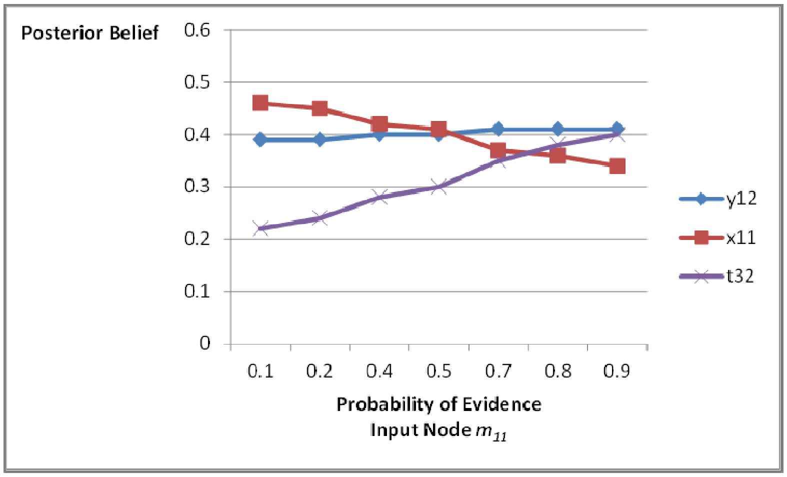


Figure 8.Belief revision in nodes $Y_1 = y_{11}$, $X_1 = x_{11}$ and $T_3 = t_{32}$ after new evidence is introduced in node $M_1 = m_{11.}$

For the second sensemaking vignette, the hypothesis variable was selected as $Y_2 = y_{22}$ (*Insurgent Ideology)* and the informational variables were $M_1 = m_{11}$(*Security Target Engagement*) and $T_2 = t_{21}$ (*Small Arms Attacks*). New evidence was introduced in node $X_3 = x_{33}$*(Intelligence Asymmetry).* Table 3 and Figure 9 show the posterior probability distributions of the variables after 7 simulation runs. 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 implies that better intelligence by the insurgent group may not directly influence this mode of operation. The 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 are inadmissible as COA.

Table 3. Belief Update in 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

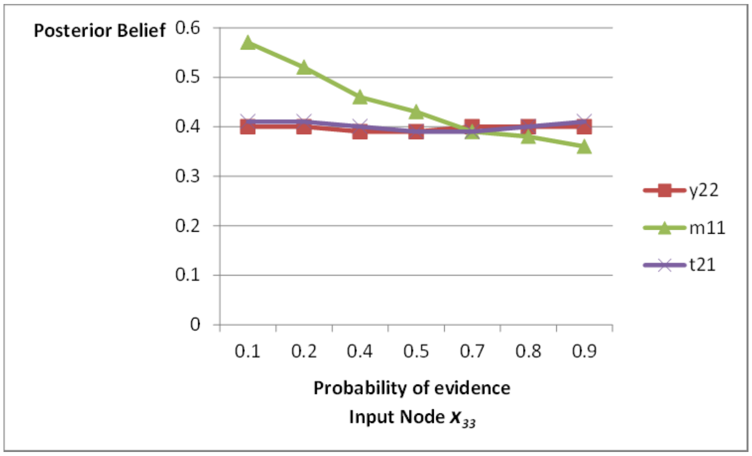


Figure 9. Belief revision in nodes $Y_2 = y_{22}$, $M_1 = m_{11}$ and $T_2 = t_{21}$ after new evidence is introduced in node $X_3 = x_{33}$

In the last vignette, we considered the hypothesis variable Y_4= y_{41} (*Nationalism*). For informational variables we set X_2 = x_{22} (*Modular Operations*) and M_2= m_{23} (*Civilian Shelters*). New evidence was introduced into variable T_3= t_{32} (*Arson*). Table 4 and Figure 10 show the posterior probability distributions. 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 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. *P*(*Insurgent Modular Operations*|*Arson*) and *P*(*Civilian Shelters*| *Arson*) are not admissible for COA analysis.

Table 4. Belief Update in the 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

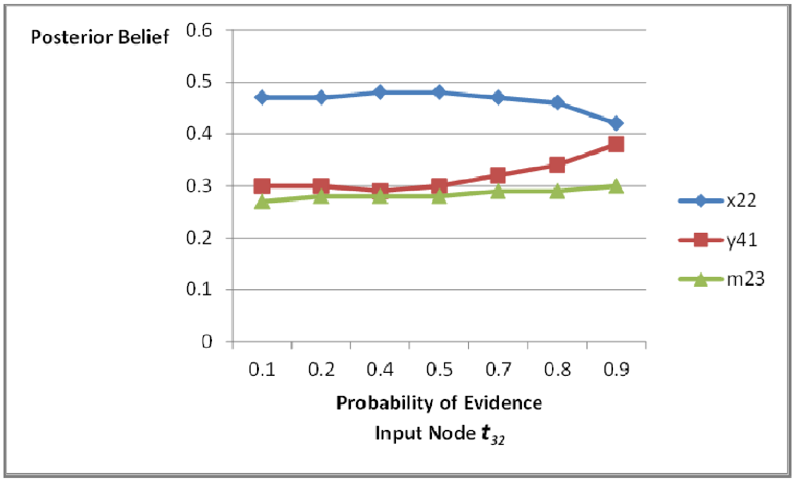


Figure 10.Belief revision in nodes $X_2 = x_{22}$, $Y_4 = y_{41}$and $M_2 = m_{23}$after new evidence is introduced in node $T_3 = t_{32}$

5.3. Discussion

The probability distributions for Strategic Effects provide an insight into the end state of the adversary. 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. The probability distributions for Tactical Effects provide inference into the actual methods, techniques, tactics and procedures that the adversary may employ to attack selected targets. By performing inference at this level, an analyst can reasonably draw conclusions about both the adversary intents and use the information for courses of action analysis as shown in Table 5 below. Results from sensitivity analysis on the experiments reported above are shown in Table 6.

Table 5. 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 (same)	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)	Decline from 50 to 30	Not supported	Operations against coalition security targets cannot be attributed to a particular group
P(Infrastructure Sabotage| Insurgent Security Target Engagement)	Increase from 20 to 40	Weakly supported	Increase in infrastructure sabotage by the insurgents may be a second order effect of targeting security because of the security gaps created.
P(Insurgent Security Target	Decline from	Strongly	Insurgents may be using the

Engagement| Intelligence Asymmetry)	60 to 35	supported	intelligence advantage to select soft targets and avoid the hard security targets
P(Small Arms Attacks| Intelligence Asymmetry)	40 (same)	Not admissible	The inferential condition is incompatible with the hypothesis
P(Insurgent ideology| Intelligence Asymmetry)	40 (same)	Not admissible	The inferential condition is incompatible with the hypothesis
P(Insurgent Modular Operations| Arson)	Decline from 50 to 40	Weakly supported	Consider incidents of arson as effects of operational modularity by the insurgents.
P(Nationalism|Arson)	Increase from 30 to 40	Strongly supported	Insurgent tactics using arson has some effect on nationalistic feeling by the local population.
P(Civilian Shelters|Arson)	30 (same)	Not admissible	The inferential condition is incompatible with the hypothesis

Table 6. Summary of Sensitivity Analysis Inferential Conditions and Courses of Action

Inferential Condition	**Conditional Probability of Evidence (%): with 40% as criterion**	**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 detonated 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 also 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
P(Convoy Ambushes|Sectarian Violence)	30	Additional analysis	No conclusive evidence to support this COA. There is a need to further 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

To further gain more insight into the simulated results, a correlations analysis was performed on the conditional probability distributions. Tables 7 & 8 show a summary of the results of the correlation analysis on some of the conditional probability distributions discussed in section 5.2.The results show the following as confirmed by the distributions plots: a) Statistically significant positive correlation (r= 0.884) between the evidence of attacks on security targets m_{11} (*Security Target Engagement)* and the targeted action t_{32} (*Infrastructure Sabotage*), b) Statisitically significant correlation (r = 0.984) between evidence of *Sectarian Identity* ($X_1 = x_{11}$) and the probability of *Insurgent security Target Engagement* (m_{11}) and c) Statisitically significant negative correlation (r = -0.987) between the evidence of intelligence asymmetry (x_{33}) and the probability of security target engagement (m_{11}).

Table 7: Correlation Analysis of the Posterior Distributions for the Variables of Figure 8

Pearson Correlation Coefficients, N = 7 (with p value in parenthesis) **Prob > |r| under H_0: Rho=0**				
	m_{11}	y_{11}	x_{11}	t_{32}
m_{11}	1.00000	0.97144 (0.0003)	0.98438 (<.0001)	0.88388 (0.0083)
y_{11}	0.97144 (0.0003)	1.00000	0.96715 (0.0004)	0.89113 (0.0071)
x_{11}	0.98438 (<.0001)	0.96715 (0.0004)	1.00000	0.83680 (0.0189)
t_{32}	0.88388 (0.0083)	0.89113 (0.0071)	0.83680 (0.0189)	1.00000

Table 8: Correlation Analysis of the Posterior Distributions for the Variables of Figure 9

Pearson Correlation Coefficients, N = 7(with p value in parenthesis) **Prob > |r| under H_0: Rho=0**				
	x_{33}	y_{22}	m_{11}	t_{21}
x_{33}	1.00000	-0.56250 (0.1887)	-0.98748 (<.0001)	-0.87070 (0.0108)
y_{22}	-0.56250 (0.1887)	1.00000	0.48284 (0.2724)	0.80064 (0.0305)
m_{11}	-0.98748 (<.0001)	0.48284 (0.2724)	1.00000	0.79249 (0.0336)
t_{21}	-0.87070 (0.0108)	0.80064 (0.0305)	0.79249 (0.0336)	1.00000

6. CONCLUSIONS AND FUTURE RESEARCH

BAMSS has been presented as a decision support tool for sensemaking analysis. At the current stage, BAMSS can identify a single most probable explanation from a BBN and extract the prevalent conditional probability values to help the sensemaking analysts to understand the cause-effect of the adversary information. The vignettes used allow BAMSS to simulate prospective sensemaking by adjusting the model of posterior probability information integration when new data are available to the analyst. This approach represents the dynamic battlefield information and replicates the mind of the adversary intention. Thus, in BAMSS, the friendly force commander uses the adversary information to prospectively make sense of "what may be the next state" or course of action of the enemy.

The BAMSS'GUI is implemented using Open Source software. The GUI allows for data acquisition, formatting for BAMSS analytics, selection of the appropriate Bayesian data fusion model, and simulation output visualization. To use BAMSS, all the development software tools have 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 software component accessible on the web is GeNie which is used for network design. As an on-going research, the following activities are planned:

a) Since BAMSS requires a user defined BN, additional research is needed to develop an automatic network module capable of taking the user's data in any format and building a corresponding network for BBN.
b) Include an intelligent help system in the GUI to provide design and analysis help to the user.
c) Transition BAMSS into a web version that can operate in a client-server model for easy access to many analysts and for use in simulation experiments.

REFERENCES

[1] 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

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

[3] 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.

[4] 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

[5] 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.

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

[7] 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.

[8] 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.

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

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

[11] 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.

[12] Wasyluk, H., Onisko,A., & Druzdzel,M.J.(2001). Support of diagnosis of liver disorders based on a causal Bayesian network model. Medical Science Monitor, 7(Suppl. 1):327-332, May 2001

[13] Zhang, Y. & Ji, Q. (2006). Active and dynamic information fusion for multisensory systems with dynamic Bayesian networks. IEEE Trans. Syst., Man,Cybern. B, Cybern., vol. 36, no. 2, pp. 467–472.

[14] Pfeffer, A.(2000). Probabilistic Reasoning for Complex Systems. PhD thesis, Dept. Comp. Sci., Stanford Univ.

[15] 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).

[16] 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.

[17] 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.

[18] Das, B. (1999). Representing uncertainties using Bayesian networks. Technical Report DSTO-TR-0918, Defense Science and Technology Organization, Salisbury, Australia.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] Paté-Cornell, E. (2001). Fusion of Intelligence Information: a Bayesian Approach. Risk Analysis Vol.22, No. 3: 445-454.

[24] 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.

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

[26] 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.

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

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

[29] 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.

[30] Druzdzel, M. J. (1999). SMILE: Structural Modeling, Inference, and Learning Engine and GeNIe: A development environment for graphical decision-theoretic models (Intelligent Systems Demonstration). In Proceedings of the Sixteenth National Conference on Artificial Intelligence (AAAI-99), AAAI Press/The MIT Press, Menlo Park, CA.

[31] Munya,P. (2014). ABayesian Abduction Model for Sensemaking. PhD dissertation, Dept. of Industrial & Systems Engineering, North Carolina A & T State University.

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