IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 3 June 2024, accepted 17 June 2024, date of publication 19 June 2024, date of current version 27 June 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3416909

APPLIED RESEARCH

Valuation Network for Ongoing Assessment of Threat to an Underwater Vehicle

BRANKO RISTIC[1], AMANDA BESSELL[2], AND SANJEEV ARULAMPALAM[2], (Senior Member, IEEE)
[1]School of Engineering, RMIT University, Melbourne, VIC 3000, Australia
[2]Information Sciences Division, Defence Science and Technology Group, Edinburgh, SA 5111, Australia

Corresponding author: Branko Ristic (branko.ristic@rmit.edu.au)

This work was supported by the Defence Science and Technology Group under the Research Agreement "Machine Reasoning with Imprecise Probabilistic Models for Underwater Surveillance."

ABSTRACT The paper develops a valuation based system for reasoning under uncertainty in the context of threat assessment onboard an underwater vehicle. The focus is on threat posed by the nearby contacts, while the vessel is navigating busy waters with warships, merchant ships and fishing vessels. A graphical model of a valuation network is developed, representing the (uncertain) contextual prior knowledge and received observations over the course of time. Two types of valuations are considered in this context: (1) probability mass functions, assuming that all probabilistic values are known precisely; (2) credal sets (sets of probabilities), when probabilistic values are specified only as the confidence intervals. The performance of two valuation networks is presented, using a typical scenario-log, involving a varying number of different types of contacts over time.

INDEX TERMS Machine reasoning, graphical models, valuation networks, maritime threat assessment.

I. INTRODUCTION

Reasoning and decision making using artificial intelligence (AI) has many applications in naval military operations, both above and under the water. Naval operations are particularly complex due to hostility, unpredictability (due to uncertainty) and the size of the ocean environment. Many countries have placed importance in developing AI systems for naval combat systems to achieve battle-space superiority. The role of these systems is to help the human naval commanders to process and comprehend the vast amounts of available data in a timely, consistent and intelligent manner [1]. The data typically appears in different forms, such as, the numerical measurements from physical sensors, the natural language statements from human operators and the contextual prior or historical knowledge-base. AI systems provide methods for fusion of all types of data to enhance tactical knowledge and suggest the best course of action in a combination with predictive capabilities [2]. This is important because crucial decisions on a battlefield usually need to be taken under stressful conditions, which could also adversely affect the human decision makers.

Early machine reasoning systems captured the knowledge of human experts by a complex system of *if-then* rules [3, Ch.9], but their main drawback was the inability to handle *uncertainty*. Subsequently, *Bayesian networks* (BN) [4], capable of reasoning under uncertainty, were developed in mid-1980s. Several architectures [5] have been proposed for exact computation of marginals of multivariate discrete probability distributions in the context of BNs. One of them was the Lauritzen-Spiegelhalter [6] architecture, which determines the marginals of a multidimensional probability density using the concept of *local computation* in *join trees*. This architecture has been generalized by Lauritzen and Jensen [7] so that it applies more generally to other uncertainty representation frameworks, including the Dempster-Shafer's belief function theory (or evidential theory) [8]. Inspired by the work of Pearl, Lauritzen and Spiegelhalter, Shenoy and Shafer proposed the valuation based system (VBS) for computing marginals in join trees and established the set of axioms that combination and marginalisation (focusing) operations need to satisfy in order to make the local

The associate editor coordinating the review of this manuscript and approving it for publication was Xuebo Zhang.

computation concept applicable [9]. Reasoning networks based on the Shenoy-Shafer architecture are referred to as *valuation networks*. A slightly modified version of the Shenoy-Shafer axiomatic formulation was developed by Kohlas [10] with the resulting mathematical structure referred to as the *valuation algebra*. The central component of a valuation algebra is a *valuation*: a quantified representation of an uncertain piece of information. The axioms of valuation algebra are satisfied in practically all frameworks of uncertainty modeling, e.g. probability theory [10], possibility theory [11], Dempster-Shafer theory [10] and imprecise probability theory [12], leading to the development and application of the corresponding valuation networks [11], [13], [14], [15].

This paper develops a valuation network (VN) for an ongoing threat assessment onboard an underwater vehicle. The focus is on threat posed by the nearby contacts, while the vessel is navigating busy waters with warships, merchant ships and fishing vessels. Two kinds of valuations are considered in this context: (1) probability mass functions, assuming that all probabilistic values are known precisely; (2) credal sets (sets of probabilities), when probabilistic values are specified only as the confidence intervals. The performance of the two valuation networks is analysed, using a typical scenario-log, involving a varying number of different types of contacts over time.

The paper is organised as follows. A literature review on threat assessment AI systems is presented in Sec. II. Sec. III describes the problem, motivated by a typical (but hypothetical) scenario-log of an underwater vehicle navigating busy waters. Sec. IV presents the solution: a VN for ongoing threat assessment in the presence of a large and time-varying number of contacts. The numerical results are presented in Sec. V and the conclusions are drawn in Sec. VI.

II. THREAT ASSESSMENT: PREVIOUS WORK

According to the JDL data fusion panel [3], higher-level fusion comprises situation assessment and threat assessment. While situation assessment refers to the comprehension and interpretation of the current situation, threat assessment projects the current situation to the future and in combination with the adversary doctrine and objectives, predicts the risks and consequences. In the last three decades, a vast volume of research papers is devoted to threat modeling (in the military context). Threat models are typically based on the classic ‘‘opportunity-capability-intent’’ paradigm [16]. For example, a threat model in the context of an intruder approaching a (static) military asset [17], is proportional to intruder’s weapons range (capability) and its radial speed, and inversely proportional to their mutual distance (intent, opportunity).

Fan et al. [18] suggest a time-varying tactical threat modelling scheme where the key factors are the environment, the strength of the opponent force (relative to the own force), the distance between the two opposing forces and the relative motion vector. Environmental factors include the terrain, weather and visibility. A dynamic Bayesian network (DBN) is suggested for sequential estimation of the posterior probability of variable *threat*, which is modelled as a Markov process. The conditional probabilities of this DBN are assumed known precisely. Another interesting feature of this article is that the posterior distribution of threat is converted to a single scalar, referred to as a threat degree. This scalar is computed as a weighted sum of threat level probabilities, where the weights are proportional to the threat level. In the example provided, the weight of the highest level of threat is 100 times higher than the weight of the lowest level of threat.

Threat model for underwater operations have been considered in [19], [20], and [21]. Reference [19] proposed a threat model, represented by a directed acyclic graph and solved using a Bayesian network. The threat in this model is a combination of platform threat, platform (technical) condition and underwater environment. Platform threat is influenced by the existence of underwater mines, an adversary submarine, and detection of enemy active sonar pings. Platform condition is a combination of the engine status, the platform load, existence and severity of a leakage and the remaining energy level. Underwater environment depends on ocean currents, ocean density, presence of underwater obstacles (terrain). Reference [20] follows the similar ideas, i.e. the threat depends on the platform operating status, environmental conditions and the adversary confrontation intent. Environmental conditions are a function of water temperature, salinity and currents. The platform operating status is modelled in a fairly complex manner. It depends on the status of the propulsion system, communication system, sensing systems (sonar, image sensor, GPS, INS, MRU, etc), platform structural health (i.e. presence of leakage) and the energy system. Finally, confrontation intent is estimated based on the heading and velocity of the adversary. Another fairly similar threat model for an underwater battlefield is formulated in [21]. Threat corresponds to the relative combat capability (potency) of our forces versus the capability (potency) of the enemy. The combat capability is a combination of the number of platforms, firepower (weapon resources), the distance and relative motion between the forces, and finally the environmental conditions (weather, sea state). This model is also solved using a Bayesian network.

Threat models in the context of maritime security are considered in [22] and [23]. In the model of [22], the threat of an attack on maritime infrastructure is a combination of events such as the vessel anomalous behaviour, the organisation (or country) the vessel belongs to, and the observed region intrusion. Reference [23] considers two models. The first model is to determine if a ship is a threat. This threat model consists of variables, such as, the ship type, its speed, known or unknown identification, and whether it is in the range of defending weapons. The second model considers the threat that a ship can damage a friendly vessel. Its variables are the potential of a collision, the distance between them, and the weapons range. Reference [24] also considers a threat model in maritime environment, where threat is influenced by target type, speed, capability behaviour and position.

Fairly detailed threat models for tactical engagements, based on "opportunity-capability-intent" paradigm, were considered in [15], [25], and [26]. Capability typically involves the size and weapon lethality of the opponent's force, combined with manoeuvrability and imminence. Intent here stands for hostile intent, and is a function of allegiance, geopolitical situation, and the patterns of (past) behaviours. Finally, opportunity is a function of the current environmental conditions (e.g. weather), social acceptance of a conflict, a degree of surprise, and similar conditions. Following the described principles, a threat model for underwater communication cables was analysed in [27].

III. PROBLEM DESCRIPTION

The objective is to develop a machine reasoning system for ongoing threat assessment onboard an underwater vehicle. The assumption is that the ownship platform status and underwater environment are favorable. Hence, the focus is on threats posed by the nearby contacts, while the vessel is navigating busy waters with warships, merchant ships and fishing vessels.

A typical scenario-log, as a motivation for this work, is presented in Table 1. Seven contacts are reported in this log during the observation interval. The left column in the table represents the discrete-time when the information, specified in the right column, is received. The actual time intervals between these discrete-time events are arbitrary. The numerical values for a range (distance) to the targets in the scenario-log are chosen without any operational meaning. The explanation of abbreviations used in the log are:

- AIS stands for *automatic identification system* and represents a maritime communication device onboard a vessel that can send and receive identifying information (including position) about itself. The lack of AIS signal indicates an unusual event, because all merchant ships and larger fishing vessels are required to broadcast AIS information.
- UM stands for an observed *unusual manoeuvre* by a contact.
- SL stands for a *shipping lane*. Shipping lanes are routes that ships regularly take across the sea.

The origin of received information can be a human operator or a physical sensor (e.g. sonar, optical sensor, laser rangefinder). The received information is uncertain, which is sometimes emphasised in the scenario-log by the use of words such as *possible*, *approximately*, *likely* and similar. Of the seven contacts reported in the log in Table 1, only one, contact C-2 (detected at discrete-time $k = 2$) is a real threat. This becomes evident, as the time progresses.

In the next section, we will develop a graphical model of threat as a valuation network. The output of this network should be the level of threat, expressed as a probability, that is, a decimal number between 0 (no threat) and 1 (the maximum threat). The scenario-log in Table 1 will subsequently be applied to this valuation network, reflecting the level of threat as a function of time.

TABLE 1. A typical log-scenario while navigating busy waters.

Time k	Information
1:	new contact detected, labelled as C-1
2:	C-1 is a possible merchant ship; SL agreement
3:	C-1, confirmed it is a merchant ship
4:	new contact detected, labelled as C-2
5:	C-1, AIS match, range 4 km
6:	C-2 is a possible warship, apparently no AIS
7:	C-2, range 22 km
8:	new contact detected, labelled C-3
9:	C-2, confirmed warship, range 20km
10	C-3 is a possible merchant ship
11	C-2, possible UM, range 18km
12	C-3, confirmed merchant ship, range 19km, no AIS, not in SL
13	new contact detected, labelled C-4
14	C-2, range 16km
15	C-4, range 20km
16	C-4, possible merchant ship
17	C-2, range 15km, confirmed hostile
18	C-1, range 6 km
19	new Contact detected, labelled C-5
20	C-5, possible fishing vessel
21	C-2, UM detected, range 14 km
22	C-5, range 7 km, no AIS
23	new Contact detected, labelled C-6
24	C-6, likely fishing vessel; range 3 km
25	new contact detected, labelled C-7
26	C-7, possible fishing vessel, range 8 km, AIS match
27	C-2, range 12km
28	C-5, range 7.5 km, confirmed fishing vessel
29	C-4, range 10km, AIS match, confirmed merchant ship
30	C-2, range 15.5 km
31	C-7, confirmed fishing vessel
32	C-2, range 18 km
33	C-6, confirmed fishing vessel, range 6.5 km

IV. VALUATION NETWORK FOR ONGOING THREAT ASSESSMENT

A. VALUATION NETWORKS: A BRIEF REVIEW

This review is based on [15] and [28]. Inference problems are modelled by a network of interrelated entities, called variables. Let $\mathbf{V}$ be the set of all variables in the network. Each variable can take values in a discrete-state space, called the *frame*. The frame of variable $X \in \mathbf{V}$ is denoted Θ_X. The (uncertain) relationships between variables are represented by the functions called valuations. Let the set of all valuations in a network be denoted by Φ. A valuation $\varphi \in \Phi$ specifies the relationship between a subset of variables, referred to as its domain $d(\varphi) \subseteq \mathbf{V}$. Operation $d : \Phi \rightarrow 2^{\mathbf{V}}$, where $2^{\mathbf{V}}$ is the power set of $\mathbf{V}$, is referred to as the *labeling operation*.

The relationship among the variables in the set $\mathbf{D} = d(\varphi)$ is specified by assigning beliefs (expressed by numerical values) to the elements of the frame of $\mathbf{D}$. This frame, denoted $\Theta_{\mathbf{D}}$, represents a set of possible configurations of $\mathbf{D}$. Suppose the frame of variable $X \in \mathbf{D}$ is Θ_X. Then, the frame of $\mathbf{D}$ is given by $\Theta_{\mathbf{D}} \overset{\triangle}{=} \times\{\Theta_X : X \in \mathbf{D}\}$, where $\times$ denotes the Cartesian product.

Example: Consider a valuation φ expressing the relationship between two variables, i.e. $d(\varphi) = \mathbf{D} = \{X_1, X_2\}$. The frames of X_1 and X_2 are $\Theta_{X_1} = \{x_{11}, x_{12}\}$ and

$\Theta_{X_2} = \{x_{21}, x_{22}, x_{23}\}$, respectively. Then $\Theta_{\mathbf{D}} = \{(x_{11}, x_{21}), (x_{11}, x_{22}), (x_{11}, x_{23}), (x_{12}, x_{21}), (x_{12}, x_{22}), (x_{12}, x_{23})\}$ consists of six configurations. Suppose the relationship can be specified by an uncertain implication rule, such as: $X_1 = x_{11} \Rightarrow X_2 = x_{22}$, with confidence 0.8. One way to express this relationship, using probability theory, is by valuation φ which assigns probability mass of 0.8 to the configuration (x_{11}, x_{22}), while the probability mass of $1 - 0.8 = 0.2$ is spread equally over the remaining five configurations. ■

There are two basic operations with valuations.

- Combination $\otimes$. If $\varphi_1, \varphi_2 \in \Phi$ are two valuations, then the combined valuation $\varphi_1 \otimes \varphi_2$ represents the aggregated knowledge from φ_1 and φ_2.
- Marginalization $\downarrow$. If $\varphi \in \Phi$ and $\mathbf{C} \subseteq d(\varphi)$, then the marginalized valuation $\varphi^{\downarrow \mathbf{C}}$ represents the knowledge obtained by focusing φ from $d(\varphi)$ to $\mathbf{C}$.

Given a finite set of valuations $\Phi = \{\varphi_1, \dots, \varphi_r\}$, inference refers to marginalization (focusing) of all available knowledge, expressed by the joint valuation $\otimes\Phi = \varphi_1 \otimes \cdots \otimes \varphi_r$, to a subset of variables $\mathbf{D}^o \subseteq \mathbf{V}$, called *decision variables*. The straightforward approach to inference would be to compute the joint valuation first and then to marginalize it to $\mathbf{D}^o$. Unfortunately, this would be cumbersome in practice even for a small scale valuation network because the domain size increases with each combination, whereas the complexity grows exponentially with the domain size. By imposing certain axioms for the operations of *labeling*, *combination*, and *marginalization* [9], [14], [29], it is possible to compute the marginal $(\otimes\Phi)^{\downarrow \mathbf{D}^o}$ on local domains, without the need to explicitly compute the joint valuation. The list of axioms is given in [10]. The concept of local computations is carried out by the *fusion algorithm*, which eliminates sequentially all variables $X \in \mathbf{V} \setminus \mathbf{D}_o$ which are of no interest to the inference problem [14], [15], [29]. The fusion algorithm is applied over a structure called the binary joint tree (BJT), where all combinations are carried on pairs of valuations, that is on a binary basis (two-by-two). Finally, marginals are computed by means of a message-passing scheme among the nodes of the BJT. Full details of software implementation of a generic valuation network can be found in [14], [15], and [29].

Uncertainty in valuations Φ can be expressed by different formalisms. The most obvious choice would be to adopt the formalism of probability theory and express the valuations as the probability mass functions (PMFs). Due to the scarcity of training data and the reliance on (subjective) expert knowledge, however, the precise probability values may be unavailable or unreliable. In this case the alternatives could be the formalisms of Dempster-Shafer theory (i.e. the evidential VN) [15], [27] and the formalism of imprecise probability theory [30] (the credal VN [12]). In this paper we omit the former (the evidential VN), because its output is less specific (and hence less useful) than the output of the corresponding credal VN [12]. Thus we focus on two frameworks for uncertainty modeling: (1) the (traditional) probabilistic framework [10], where valuations are represented by PMFs and (2) the (imprecise) set-probabilistic or credal framework [12], [30], where valuations are represented by the sets of PMFs, specified as coherent probability intervals on singletons [30], [31].

The relationship between valuation networks and other approaches to reasoning under uncertainty are discussed in Appendix of [12]. Valuation networks are the most general approach. For example, the dependence of variables in a Bayesian network can be equivalently represented by a valuation network, but vice versa does not hold.

B. A VALUATION BASED GRAPHICAL MODEL OF THREAT

We focus on a threat model which considers only the (time-varying) number of maritime contacts and the geopolitical climate. The model, expressed by the VN in Figs. 1 and 2, reflects the context and the information contained in the log-scenario of Table 1. Ownship status and underwater environment are assumed favorable and hence will not be included in the model, although this could be added easily, if required.

The valuation network for threat from the nearby contacts is shown in Fig. 1. This network is a hypergraph, in which circles represent variables, whereas diamonds are valuations. Variable C_i, represents the threat from contact $i = 1, 2, \dots, m_k$, where $m_k \geq 0$ is the current number of detected contacts. In the absence of any contacts (i.e. if $m_k = 0$), the threat level is determined by prior information, expressed by the variable G. This prior takes into account the factors such as the geographical region and the political climate. The overall threat from all contacts and the prior is represented by variable T (threat). This is our decision variable, i.e. $\mathbf{D}^o = \{\mathrm{T}\}$. Valuation φ_0 is an expression of how T is related to C_i, $i = 1, \dots, m_k$ and G. Let variables C_i and variable G be binary, with the (identical) frame $\Theta = \{0, 1\}$. By convention, $C_i = 1$ denotes the truth, that is, the event that contact C_i, is a threat, while $C_i = 0$ is the opposite. Similarly, G$=0$ indicates no threat, based on the current geopolitical situation. Valuation φ_i, $i = 1, \dots, m_k$, is a quantified belief about variable C_i being true. Depending on the adopted uncertainty framework, this belief will be expressed by a PMF in the probabilistic framework, or a credal set in the set probabilistic framework. In order to ensure variable T is also binary, for φ_0 we adopt a logical disjuction,[1] i.e. OR operation:

$$\varphi_0 : \quad \mathrm{T} = \mathrm{G} \vee \mathrm{C}_1 \vee \mathrm{C}_2 \vee \cdots \vee \mathrm{C}_{m_k}. \tag{1}$$

We can assign a level of confidence α_0, or a confidence interval $[\underline{\alpha}_0, \overline{\alpha}_0]$ to the relationship expressed by (1). Note that the potential existence of non-detected contacts can be included in G.

Next we expand the valuation φ_i, expressing the belief about variable C_i, for $i = 1, \dots, m_k$. Fig. 2 shows the

[1] The alternative is an additive operation for φ_0, as in [15]. This, however, would be cumbersome, because the size of the frame of variable T would be $m_k + 2$, and hence time-varying.

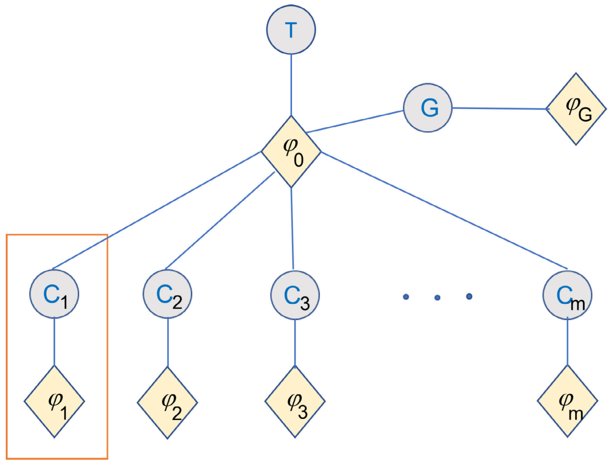

FIGURE 1. Model of threat from all nearby contacts.

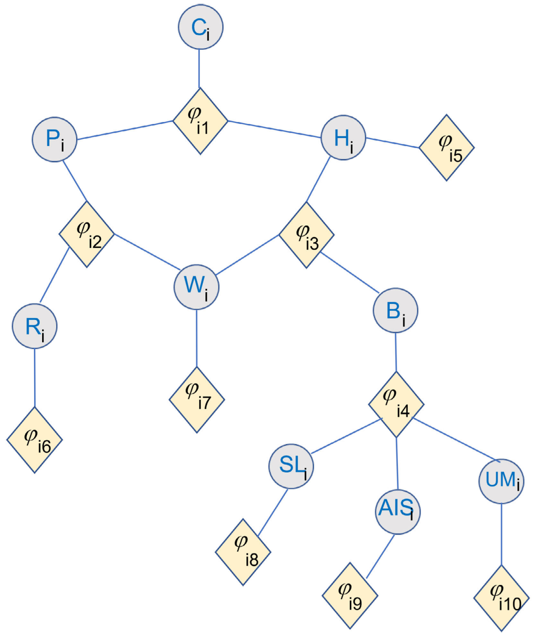

FIGURE 2. Model of threat from a single contact C_i, where $i = 1, \dots, m$.

corresponding valuation network, while Table 2 presents a description of variables. The critical distances for variable R_i (range) are adopted as follows. The critical distance (i) for a distinction between $R_i = 0$ and $R_i = 1$ is 15 km; (ii) for a distinction between $R_i = 1$ and $R_i = 2$ is 5 km. The transitions are fuzzified.

Let us now specify the (uncertain) relationships expressed by valuations in the model of Fig. 2. The confidence in the specification of valuations will be expressed by: (1) precise probabilities, which will represent the "ground truth", and (2) interval probabilities (confidence intervals), expressing epistemic uncertainty. In the former case, inference will be performed using a probabilistic VN [10], while in the latter case, using a credal VN [12].

Valuation φ_{i1} states that contact C_i poses a treat only if it is both hostile (i.e. it has a hostile intent) *and* it has a potential to cause harm. Thus:

TABLE 2. Variables of the threat model for contact C_i, $i = 1, \dots, m$.

Variable	Description	Frame	Explanation
C_i	Contact threat	$\{0, 1\}$	0 is false, 1 is true
H_i	Hostile (intent)	$\{0, 1\}$	0 is false, 1 is true
P_i	Potency	$\{0, 1\}$	0 is false, 1 is true
W_i	Warship	$\{0, 1\}$	0 is false; 1 is true
B_i	Behaviour	$\{0, 1\}$	1 for disorderly
R_i	Range	$\{0, 1, 2\}$	far, medium and near range
SL_i	Shipping lane	$\{0, 1\}$	1 for disagreement
AIS_i	AIS	$\{0, 1\}$	1 for no match or turned off
UM_i	Manoeuvre	$\{0, 1\}$	1 for an unusual manoeuvre

$$\varphi_{i1} : \quad C_i = P_i \wedge H_i, \text{ with confidence } \alpha_{i1} \in [\underline{\alpha}_{i1}, \overline{\alpha}_{i1}]. \quad (2)$$

We assume valuation φ_{2i} is expressed by a conditional probability table (CPT), consisting of

$$\varphi_{i2} : \quad Pr\{P_i = i | W_i = j, R_i = \ell\} = p_{ij\ell} \in [\underline{p}_{ij\ell}, \overline{p}_{ij\ell}] \quad (3)$$

for $i \in \{0, 1\}$, $j \in \{0, 1\}$ and $\ell \in \{0, 1, 2\}$. This table models the belief that contact i has a potential to cause harm (P_i), for different combinations of values of W_i and R_i. Clearly, a smaller range and a warship type contact, increase this potential.

Valuation φ_{i3} specifies how variable H_i depends on W_i and B_i. This relationship is represented by logical AND operation:

$$\varphi_{i3} : \; H_i = W_i \wedge B_i, \text{ with confidence } \alpha_{i3} \in [\underline{\alpha}_{i3}, \overline{\alpha}_{i3}]. \quad (4)$$

Clearly, unusual behaviour indicates a hostile contact. The rationale for including variable W_i in (4) is that, if the contact is not of type "warship", then it is neutral and hence not hostile.

The unusual (disorderly) behaviour of a contact B_i is indicated by SL_i, AIS_i or UM_i. Hence, we express φ_{i4} using the logical disjunction:

$$\varphi_{i4} : \; B_i = SL_i \vee AIS_i \vee UM_i, \text{ with conf. } \alpha_{i4} \in [\underline{\alpha}_{i4}, \overline{\alpha}_{i4}]. \quad (5)$$

The remaining valuations in the VN of Fig. 1 are input valuations. For example, allegiance information may be received from other sources (e.g. by an optical sensor), as illustrated by the statement received at $k = 17$ in the log of Table 1. This input is represented by φ_{i5}. Similarly φ_{i6}, φ_{i7}, φ_{i8}, φ_{i9} and φ_{i10} are input valuations for variables R_i, W_i, SL_i, AIS_i and UM_i, respectively. Initially, before any of the input valuations are known, we can set them to equal the neutral element of the corresponding combination rule (in this way they express *ignorance*).

C. REPRESENTATION OF "OR", "AND" AND CPT VALUATIONS

This section explains a computer representation of valuations expressed by OR, AND and CPT.

Valuation OR appears in (1) and (5). We will explain its representation using a simple example involving three binary variables: X, Y and Z. The case with more variables is a straightforward extension of this example. Thus, consider a valuation expressed by:

$$\phi: \quad \mathrm{Z} = \mathrm{X} \vee \mathrm{Y} \text{ with confidence } \alpha \in [\underline{\alpha}, \overline{\alpha}]. \qquad (6)$$

The domain of this valuation is $d(\phi) = \{\mathrm{X}, \mathrm{Y}, \mathrm{Z}\} = \mathbf{D}$, while its frame is the Cartesian product $\Theta_{\mathbf{D}} = \Theta_X \times \Theta_Y \times \Theta_Z$. All eight configurations of $\Theta_{\mathbf{D}}$ are listed in Table 3: the configuration number is in column 1, while the configuration itself is a triple specified by columns 2, 3 and 4. Column five is the probability mass assigned to each configuration, assuming that confidence α is a precisely known value. In order to explain this column, note that there are four configurations (number 1, 4, 6 and 8) with the property $\mathrm{Z} = \mathrm{X} \vee \mathrm{Y}$ satisfied. The probability mass α is equally (uniformly) distributed among them, and thus they are allocated probability mass $\alpha/4$. The remaining $(1-\alpha)$ is equally distributed across the other four configurations (i.e. 2, 3, 5 and 7). Column six in Table 3 specifies the probability mass intervals assigned to each configuration of $\Theta_{\mathbf{D}}$. The probability intervals satisfy the conditions of *coherence* [30, Sec.2.7], [12, App. B].

TABLE 3. Computer representation of OR valuation ϕ of (6).

Config.	Z	X	Y	prob.	prob. interval
1	0	0	0	$\alpha/4$	$[\underline{\alpha}/4, \overline{\alpha}/4]$
2	1	0	0	$(1-\alpha)/4$	$[1-\overline{\alpha}/4, 1-\underline{\alpha}/4]$
3	0	1	0	$(1-\alpha)/4$	$[1-\overline{\alpha}/4, 1-\underline{\alpha}/4]$
4	1	1	0	$\alpha/4$	$[\underline{\alpha}/4, \overline{\alpha}/4]$
5	0	0	1	$(1-\alpha)/4$	$[1-\overline{\alpha}/4, 1-\underline{\alpha}/4]$
6	1	0	1	$\alpha/4$	$[\underline{\alpha}/4, \overline{\alpha}/4]$
7	0	1	1	$(1-\alpha)/4$	$[1-\overline{\alpha}/4, 1-\underline{\alpha}/4]$
8	1	1	1	$\alpha/4$	$[\underline{\alpha}/4, \overline{\alpha}/4]$

Valuation AND appears in (2) and (4). In order to explain its representation, consider a valuation expressed by:

$$\psi: \quad \mathrm{Z} = \mathrm{X} \wedge \mathrm{Y} \text{ with confidence } \beta \in [\underline{\beta}, \overline{\beta}]. \qquad (7)$$

Table 4 lists the configurations and probability masses (precise and interval valued) according to (7). There are four configurations (number 1, 3, 5 and 8) which satisfy the logical AND operation $\mathrm{Z} = \mathrm{X} \wedge \mathrm{Y}$. The probability mass β is equally distributed among them, and thus they are allocated probability mass $\beta/4$. The remaining $(1-\beta)$ is equally distributed across the other four configurations (i.e. 2, 4, 6 and 7). The probability mass intervals are given in column six of Table 4.

Valuation φ_{i2} of (4) is specified by a CPT, given in Table 5. The probability masses assigned to each configuration in column five express the domain knowledge that a smaller range (i..e a large value of R) and the warship type (i.e. W = 1) result in a higher probability that P = 1 (i.e. in a higher potential). For example, consider configuration 1: W = 0 (not a warship), R = 0 (large range), P = 0 (no potential) is assigned probability mass 1, divided by 6 for normalisation. Configuration 12 encodes the opposite situation (W = 1, R = 2 and P = 1), and is also assigned the highest probability mass. In practice probability masses in column five may be difficult to know precisely, and thus in column six we specify them as coherent intervals $[\underline{p}_{ij\ell}, \overline{p}_{ij\ell}]$.

TABLE 4. Computer representation of AND valuation, see(7).

Config.	Z	X	Y	prob.	prob. interval
1	0	0	0	$\beta/4$	$[\underline{\beta}/4, \overline{\beta}/4]$
2	1	0	0	$(1-\beta)/4$	$[1-\overline{\beta}/4, 1-\underline{\beta}/4]$
3	0	1	0	$\beta/4$	$[\underline{\beta}/4, \overline{\beta}/4]$
4	1	1	0	$(1-\beta)/4$	$[1-\overline{\beta}/4, 1-\underline{\beta}/4]$
5	0	0	1	$\beta/4$	$[\underline{\beta}/4, \overline{\beta}/4]$
6	1	0	1	$(1-\beta)/4$	$[1-\overline{\beta}/4, 1-\underline{\beta}/4]$
7	0	1	1	$(1-\beta)/4$	$[1-\overline{\beta}/4, 1-\underline{\beta}/4]$
8	1	1	1	$\beta/4$	$[\underline{\beta}/4, \overline{\beta}/4]$

TABLE 5. Computer representation of valuation φ_{i2}, see (3).

Config.	P	R	W	prob.	prob. interval
1	0	0	0	1/6	[0.99/6, 1.00/6]
2	1	0	0	0	[0.00/6, 0.01/6]
3	0	1	0	0.95/6	[0.94/6, 0.96/6]
4	1	1	0	0.05/6	[0.04/6, 0.06/6]
5	0	2	0	0.3/6	[0.29/6, 0.31/6]
6	1	2	0	0.7/6	[0.69/6, 0.71/6]
7	0	0	1	0.7/6	[0.69/6, 0.71/6]
8	1	0	1	0.3/6	[0.29/6, 0.31/6]
9	0	1	1	0.05/6	[0.04/6, 0.06/6]
10	1	1	1	0.95/6	[0.94/6, 0.96/6]
11	0	2	1	0	[0.00/6, 0.01/6]
12	1	2	1	1/6	[0.99/6, 1.00/6]

V. NUMERICAL RESULTS

A. PROBABILISTIC VN

This section shows the results obtained by running the log-scenario in Table 1 through the probabilistic VN [10] (where valuations are represented by PMFs). The combination operation in this case is the point-wise multiplication of PMFs, see [12]. The following confidence parameters were used: $\alpha_0 = 1.0$, $\alpha_{i1} = 1.0$, $\alpha_{3i} = 0.95$, $\alpha_{i4} = 0.95$, for all contacts $i = 1, 2, \dots, m_k$. The resulting threat level (i.e. the probability $Pr\{\mathrm{T} = 1\}$) as a function of time is presented in Fig. 3 with the blue solid line. Initially, at time index $k = 0$, there are no contacts and hence variable T is determined only by variable G. We have adopted input valuation φ_{G} (see Fig. 1) as a PMF, expressed as $[Pr\{G = 0\}, \quad Pr\{G = 1\}] = [0.95, \quad 0.05]$. Hence the threat level at $k = 0$ equals 0.05.

At $k = 1$, a new contact C-1 is declared. At this point of time, no additional information on this contact is known, hence we set input valuations φ_{i5}, φ_{i6}, φ_{i7}, φ_{i8}, φ_{i9} and φ_{i10} to the neutral element of the probabilistic VN: the uniform PMF of the respective variable. This results in the probability of contact C-1 threat, i.e. $Pr\{C_1 = 1\} = 0.3$, and the (overall) threat level of $Pr\{\mathrm{T} = 1\} = 0.34$ (see Fig. 3).

Based on the information received at $k = 2$, we set $\varphi_{1,7}$ to a PMF $[Pr\{W = 0\}, \quad Pr\{W = 1\}] = [0.7, \quad 0.3]$, expressing thus the uncertainty related to the statement "possible merchant ship". Valuation $\varphi_{1,8}$ is based on a categorical statement about the SL agreement, and hence

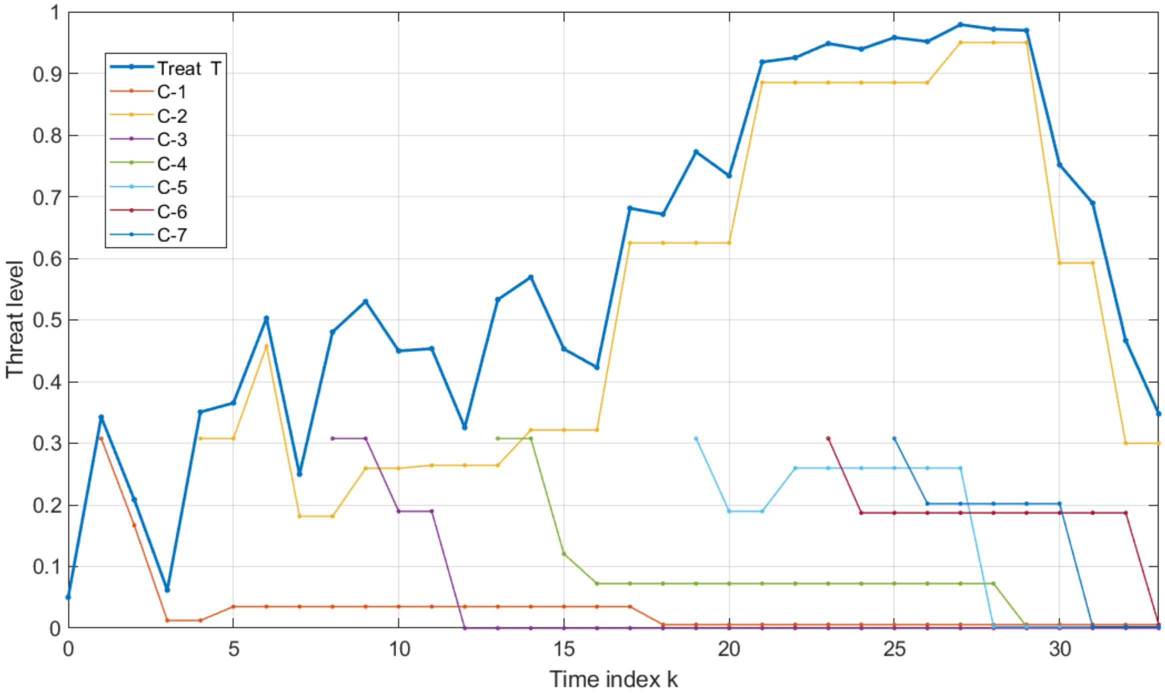

FIGURE 3. Threat level as a function of time, obtained using the Probabilistic Valuation Network. Input is the log-scenario of Table 1; output (blue solid line) is the probability $Pr\{T = 1\}$. Other lines (C-1, ..., C-7) indicate the probabilities that individual contacts are a threat.

represented by the PMF $[Pr\{SL = 0\}, \quad Pr\{SL = 1\}] = [1, \ 0]$. As a consequence, the contact threat $Pr\{C_1 = 1\}$ drops to 0.17 and the (overall) threat levels reduces to 0.21. At $k = 3$ the threat level drops even further, to $Pr\{\mathrm{T} = 1\} = 0.06$, because now we have a categorical statement that C-1 is not a warship, that is, the input valuation $\varphi_{1,7}$ is a PMF $[Pr\{W = 0\}, \ Pr\{W = 1\}] = [1.0, \ 0.0]$.

Contact C-2 is declared at $k = 4$. At this point of time, no additional information about C-2 is available, and by default $Pr\{C_2 = 1\} = 0.3$, which increases the (overall) threat level to 0.35. This contact is a genuine threat and this is soon reflected by the output of the VN. For example, at $k = 6$, when we receive the information that C-2 is a possible warship with no AIS, the threat level for the first time grows above 0.5. Because of C-2's long range, the threat level oscillates about 0.5, until $k = 17$, when it is reported at the range of 15 km (which is the critical distance when variable R changes from 0 to 1) and confirmed hostile. At that point of time, the threat level grows to 0.68. As C-2 is approaching the ownship, the threat level grows and at $k = 21$ it is above 0.9. It stays close to 1.0 until $k = 29$, when the reported range exceeds the critical distance of 15 km. As C-2 is moving away, its threat level drops and at $k = 32$ it reduces to $Pr\{C_2 = 1\} = 0.36$, while the overall threat at this tame equals $Pr\{T = 1\} = 0.47$.

Contacts other than C-2, do not pose a threat during the observation period of the log-scenario. As it can be seen from Fig. 3, their contribution to the overall threat level is significant only initially, when they are detected and reported. As soon as the new information, indicating their harmlessness, becomes available, their respective threat levels drop and consequently their contributions to the overall threat level become negligible. Indeed, note that the blue line (the overall threat T) in Fig. 3 is mainly correlated with the yellow line (the threat level of contact C-2), especially after $k = 17$.

B. CREDAL VN

Credal valuation network was developed to carry out reasoning with valuations specified as credal sets, defined by coherent probability intervals on singletons [12]. The following confidence intervals were used: $\alpha_0 \in [1.0 - \delta_1, \ 1.0]$, $\alpha_{i1} \in [1 - \delta_1, \ 1.0]$, $\alpha_{3i} \in [0.95 - \delta_1, \ 0.95 + \delta_1]$, $\alpha_{i4} \in [0.95 - \delta_1, 0.95 + \delta_1]$, for all contacts $i = 1, 2, \ldots, 7$, with $\delta_1 = 0.005$. Furthermore, the probabilities assigned to the pieces of received information in Table 1, are also expressed as intervals. For example, "possible", "likely" and "confirmed" are expressed with probability intervals $[0.7 - \delta_2, 0.7 + \delta_2]$, $[0.8 - \delta_2, 0.8 + \delta_2]$, and $[1 - \delta_2, 1]$, respectively, with $\delta_2 = 0.001$. Finally, $Pr\{G = 1\} \in [0.05 - \delta_2, 0.05 + \delta_2]$.

The theory and a practical implementation of the Credal VN are presented in [12]. The combination operation is the minimum (for lower probability) and the maximum (for the upper probability) of point-wise multiplication over all possible PMFs defined by the probability intervals. One important feature of the developed Credal VN for treat assessment deals with the implementation of the valuation

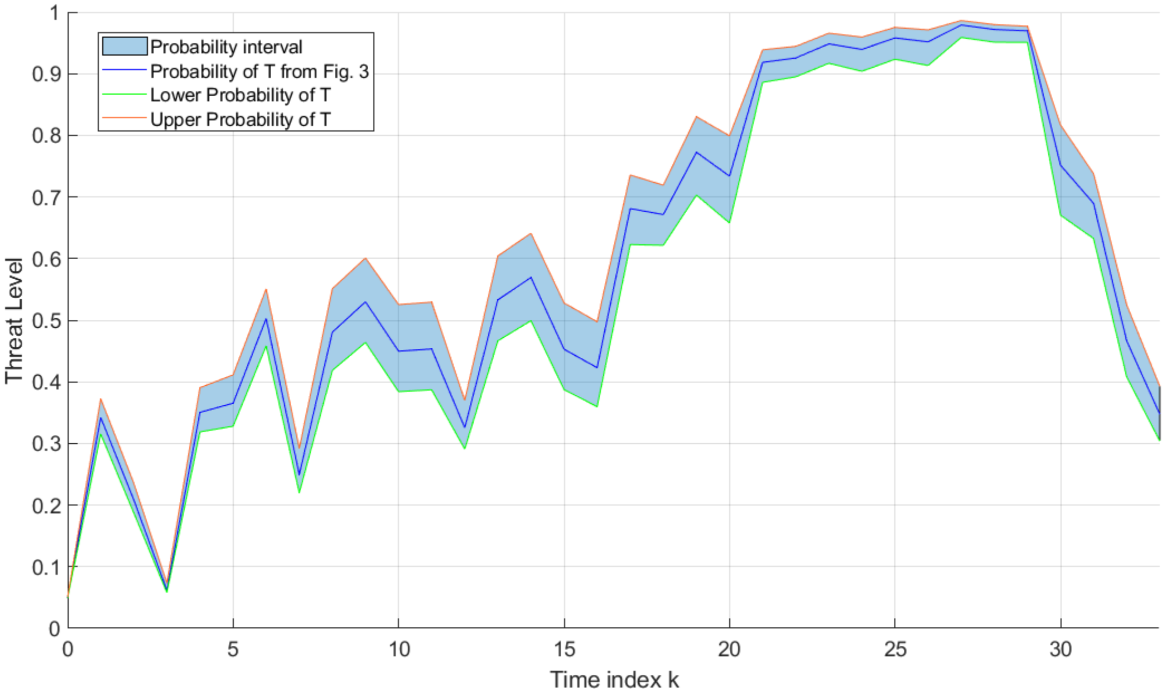

FIGURE 4. Threat level as a function of time, obtained using the Credal Valuation Network. Input is the log-scenario of Table 1; output is the probability interval for *Pr*{T = 1}. The red line is the same as *Pr*{T = 1} in Fig. 3.

φ_0 in Fig. 1. In order to speed up the computation and improve the accuracy of optimisation (i.e. minimisation and maximisation), this valuation is implemented by a pairwise OR operation over the sequence of the current number (m_k) of contacts.

Fig. 4 shows the output of the developed Credal VN: the orange and the green lines represent the resulting upper and lower probabilities, respectively. The blue line is shown only for comparison - it indicates the output of the Probabilistic VN (i.e. this is a copy of the blue line in Fig. 3). Credal Valuation Networks are used when the probabilities, assigned to prior knowledge and/or received information, are available only as the confidence intervals, rather than the precise values. In this sense, we can think of the output of the Probabilistic VN as the "ground truth", obtained in the absence of epistemic uncertainty (i.e. when all probabilistic values are known exactly). Fig. 4 shows that the output probabilistic interval, obtained in the presence of epistemic uncertainty using the Credal VN, includes at all time steps $k = 0, 1, 2, \cdots$ the "ground truth" value of $Pr\{\mathrm{T} = 1\}$. The Creadal VN is thus confirmed as a generalisation of the Probabilistic VN, capable of handling accurately the epistemic uncertainty involved in problem specification.

VI. CONCLUSION

The paper developed a valuation network for real-time threat assessment onboard an underwater vehicle. The focus was on the threat level posed by nearby contacts, while the ownship status and underwater environment were assumed favorable. Some noteworthy characteristics of the developed VN are: its structure and the level of complexity are motivated by the typical log-scenario in Table 1; it combines the threat levels of individual contacts to a single score; the scale of the VN is dynamic, as the number of nearby contacts varies with time. Two types of valuation networks were implemented and compared: (i) a Probabilistic VN, which assumes that all probabilities, expressing the uncertainty in prior knowledge and received information, are known as exact values; (ii) a Credal VN, which is able to perform reasoning using probability (confidence) intervals, rather than the precise values. The performance of the two implementations of the proposed VN have been demonstrated using a typical scenario log of an underwater vehicle navigating busy waters.

REFERENCES

[1] T. Mukherjee, "The role of artificial intelligence in naval operations," *Observer Res. Found.*, 2018, Paper 159.

[2] B. Johnson, "Artificial intelligence—An enabler of naval tactical decision superiority," *AI Mag.*, vol. 40, no. 1, pp. 63–78, Mar. 2019.

[3] E. Waltz and J. Llinas, *Multisensor Data Fusion*, vol. 685. Norwood, MA, USA: Artech House, 1990.

[4] J. Pearl, *Probabilitic Reasoning in Intelligent Systems*. San Francisco, CA, USA: Morgan Kaufmann, 1988.

[5] V. Lepar and P. P. Shenoy, "A comparison of Lauritzen–Spiegelhalter, Hugin and Shenoy–Shafer architectures for computing marginals of probability distributions," in *Proc. 14th Conf. Uncertainty Artif. Intell.*, 1998, pp. 328–337.

[6] S. L. Lauritzen and D. J. Spiegelhalter, "Local computations with probabilities on graphical structures and their application to expert systems," *J. Roy. Stat. Soc. Ser. B, Stat. Methodology*, vol. 50, no. 2, pp. 157–194, Jan. 1988.

[7] S. L. Lauritzen and F. V. Jensen, "Local computation with valuations from a commutative semigroup," *Ann. Math. Artif. Intell.*, vol. 21, no. 1, pp. 51–69, 1997.

[8] G. Shafer, *A Mathematical Theory of Evidence*. Princeton, NJ, USA: Princeton Univ. Press, 1976.

[9] 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, USA: Morgan Kaufmann, 1990, pp. 575–610.

[10] J. Kohlas, *Information Algebras: Generic Structures for Inference*. London, U.K.: Springer, 2003.

[11] P. P. Shenoy, "Using possibility theory in expert systems," *Fuzzy Sets Syst.*, vol. 52, no. 2, pp. 129–142, Dec. 1992.

[12] B. Ristic, A. Benavoli, and S. Arulampalam, "Credal valuation networks for machine reasoning under uncertainty," *IEEE Trans. Artif. Intell.*, vol. 5, no. 1, pp. 51–60, Jan. 2024.

[13] R. G. Almond, *Graphical Belief Modeling*. London, U.K.: Chapman, 1995.

[14] R. Haenni, "Ordered valuation algebras: A generic framework for approximating inference," *Int. J. Approx. Reasoning*, vol. 37, no. 1, pp. 1–41, Aug. 2004.

[15] A. Benavoli, B. Ristic, A. Farina, M. Oxenham, and L. Chisci, "An application of evidential networks to threat assessment," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 45, no. 2, pp. 620–639, Apr. 2009.

[16] J. D. Singer, "Threat-perception and the armament-tension dilemma," *J. Conflict Resolution*, vol. 2, no. 1, pp. 90–105, Mar. 1958.

[17] N. Okello and G. Thorns, "Threat assessment using Bayesian networks," in *Proc. 6th Int. Conf. Inf. Fusion*, 2003, pp. 1102–1109.

[18] Z.-H. Fan, B.-H. Shi, J.-Y. Chen, and T.-L. Duan, "A novel dynamic Bayesian network based threat assessment algorithm," in *Proc. 4th Int. Conf. Syst. Informat. (ICSAI)*, Nov. 2017, pp. 611–615.

[19] H. Yao, H. Wang, Y. Li, Y. Wang, and C. Han, "Research on unmanned underwater vehicle threat assessment," *IEEE Access*, vol. 7, pp. 11387–11396, 2019.

[20] S. Niu, H. Wang, Y. Gu, W. Gao, H. Tong, and H. Wang, "Research on UUVs swarm threat assessment and strategy selection," in *Proc. Oceans*, Oct. 2020, pp. 1–6.

[21] D. Li, M. Liu, and S. Zhang, "Underwater target threat assessment method based on Bayesian network," in *Proc. 40th Chin. Control Conf. (CCC)*, Jul. 2021, pp. 3363–3367.

[22] K. S. O. Tan and S. S. Tng, "An integrated maritime reasoning and monitoring system," in *Proc. 15th Int. Conf. Inf. Fusion*, Jul. 2012, pp. 1345–1350.

[23] G. Pilato, A. Augello, M. Missikoff, and F. Taglino, "Integration of ontologies and Bayesian networks for maritime situation awareness," in *Proc. IEEE 6th Int. Conf. Semantic Comput.*, Sep. 2012, pp. 170–177.

[24] Y. Jinyong, L. Keke, and W. Wenjing, "Ship-aircraft joint situation assessment by using fuzzy dynamic Bayesian network," in *Proc. IEEE Int. Conf. Unmanned Syst. (ICUS)*, Oct. 2017, pp. 220–224.

[25] S. Kumar and B. K. Tripathi, "Modelling of threat evaluation for dynamic targets using Bayesian network approach," *Proc. Technol.*, vol. 24, pp. 1268–1275, Jan. 2016.

[26] L. Hammond, "An evidential network approach applied to threat evaluation in above water warfare," Defence Sci. Technol. Group, Tech. Rep., DST Group-TR-3349, Edinburgh, SA, Australia, 2017.

[27] P. Kowalski, M. Zocholl, and A.-L. Jousselme, "Explainability in threat assessment with evidential networks and sensitivity spaces," in *Proc. IEEE 23rd Int. Conf. Inf. Fusion (FUSION)*, Jul. 2020, pp. 1–8.

[28] A. Benavoli and B. Ristic, "Evidential networks for decision support in surveillance systems," in *Integrated Tracking, Classification, and Sensor Management*, M. Mallick, V. Krishnamurthy, and B.-N. Vo, Eds. Hoboken, NJ, USA: Wiley, 2013, ch. 17, pp. 661–704.

[29] 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, NY, USA: Wiley, 1992, ch. 4, pp. 83–104.

[30] P. Walley, *Statistical Reasoning With Imprecise Probabilities*. London, U.K.: Chapman, 1991.

[31] L. M. De Campos, J. F. Huete, and S. Moral, "Probability intervals: A tool for uncertain reasoning," *Int. J. Uncertainty, Fuzziness Knowl.-Based Syst.*, vol. 2, no. 2, pp. 167–196, Jun. 1994.

BRANKO RISTIC received the Ph.D. degree from Queensland University of Technology, in 1995. He held various research/engineering positions in former Yugoslavia and Australia, until he joined the Defence Science and Technology Organization, in 1996. Since 2015, he has been a Principal Research Fellow with the School of Engineering, RMIT University. He coauthored two books, such as *Beyond the Kalman Filter: Particle Filters for Tracking Applications* (Artech House, 2004) and *Particle Filters for Random Set Models* (Springer, 2013), as well as over 100 journal articles. His research interests include information fusion, Bayesian estimation, target tracking, Monte Carlo methods, search techniques, sensor control, and machine reasoning under uncertainty.

AMANDA BESSELL received the Bachelor of Computer Science and Master of Science degrees in signal and information processing from The University of Adelaide, South Australia, in 2001 and 2007, respectively. She is currently a Senior Researcher with the Information Sciences Division, Defence Science and Technology Group. Her research interests include estimation theory, target tracking, data fusion, and sensor control.

SANJEEV ARULAMPALAM (Senior Member, IEEE) received the Ph.D. degree in electrical and electronic engineering from The University of Melbourne, Melbourne, VIC, Australia, in 1998. In March 2000, he was a recipient of the Anglo-Australian Postdoctoral Research Fellowship, awarded by the Royal Academy of Engineering, London, U.K. This postdoctoral research was carried out in the U.K., both at the Defence Evaluation and Research Agency and at Cambridge University, where he worked on particle filters for nonlinear tracking problems. Recently, he was a Chief Defence Scientist Fellow, investigating multimodal information fusion for undersea warfare to support research with the Undersea Command and Control Branch of Maritime Division, Defence Science and Technology Group (DSTG), Australia. He is currently a Senior Scientist with the Maritime Division, DSTG, and an Adjunct Professor with The University of Adelaide. He has coauthored the book *Beyond the Kalman Filter: Particle Filters for Tracking Applications* (Artech House, 2004). His research interests include estimation theory, target tracking, and sequential Monte Carlo methods. He was a recipient of the 2018 IEEE Signal Processing Society's Donald G. Fink Award for one of his papers for its substantial impact over several years.