Threat Modelling and Assessment Using Evidential Networks

Alessio Benavoli
DSI
Università di Firenze
Italy

Branko Ristic
ISR Division
DSTO
Australia

Alfonso Farina
Engineering Division
SELEX Sistemi Integrati
Italy

Martin Oxenham
ISR Division
DSTO
Australia

Luigi Chisci
DSI
Università di Firenze
Italy

***Abstract*— The paper develops an information fusion system that aims at supporting a commander's decision making by providing an assessment of *threat*, that is an estimate of the extent to which an enemy platform poses a threat based on evidence about its intent and capability. Threat is modelled in the framework of the valuation-based system (VBS), by a network of entities and relationships between them. The uncertainties in the relationships are represented by belief functions as defined in the theory of evidence. Hence the resulting network for reasoning is referred to as an *evidential network*. Local computations in the evidential network are carried out by inward propagation on the underlying joint binary tree. This allows the dynamic nature of the external evidence, which drives the evidential network, to be taken into account by recomputing only the affected paths in the joint binary tree.**

Keywords: Threat assessment, data fusion, valuation-based system, local computations, theory of evidence.

I. Introduction

[1] Situation and threat assessment as Level 2 and 3 fusion processes, are considered to be more complex than those needed at Level 1 [1]. Situation assessment establishes a view of the battlespace in terms of the observed activities, events, locations and manoeuvres of the enemy force elements and from this view infers what is happening or what is going to happen on the battlefield. Threat assessment, on the other hand, estimates the degree of severity with which the engagement events will occur; this degree is in proportion to the perceived capability of the enemy to carry out its hostile intent. The development of both situation and threat assessment typically involves multiple types of expertise, where reasoning is based on various possibly disparate types of observed evidence. In addition, the amounts of data potentially relevant and available to a decision maker in a modern warfare by far exceeds the human ability to review and comprehend them in a timely manner. All this leads to a need for a development of an automatic reasoning system that will support the commander's decision process in a reliable, timely and consistent manner [2]. Similar problems exist in other fields of human endeavour (e.g. management of commercial enterprises, medical diagnosis, etc), although the military command and control domain is particularly challenging due to inherently uncertain and imprecise knowledge base and observed evidence.

A review of the early (pre 1990s) attempts in building knowledge-based and expert systems for situation and threat assessment are presented in [1, Ch.9]. The main problem with these early attempts, however, was the lack of means to deal with the uncertain domain knowledge and imprecise or nonspecific evidence. The invention of Bayesian networks [3] for knowledge representation and probabilistic inference represents an important stepping stone in the development of expert systems. As a result several situation assessment [4]–[6], threat assessment [7] and intent estimation [8], [9] solutions based on the Bayesian networks have been reported in the literature. The limitation of a Bayesian network as a formalism for managing uncertainty, however, is the assumption that all data (domain knowledge, accumulated evidence) can be represented by probability functions. In reality this is not always possible, and consequently other mathematical theories of uncertainty, such as the possibility theory [10] and the theory of evidence (or the belief function theory) [11] have been developed.

The *valuation-based system* (VBS) [12] is a general framework for managing uncertainty in expert systems: it can be applied in the context of all three major theories of uncertainty, namely the probability theory, the possibility theory and the theory of evidence. In VBS, knowledge is represented by a network of variables (nodes) corresponding to entities of the domain (and their states), and of links (edges) representing the relationships between these entities. The values (called valuations) are assigned to the links of the VBS, based on our domain knowledge and on the external evidence. The inferences are made in VBS using two operators called *combination* and *marginalisation*. Combination corresponds to the aggregation of knowledge, while marginalisation refers to the focusing (coarsening) of knowledge. Typically we make inferences on a small subset of variables in the valuation-based network. A "brute-force" approach to reasoning in VBS would be to compute the joint valuation for the entire network and then to marginalise it to the subset of variables that are of interest for decision making. The problem with this approach, however, is that it becomes computationally

[1]Emails: benavoli@dsi.unifi.it;
branko.ristic@dsto.defence.gov.au;
afarina@selex-si.com;
martin.oxenham@dsto.defence.gov.au;
chisci@dsi.unifi.it.

The authors would like to thank The University of Melbourne for hosting A. Benavoli while he was working on the paper.

intractable even for small scale problems. A better alternative to the brute-force approach is to perform *local computations*, that is to compute the required marginals of the joint valuations without explicitly computing the joint valuation. Shenoy and Shafer [13] introduced the set of axioms that combination and marginalisation need to satisfy in order to apply the local computation concept. These axioms are satisfied for all three major theories of uncertainty mentioned earlier.

In this paper we adopt VBS to represent the valuations by belief functions (as defined in the theory of evidence), due to their superior expressive power in relation to both the probability functions and the possibility/necessity functions [14, Ch.2]. This is particularly important when the valuations need to represent a domain knowledge-base in the form of uncertain implication (if-then) rules [15]. The resulting valuation-based network is referred to as *evidential network*. The paper develops a model of threat in the context of air surveillance. An evidential network is implemented for the representation of the threat model and for reasoning, that is assessment of threat.

II. Background

A. Belief functions and operations

Let $\mathbf{\Theta}_x$ denote the set of possible values (the *state space* or *frame*) of a variable x. When modelling real world problems we often deal with many interrelated variables and the resulting joint state space is multi-dimensional. All variables that we consider throughout the paper have finite state spaces. Let $\mathbf{D}$ denote a set of variables. The Cartesian product $\mathbf{\Theta_D} \stackrel{\triangle}{=} \times\{\mathbf{\Theta}_x : x \in \mathbf{D}\}$ is the state space for $\mathbf{D}$. The elements of $\mathbf{\Theta_D}$ are called the *configurations* of $\mathbf{D}$.

The beliefs about the true value of $\mathbf{D}$ are expressed on the subsets of $\mathbf{\Theta_D}$. The basic belief assignment (BBA) $m^{\mathbf{D}}$ on domain $\mathbf{D}$ is a *multivariate* belief function which assigns to every subset A of $\mathbf{\Theta_D}$ a value in $[0,1]$, i.e. $m^{\mathbf{D}} : 2^{\mathbf{\Theta_D}} \rightarrow [0,1]$. The following condition is assumed to be satisfied: $\sum_{A\subseteq\mathbf{\Theta_D}} m^{\mathbf{D}}(A) = 1$. The subsets A with a property $m^{\mathbf{D}}(A) > 0$ are referred to as the focal elements of the BBA. The state of complete ignorance about the set of variables $\mathbf{D}$ is represented by a *vacuous* BBA defined as $m^{\mathbf{D}}(A) = 1$ if $A = \mathbf{\Theta_D}$ and zero otherwise.

Three basic operations on multivariate belief functions are of interest here: *vacuous extension*, *marginalisation* and *combination* [16], [17].

Vacuous extension of a BBA defined on domain $\mathbf{D}'$, to a larger domain $\mathbf{D} \supseteq \mathbf{D}'$ is defined as [12]

$$m^{\mathbf{D}'\uparrow\mathbf{D}}(B) = \begin{cases} m^{\mathbf{D}'}(A) & \text{if } B = A^{\mathbf{D}'\uparrow\mathbf{D}} \\ 0 & \text{otherwise.} \end{cases}$$

Marginalisation is a projection of a BBA defined on $\mathbf{D}$ into a BBA defined on a coarser domain $\mathbf{D}' \subseteq \mathbf{D}$:

$$m^{\mathbf{D}\downarrow\mathbf{D}'}(A) = \sum_{B:B^{\downarrow\mathbf{D}'}=A} m^{\mathbf{D}}(B)$$

Combination of two BBAs $m_1^{\mathbf{D}_1}$ and $m_2^{\mathbf{D}_2}$ is carried out using the Dempster's rule of combination. However, before we apply the Dempster's rule we need to vacuously extend both $m_1^{\mathbf{D}_1}$ and $m_2^{\mathbf{D}_2}$ to the joint domain $\mathbf{D} = \mathbf{D}_1 \cup \mathbf{D}_2$. The result will be a BBA $m_{12}^{\mathbf{D}}$ defined on domain $\mathbf{D}$. Formally we write:

$$\begin{aligned}[m_1^{\mathbf{D}_1} \oplus m_2^{\mathbf{D}_2}](A) &= m_{12}^{\mathbf{D}} \\ &= \alpha \sum_{B,C:B^{\uparrow\mathbf{D}}\cap C^{\uparrow\mathbf{D}}=A} m_1^{\mathbf{D}_1}(B)\cdot m_2^{\mathbf{D}_2}(C)\end{aligned}$$

where α is the normalisation constant such that

$$\alpha^{-1} = 1 - \sum_{B,C:B^{\uparrow\mathbf{D}}\cap C^{\uparrow\mathbf{D}}=\emptyset} m_1^{\mathbf{D}_1}(B)\cdot m_2^{\mathbf{D}_2}(C).$$

a) Implication rules.: In expert systems we often deal with the prior (domain) knowledge-base expressed by a number of uncertain implication rules. Consider two non-intersecting domains, $\mathbf{D}_1$ and $\mathbf{D}_2$ with associated frames $\mathbf{\Theta}_{\mathbf{D}_1}$ and $\mathbf{\Theta}_{\mathbf{D}_2}$, respectively. Formally, an implication rule is an expression of the form

$$A \subseteq \mathbf{\Theta}_{\mathbf{D}_1} \Rightarrow B \subseteq \mathbf{\Theta}_{\mathbf{D}_2} \tag{1}$$

Furthermore, let us assume that this implication rule is valid only in a certain percentage of cases, i.e. with a probability p such that $p \in [\alpha, \beta]$, with $0 \leq \alpha \leq \beta \leq 1$. An implication rule can be expressed by a BBA using the principle of *minimum commitment* [18] and its instantiation referred to as the *ballooning extension* [15], [18]. Thus the implication rule of (1) can be expressed by a BBA consisting of 3 focal sets on the joint domain $\mathbf{D}_1 \cup \mathbf{D}_2$:

$$m^{\mathbf{D}_1\cup\mathbf{D}_2}(C) = \begin{cases} \alpha, & \text{if } C = (A\times B)\cup(\bar{A}\times\mathbf{\Theta}_{\mathbf{D}_2}) \\ 1-\beta, & \text{if } C = (A\times\bar{B})\cup(\bar{A}\times\mathbf{\Theta}_{\mathbf{D}_2}) \\ \beta-\alpha, & \text{if } C = \mathbf{\Theta}_{\mathbf{D}_1\cup\mathbf{D}_2} \end{cases}$$

where $\bar{A}$ is the complement of A in $\mathbf{\Theta}_{\mathbf{D}_1}$, and accordingly $\bar{B}$ is the complement of B in $\mathbf{\Theta}_{\mathbf{D}_2}$.

B. Evidential networks

1) Formulation: A valuation based system (VBS) is a generic framework for knowledge representation and inference. Real-world problems are modelled in this framework by a network of interrelated entities, called variables. The variables represent the nodes of the network. Let the set of all variables in a model be denoted by $\mathbf{V}$. The relationships between the variables (possibly uncertain or imprecise) are represented by the functions called valuations. The valuations are the edges (links) of the network. A domain of each valuation is a subset of $\mathbf{V}$. The two basic operations for making inference in a VBS are the combination and marginalization.

We will adopt the belief functions as valuations in the valuation-based network, with operations of combination and marginalization defined in Sec.II-A. The resulting VBS network is referred to as the *evidential network*. The domain of a BBA m in an evidential network is denoted by $d(m)$. Given a subset $\mathbf{D} \subseteq \mathbf{V}$, $\mathbf{M_D}$ denotes the set of all valuations (BBAs) m such that $d(m) = \mathbf{D}$. Let $\mathbf{M} = \cup\{\mathbf{M_D} : \mathbf{D} \subseteq \mathbf{V}\}$ denote the set of all BBAs m in the evidential network such that $d(m) \subseteq \mathbf{V}$.

In summary, en evidential network is defined by a system $(\mathbf{V}, \mathbf{M}, d, \oplus, \downarrow)$ [19]. The operation of marginalisation $\downarrow$ in this system is sometimes replaced by another basic operation called *variable elimination*, defined and denoted as $m^{-x} \triangleq m^{\downarrow d(m)\backslash\{x\}}$ with $x \in \mathbf{V}$. Notice that $x \notin d(m)$ implies $m^{-x} = m$.

The joint valuation (BBA) of an evidential network $(\mathbf{V}, \mathbf{M}, d, \oplus, \downarrow)$ represents a combination of all valuations $\mathbf{M}$ in the network, and is denoted by $\oplus\mathbf{M}$; its domain is $\mathbf{V}$. To make inference, one is typically interested in a joint valuation $\oplus\mathbf{M}$ marginalised to a sub-domain of interest $\mathbf{D}^o \subseteq \mathbf{V}$, that is the objective is to compute $(\oplus\mathbf{M})^{\downarrow\mathbf{D}^o}$. A straightforward approach to obtain $(\oplus\mathbf{M})^{\downarrow\mathbf{D}^o}$ would be to compute first the joint valuation and then to marginalise it to $\mathbf{D}^o$. However, this is very inefficient since the computational complexity grows exponentially with the number of variables in the model (i.e. with the number of nodes in the network).

2) Computation algorithms: The *fusion algorithm* [12], [19] allows to compute the required marginal of the joint valuation $(\oplus\mathbf{M})^{\downarrow\mathbf{D}^o}$ without the need to explicitly compute the joint valuation $(\oplus\mathbf{M})$. As such it is therefore a more efficient alternative for inference than the straightforward approach described above. Let $\mathbf{M} = \{m_1, m_2, \ldots, m_r\}$ be the complete set of BBAs in the evidential network and $\mathbf{D}^o \subseteq \mathbf{V}$, with $\mathbf{V} = d(m_1) \cup d(m_2) \cup \cdots \cup d(m_r)$, the domain of interest for decision making. The fundamental operation of the fusion algorithm is to delete successively all variables $x \in \mathbf{\Delta}$, where $\mathbf{\Delta} \triangleq \mathbf{V}\backslash\mathbf{D}^o$, from the network. The variables can be deleted in any sequence, although different deletion sequences can have different computational costs. Finding an optimal elimination sequence is an NP-hard problem [12], but there exist several heuristics for finding a good elimination sequence [16], [20].

Suppose that variable $x \in \mathbf{\Delta}$ is to be eliminated. Then one can define two subsets of $\mathbf{M}$ as follows:

$$\mathbf{M}_x \triangleq \{m \in \mathbf{M} : x \in d(m)\} \text{ and}$$
$$\mathbf{M}_{\bar{x}} \triangleq \{m \in \mathbf{M} : x \notin d(m)\}.$$

Due to distributivity of marginalisation over combination in the theory of evidence, only the BBAs in $\mathbf{M}_x$ are affected by the elimination of x. Thus, the remaining set of BBAs after eliminating x from $\mathbf{M}$ is

$$Fus_x\{m_1, m_2, \ldots, m_r\} \triangleq \{\oplus\mathbf{M}_x\}^{\downarrow(\mathbf{S}\backslash\{x\})} \cup \mathbf{M}_{\bar{x}}$$

where $\mathbf{S} \triangleq \bigcup_{m_i : x \in d(m_i)} d(m_i)$ The BBA on the domain of interest $\mathbf{D}^o$ can be obtained by applying recursively the fusion algorithm and deleting all variables in $\mathbf{\Delta} = \{x_1, x_2, \ldots, x_d\}$.

$$(m_1 \oplus m_2 \oplus \cdots \oplus m_r)^{\downarrow\mathbf{D}^o} = \\ \oplus \left\{ Fus_{x_d} \left\{ Fus_{x_{d-1}} \left\{ \ldots Fus_{x_1}\{m_1, m_2, \ldots, m_r\} \right\} \right\} \right\}$$

This technique allows to reduce the computational load because the beliefs are combined on local domains and the variable elimination maintains the domains of the combined beliefs of small sizes.

The fusion algorithm is an efficient algorithm if the BBAs are invariant over time. However, every time a BBA in the network changes (this can for example happen if a new piece of evidence about the battlefield situation becomes available), one needs to repeat the application of the fusion algorithm. Clearly this would be inefficient, since there would be much duplication of effort. When BBAs are time varying it is more efficient to implement the local computations using a *binary joint tree* (BJT). A BJT is a binary tree (N, E) of nodes N and edges E where each node has at most three neighbors, one father and two sons [12]. A node without sons is called a *leaf*. A node without a father is called a *root*. The leaves of the BJT are the elements of $\mathbf{M} = \{m_1, m_2, \ldots, m_r\}$, while the domain of the root is such that $\mathbf{D}^o \subseteq d(root)$. Like the fusion algorithm, the structure of the BJT (i.e. nodes and edges) depends strongly of the elimination sequence $\mathbf{\Delta}$.

In a BJT, the marginals are computed by means of a message-passing scheme among the nodes. Initially only the BBAs of the leaves of the BJT are specified. The process of propagating the beliefs from the leaves toward the root of a BJT is called *inward propagation* [12], [19]. The key feature of the BJT and inward propagation is that the combination operator is applied only in the non-leaf nodes of the tree, between their left and right sons. The advantage of using inward propagation on BJT instead of the fusion algorithm is the possibility of reusing the computations of the inward phase in the case the marginals must be re-computed. So every time one or more valuations of the leaves of the BJT change, the inward phase re-calculates the valuations for all the nodes in the BJT which are affected by the change. That is if n_i is the leaf node whose BBA has changed, then the inward phase re-computes the BBAs of only the nodes of the BJT along the path from n_i to the root.

III. Modelling Threat

A. Graphical model

In this section we introduce a model of threat in the context of air-to-air engagement. The model is shown in the form of an evidential network in Fig.1, where the variables are represented by circular nodes, while the valuations (BBAs) are indicated by the diamond shaped signs. The list of variables with explanation and frame definitions is given in Table I. Each valuation is connected by edges to the subset of variables which define its domain. For example, the domain of BBA m_1 is the set of variables {T, HI,C}. Any pair of variables which are not directly connected are assumed to be conditionally independent. The domain of interest for decision making is a singleton $\mathbf{D}^o = \{\text{T}\}$.

B. Specification of expert knowledge

Prior expert knowledge about the problem is expressed by BBAs m_1, m_2, ..., m_7. According to the threat model in Fig.1, variable T (threat) depends on the degree of hostile intent (HI) of the opponent and on its capability (C). Clearly, the threat is directly proportional to both HI and C, and therefore we choose to represent the valuation m_1 with the

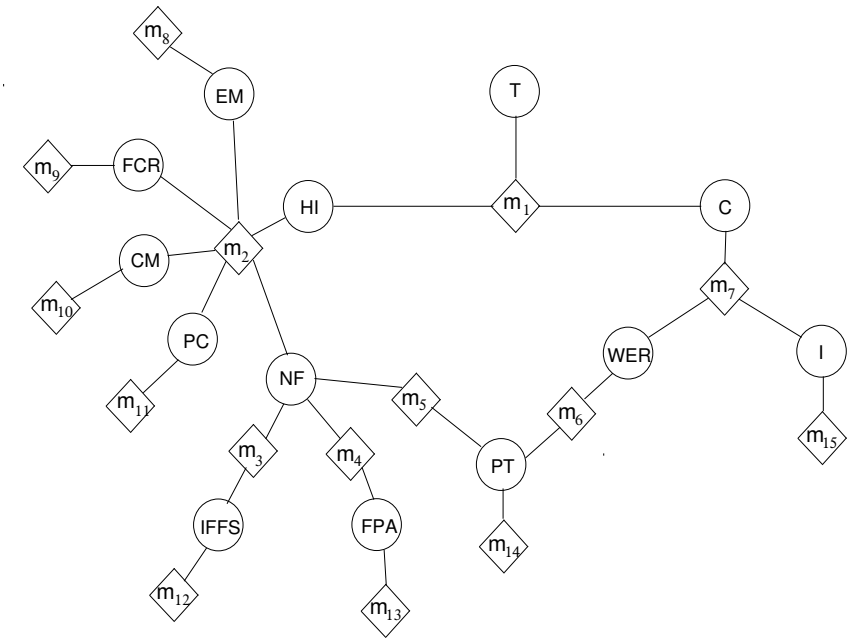

Fig. 1. *An evidential network as a graphical model of threat*

TABLE I

Variables of the threat assessment model

Variable	Description	Frame	Explanation
T	Threat	$\{0, 1, \ldots, 10\}$	0 none, 10 highest degree of T
HI	(Hostile) Intent	$\{0, 1, \ldots, 6\}$	0 none (benign), 6 highest degree of HI
C	Capability	$\{0, 1, 2, 3, 4\}$	0 none, 4 highest degree of C
EM	Evasive manoeuvre	$\{0, 1\}$	0 is false, 1 is true
FCR	Fire Control Radar	$\{0, 1\}$	0 is OFF, 1 is ON
CM	Countermeasures	$\{0, 1\}$	0 is false, 1 is true
PC	Political climate	$\{0, 1\}$	0 is peace, 1 is war
NF	Non-friendly platform	$\{0, 1\}$	0 is false, 1 is true
IFFS	correct IFF squawking	$\{0, 1\}$	0 is false, 1 is true
FPA	Flight plan agreement	$\{0, 1\}$	0 is false, 1 is true
PT	Platform type	$\{0, 1, \ldots, 5\}$	E.g. 0 is EuroFighter, 1 is FA-22 raptor, etc.
WER	Weapon Engagement range	$\{0, 1, 2\}$	0 is small, 1 medium, 2 long range
I	Imminence	$\{0, 1, 2\}$	0 is low, 1 medium, 2 is high

following rule: T=HI+C. Consider in the Cartesian product space T $\times$ HI $\times$ C the set of triples (t, h, c), such that $t = h + c$, where according to the frames of variables in Table I, $t \in \{0, \ldots, 10\}$, $h \in \{0, \ldots, 6\}$ and $c \in \{0, \ldots, 4\}$. Then we can represent the rule $T = HI + C$ by the following categorical BBA:

$$\begin{aligned} m_1(\{&(0,0,0),(1,0,1),\ldots,(4,0,4),\\ &(1,1,0),(2,1,1),\ldots,(5,1,4),\\ &\ldots\\ &(6,6,0),(7,6,1),\ldots,(10,6,4)\}) = 1. \end{aligned} \tag{2}$$

This BBA has a single focal set consisting of 35 triples (t, h, c). The degree of hostile intent (HI) is proportional to the evidence that the target (opponent) behaves in a hostile manner. In particular, the target may perform evasive manoeuvres (EM), it may employ countermeasures (CM), such as deception jamming or chaff, we may have evidence that it is not a friendly (NF) platform, and most importantly, its fire-control-radar (FCR) could be turned on (meaning it intends to fire a weapon soon). In addition, the political climate (PC) has an influence on the HI variable in the sense that the climate of political tension means that the target is more likely to have a hostile intent. The relationship between the six mentioned variables (HI,EM,FCR,CM,PC,NF), is captured by the valuation m_2. How this relationship will be represented by m_2 depends on many factors (doctrine, engagement rules, etc), but for the sake of illustration we adopt the following simple rule: HI = EM+2·FCR+CM+PC+NF. This rules reflects the fact that the FCR variable is weighted higher than other variables in contributing to the HI. The adopted rule is represented by BBA m_2 defined on a 6 dimensional product

space HI×EM×FCR×CM×PC×NF as follows:

$$m_2(\{(0,0,0,0,0,0),(1,0,0,0,0,1),(1,0,0,0,1,0),(2,0,0,0,1,1),(1,0,0,1,0,0)\ldots,(2,0,1,0,0,0),\ldots,(6,1,1,1,1,1)\}) = 1 \quad (3)$$

Thus m_2 also has a single focal set consisting of 32 six-tuples.

Identification friend or foe (IFF) is a radio interrogator device for positive identification of friendly aircraft. Variable IFFS is true if the target responds correctly to interrogation. In order to define the valuation m_3 on domain $\{\text{NF}, \text{IFFS}\}$, suppose that we have confidence that in 95% of the cases when IFFS is true, the target is a indeed a friend (i.e. NF $= 0$). On the other hand, suppose the evidence indicates that the lack of response to IFF interrogation (IFFS=0) is due to adversary platform being interrogated (NF$= 1$) only in 10 to 30% of the cases. We can then summarise this "expert" knowledge about the domain $\{\text{NF}, \text{IFFS}\}$ by the following set of rules:

$(\text{IFFS} = 1) \Rightarrow (\text{NF} = 0)$ with confidence 0.95

$(\text{IFFS} = 0) \Rightarrow (\text{NF} = 1)$ with confidence between 0.1 and 0.3

Then according to Sec.II-A, each above rule can be represented by a BBA; when these BBAs are combined by the Dempster's rule we obtain the following valuation on product space IFFS$\times$ NF:

$$\begin{array}{llllll} m_3 & (\{ & (0,0), & (0,1), & & \}) = 0.6650 \\ m_3 & (\{ & (0,0), & (0,1), & (1,0) & \}) = 0.1900 \\ m_3 & (\{ & & (0,1), & (1,0) & \}) = 0.0950 \\ m_3 & (\{ & (0,0), & (0,1), & (1,1) & \}) = 0.0350 \\ m_3 & (\{ & & (0,1), & (1,0), \quad (1,1) & \}) = 0.0050 \\ m_3 & (\{ & (0,0), & (0,1), & (1,0), \quad (1,1) & \}) = 0.0100 \end{array}$$

Flight plans are filed by pilots with the local aviation authority prior to flying. They generally include basic information such as departure and arrival points, estimated time, etc. If there is evidence that an air target is flying in accordance with a flight plan (variable FPA $= 1$), than this is a strong indication that it is a friend (or neutral), i.e. NF$= 0$. Suppose we can again summarise expert knowledge about the domain $\{\text{FPA}, \text{NF}\}$ by the following set of rules:

$(\text{FPA} = 1) \Rightarrow (\text{NF} = 0)$ with confidence 0.95

$(\text{FPA} = 0) \Rightarrow (\text{NF} = 1)$ with confidence between 0.1 and 0.3

As described above, these two rules can be translated to the corresponding BBA m_4 on its domain $\{\text{FPA}, \text{NF}\}$.

Suppose we have at our disposal a sensor such as an electronic support measures (ESM) system, which can report on the platform type (PT) variable. Valuation m_5 captures the expert knowledge which relates the PT to the NF variable. Suppose this knowledge is represented by the following implication rule:

$$(\text{NF} = 1) \Rightarrow (\text{PT} \in \{3,4,5\}) \text{ with confidence } 0.50$$

This rule represents our prior knowledge (e.g. from intelligence sources) that non-friendly aircrafts in the battlespace of interest are of type 3, 4 or 5, with confidence 50%. For each PT, it is usually known a priori what types of weapons (and its capabilities) it carries [21]. Variable m_6 represents the relationship between the weapons engagement range (WER) variable and the PT. Suppose m_6 is defined by the following set of rules:

$(\text{PT} \in \{0,1\}) \Rightarrow (\text{WER} \in \{0\})$ with confidence 0.40

$(\text{PT} \in \{2,3\}) \Rightarrow (\text{WER} \in \{1,2\})$ with confidence 0.40

$(\text{PT} \in \{4,5\}) \Rightarrow (\text{WER} \in \{2\})$ with confidence 0.40

Variable C (capability) in our threat model is related to the WER and the imminence (I) of an attack. The degree of imminence is measured by the distance, heading and speed of the target, and according to Table I can be low, medium or high. We define valuation m_7 by the following rule on the product space C $\times$ WER $\times$ I: C=WER+I. This rule captures the simple notion that the capability is high if the WER is large and the imminence is high. Thus m_7 is a categorical BBA:

$$m_7(\{(0,0,0),(1,0,1),(2,0,2),(1,1,0),(2,1,1),(3,1,2),(2,2,0),(3,2,1),(4,2,2)\}) = 1.$$

Other BBAs of the evidential network $(m_8, \ldots, m_{15})$ will be specified in the next section.

IV. Numerical results

To assess the degree of threat using the evidential network of Fig.1 we need to first construct the binary joint tree. For this we need to specify three inputs: (i) the set of variables of interest for decision making $\mathbf{D}^o = \{\text{T}\}$; (ii) the set of variables to be eliminated $\mathbf{\Delta} = \{\text{HI,C,EM,FCR,CM,PC,NF,IFFS,FPA,PT,WER,I}\}$ and the set of the valuations (BBAs) $\mathbf{M}$ with associated domains d. A resulting BJT shown in Fig. 2 is obtained with the following variable elimination sequence: IFFS, FPA, I, C, EM, FCR, CM, PC, WER, HI, NF. This elimination sequence was selected using the heuristic called *One Step Look Ahead - Smallest Clique, Fewest Focal sets* (OSLA-SCFF) [16, p.61]. The nodes in the BJT are labelled by integer numbers from 1 to 29. The leaves of the tree (the nodes labelled from 1 to 15) represent the original valuations specified by the set $\mathbf{M} = \{m_1, \ldots, m_{15}\}$. The remaining nodes in the BJT represent the intermediate steps of the fusion algorithm; as such they specify the order in which the valuations must be combined in order to calculate the valuation for the variable T. The vertical labels next to the nodes of the BJT denote the domains (the subsets of variables) of the nodes.

Once we have created the BJT, the threat assessment calculations are carried out in the following order: (1) initialise the leaves of the BJT with the BBAs $\mathbf{M}$; (2) apply the inward propagation algorithm; (3) marginalise the belief of the root of the BJT to $\mathbf{D}^o = \{\text{T}\}$; (4) apply the pignistic transformation to obtain the pignistic probability mass function (PMF) for the degree of threat (from 0 to 10 in our case).

We have specified BBAs m_1 to m_7 in Sec.III-B. The remaining BBAs of the evidential network in Fig.1, namely m_8, m_9, $\ldots$, m_{15}, are referred to as *input valuations*, since they are typically supplied during the observation period by

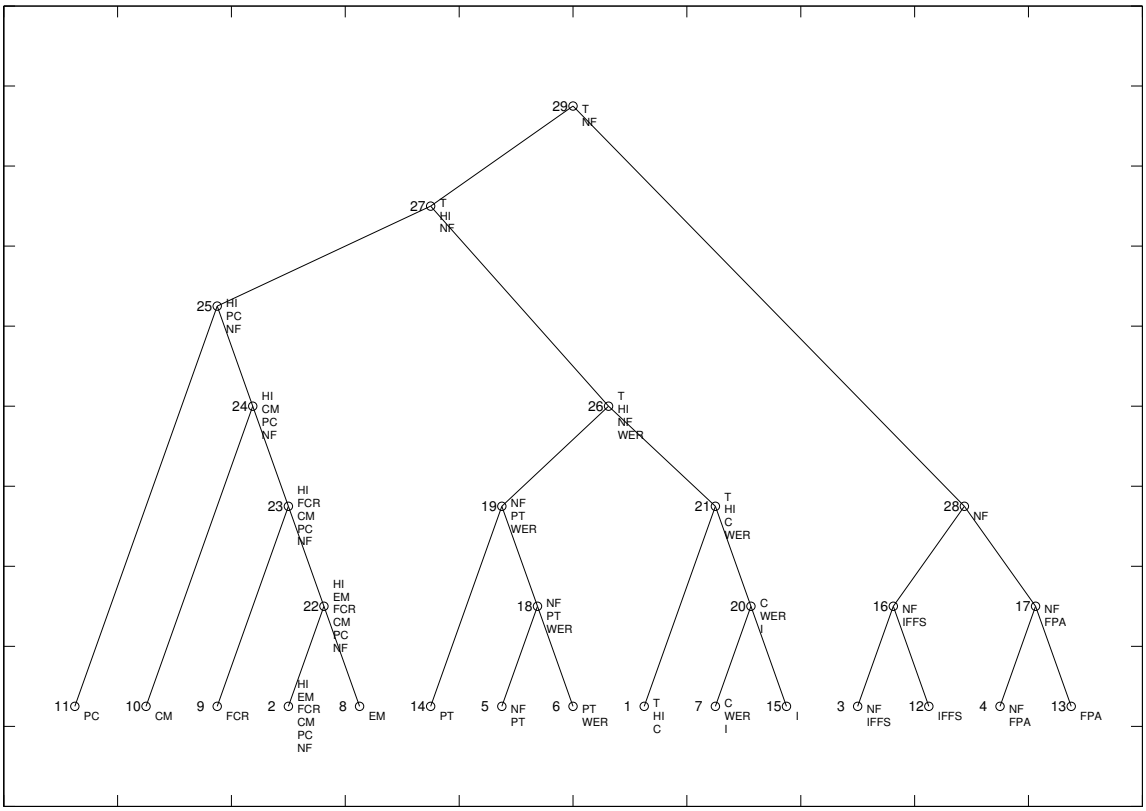

Fig. 2. Binary joint tree for the threat assessment evidential network

the surveillance sensors, external sources and/or intelligence reports. The input valuations are the drivers of the evidential network for threat assessment. Initially they will be vacuous BBAs (before any input data is available). Suppose the sequence of incoming evidence in the form of input valuations is as specified by Table II. At time t_1 we feed into the network the current state of the political climate (PC) represented by BBA m_{11}. For the argument sake, let this BBA reflect the state of a political tension in the region; hence the belief mass given to the state of war is 0.7, while the remaining 0.3 is assigned to ignorance. Then at time t_2 some evidence about the EM variable becomes available (it appears that the target is performing an evasive manoeuvre, belief mass 0.8). Each time a new piece of evidence is available, the situation becomes more informative (less uncertain) which is reflected by the pignistic PMF of threat, shown in Fig 3. Note how this PMF evolves from being totaly uninformative at time t_0 to becoming concentrated ("peaky") at time t_9. At this last time instant the degree of threat with the highest probability is 8 (on the scale from 0 to 10).

The evidential network for threat assessment was implemented in MATLAB(c). One run with input valuations as shown in Table II takes about 5 seconds. For comparison sake we have also tried to compute the joint valuation $\oplus\mathbf{M}$ and then to marginalise it to variable T. The computer program for this case did not finish even after 48 hours of running.

V. Conclusions

Reasoning for threat assessment is carried out in the framework of valuation based systems using belief functions. Local computations are performed using the binary joint tree and the inward propagation algorithm. The result is a tool capable of timely and accurate processing of vast amounts of data in support of commander's decision making. Future work will consider the refinement of the threat model to more realistic situations, with possibly more entities in the network and larger frames. The developed tool for reasoning using evidential networks is universal and can be easily adapted to perform other tasks in support of commander's decision making, such as target identification and situation assessment also for homeland security.

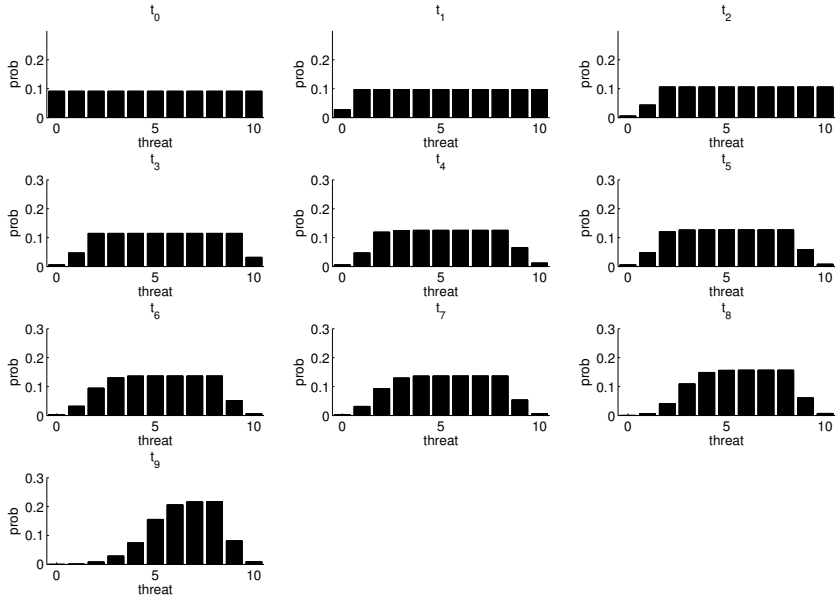

Fig. 3. Pignistic probability mass function for variable T (threat) in a dynamic situation (from time t_0 to t_9)

TABLE II

The sequence of incoming evidence

Time	BBA	domain	focal set	mass
t_1	m_{11}	PC	$\{1\}$	0.7
			$\{0,1\}$	0.3
t_2	m_8	EM	$\{1\}$	0.8
			$\{0,1\}$	0.2
t_3	m_{15}	I	$\{0,1\}$	0.7
			$\{0,1,2\}$	0.3
t_4	m_{13}	FPA	$\{1\}$	0.9
			$\{0,1\}$	0.1
t_5	m_{15}	I	$\{1\}$	0.8
			$\{0,1,2\}$	0.2
t_6	m_{14}	PT	$\{2\}$	0.6
			$\{3\}$	0.3
			$\{4\}$	0.1
t_7	m_{12}	IFFS	$\{0\}$	0.9
			$\{0,1\}$	0.1
t_8	m_{10}	CM	$\{1\}$	0.9
			$\{0,1\}$	0.1
t_9	m_9	FCR	$\{1\}$	0.8
			$\{0,1\}$	0.2

REFERENCES

[1] E. Waltz and J. Llinas, *Multisensor Data Fusion*. Artech House, 1990.

[2] A. Kott, M. Pollack, and B. Krogh, "The situation assessment problem: Toward a research agenda," in *Proc. DARPA-JFACC Symposium on Advances in Enterprise Control*, San Diego, CA, Nov. 1999.

[3] J. Pearl, *Probabilistic reasoning in intelligent systems*. San Francisco: Morgan Kaufmann Publishers, 1988.

[4] S. Das, R. Grey, and P. Gonsalves, "Situation assessment via Bayesian belief networks," in *Proc. Fifth Int. Conf. Information Fusion*, Annapolis, MD, July 2002.

[5] P. Bladon, R. J. Hall, and W. A. Wright, "Situation assessmennt using graphical models," in *Proc. Fifth Int. Conf. Information Fusion*, Annapolis, MD, July 2002.

[6] F. Mirmoeini and V. Krishnamurthy, "Reconfigurable Bayesian networks for adaptive situation assessment in battlespace," in *Proc. IEEE Conf. Networking, Sensing and Control*, March 2005, pp. 810 – 815.

[7] N. Okello and G. Thomas, "Threat assessment using bayesian networks," in *Proc. Sixth Int. Conf. Information Fusion*, Cairns, Australia, July 2003.

[8] X. Nguyen and P. Heuer, "Automated intent assessment simulation environment," in *Proc. Information, Decision and Control*, Adelaide, Australia, Feb. 2002.

[9] K. D. Lee and J. Llinas, "Hybrid model for intent estimation," in *Proc. Sixth Int. Conf. Information Fusion*, Cairns, Australia, July 2003.

[10] D. Dubois and H. Prade, *Possibility theory: An approach to computerised processing of uncertainty*. Plenum Pub., 1988.

[11] G. Shafer, *A mathematical theory of evidence*. Princeton University Press, 1976.

[12] P. P. Shenoy, "Valuation based systems: A framework for managing uncertainty in expert systems," in *Fuzzy Logic and the Management of Uncertainty*, L. A. Zadeh and J. Kacprzyk, Eds. New York: Wiley, 1992, ch. 4, pp. 83–104.

[13] P. P. Shenoy and G. Shafer, "Axioms for probability and belief-function propagation," in *Readings in uncertain reasoning*, J. P. G. Shafer, Ed. San Mateo, CA: Morgan Kaufmann, 1990, pp. 575–610.

[14] G. J. Klir and M. J. Wierman, *Uncertainty-based information: Elements of generalized information theory*. New York: Physica-Verlag.

[15] B. Ristic and P. Smets, "Target identification using belief functions and implication rules," *IEEE Trans. Aerospace and Electronic Systems*, vol. 41, no. 3, pp. 1097–1103, July 2005.

[16] N. Lehmann, *Argumentation Systems and Belief Functions*. Tech. report 01-30. Department of Informatics, University of Fribourg, 2001.

[17] R. Haenni and N. Lehmann, "Probabilistic argumentation systems: a new perspective on the of Dempster-Shafer theory," *International Journal of Intelligent Systems*, vol. 18, no. 1, pp. 93–106, 2003.

[18] P. Smets, "Belief functions: the disjunctive rule of combination and the generalized Bayesian theorem," *Int. Journal of Approximate Reasoning*, vol. 9, pp. 1–35, 1993.

[19] R. Haenni, "Ordered valuation algebras: a generic framework for approximate inference," *Int. Journal of Approximate Reasoning*, vol. 37, pp. 1–41, 2004.

[20] R. G. Almond, *Graphical Belief Modeling*. Chapman and Hall, 1995.

[21] "Fighter planes," Web: http://www.fighter-planes.com/.