

## SENSITIVITY ANALYSIS OF A BAYESIAN BELIEF NETWORK IN A TACTICAL INTELLIGENCE APPLICATION

Amanda Jane Brosnan<sup>1</sup>

**Abstract.** In this paper, a variety of targeted sensitivity analysis approaches are explored for a Bayesian Belief Network (BBN) constructed as an expert tool for enemy course of action (COA) assessment at the tactical level in a conventional mid-intensity scenario. Robustness analysis is used to measure the level to which the posterior probability of the states at the root node are affected by instantiation of individual nodes in the network. Likewise, value of information analysis and gain in belief updating are used to compare how nodes of interest affect posterior probabilities at the root node, the former measuring Shannon Entropy and the latter Kullback Distance. Finally, sensor effectiveness analysis is used to measure how the reliability of reconnaissance and surveillance (R&S) assets affects updating of belief at the root node. It was found that each of the sensitivity analysis approaches could be used to optimise allocation of R&S, to identify the commander's decision points, and to identify influential nodes for which the conditional probability tables (CPTs) should be refined. In terms of utility, it was concluded that, as in the case of the use of BBNs in the tactical COA assessment domain in general, the utility of sensitivity analysis of the BBN would be reduced in conditions of high operational tempo and myriad variables influencing tactical COA selection. Nevertheless, in a slower operational tempo environment, the benefits in refinement and utility of the BBN derived through sensitivity analysis would be significant.

### INTRODUCTION

In a previous article [1], Bayesian Belief Networks (BBNs) were constructed to explore their use as expert tools to aid assessment of enemy course of action (COA) at the tactical level of war. Two scenarios were considered: Scenario 1, a conventional mid-intensity scenario; and Scenario 2, a Peace Support Operations (PSO) low-intensity scenario. Using intelligence collection plans for the respective scenarios, BBNs were constructed where enemy COA options that had been identified were root nodes, and combat indicators and reconnaissance and surveillance (R&S) assets tasked to collect information on the combat indicators were child nodes separated from the root node by various generations depending on their relationship to the root node.

Sensitivity analysis can be used to refine such BBNs in a variety of ways. Because of the number of possible combinations of nodal states that could be involved in this process, simple sensitivity analysis can quickly become a significant task in terms of time and computational effort required. For this reason, it makes sense to target sensitivity analysis.

Using the Scenario 1 BBN from [1], the aim of this paper is to describe and comment on four forms of sensitivity analysis applied to a BBN designed to assess enemy COA at the tactical level:

- testing the robustness of a network,
- determining the value of information,
- calculating the gain in belief updating, and
- calculating sensor effectiveness.

### ROBUSTNESS ANALYSIS

Robustness analysis can be used to determine the extent to which posterior probabilities at the root node are changed when child nodes are instantiated. This type of robustness analysis is valuable in the context of using a BBN to assess enemy COA because it is important that the assessment is not

heavily influenced by one or two nodes. If it were, there would be a potential for 'nasty surprises', that is, strong changes in the relative probabilities of the possible COAs after the inputting of just one or two pieces of evidence in the network. In such a case the commander would have very little warning of the need to alter an existing COA or activate a contingency plan. The ideal would be a gradual build-up of probability in one direction for each COA as evidence is added to the network. Robustness analysis can also be used to minimize affects of poorly calibrated or biased conditional probabilities elicited from experts. In that case, once influential nodes have been identified, their conditional probabilities can be refined using robustness analysis to gain an indication of the range in which changes in the conditional probabilities will change the posterior probabilities at the root node.

To perform robustness analysis, a prior probability distribution is compared with a posterior probability distribution after evidence has been added and propagated through the selected conditional probability distributions in the network. In a BBN, the posterior probability relates to a conditional probability as a quotient of two linear functions:

$$\Pr(COA | e) = \frac{a \cdot x + b}{c \cdot x + d} \quad (1)$$

where:  $e$  is evidence,

$x$  is the conditional probability, and

$a, b, c$  and  $d$  are constants.

Netica, the programme used to construct the BBN, contains a facility for conducting single-finding sensitivity analysis. The report produced includes robustness measures in the form of the minimum and maximum values the posterior probability of a node will take when another node containing a conditional probability table is instantiated.

In terms of ranking, examination of the sensitivity report for the Scenario 1 BBN showed that COA2 tended to have the largest differences between prior and posterior probabilities. These ranged from 0.0205 to 0.4165. COA2 is therefore the least robust root node state to new evidence in the network.

<sup>1</sup> Capability Analysis and Doctrine Branch, Army General Staff, PO Box 905, Trentham, Upper Hutt, New Zealand.