Proceedings of the 2015 ORSSA Annual Conference
pp. 123–133
www.orssa.org.za/wiki/uploads/Conf/2015ORSSAConferenceProceedings.pdf

ORSSA Proceedings
ISBN
978-1-86822-666-5

Value-based methods for threat value fusion within a ground-based air defense environment

ML Truter* JH van Vuuren†

Abstract

The ability to estimate accurately the threat levels posed by aircraft is a key factor in ensuring success when countering hostile aerial threats in a ground-based air defense environment. Threat evaluation, in this context, is the process whereby aerial threats are prioritised according to the estimated level of danger they pose to the defended system. This process is a high-level information fusion problem aimed at enhancing decision making by fire control officers who are responsible for solving the threat evaluation problem in real time, in order to counter threats effectively. Some context to the process of threat evaluation is provided in this paper, after which a novel data fusion process is proposed which employs two value-based fusion methods in conjunction with one another — a multi-attribute utility function method and an additive aggregation method.

Key words: Threat evaluation, High-level data fusion, Ground-based air defense, Decision support, Aggregation.

1 Introduction

In a *Ground-Based Air Defense* (GBAD) scenario, numerous *Defended Assets* (DAs) are distributed over a geographical region and are afforded protection by a variety of weapon systems which are, in turn, used to counter hostile aircraft [8]. In order to protect the DAs, it is important to be able to quantify the threat level posed by each aircraft to the defended system. This is required so as to understand the risk associated with each aircraft and, consequently, facilitate selection of a suitable countering strategy.

A so-called *Threat Evaluation* (TE) process is an important input process to the weapon assignment process in order to ensure that available ground-based resources (weapons and

*Stellenbosch Unit for Operations Research and Engineering, Department of Industrial Engineering, Stellenbosch University, Private Bag X1, Matieland, 7602, South Africa, email: louw.truter@gmail.com

†**(Fellow of the Operations Research Society of South Africa)**, Stellenbosch Unit for Operations Research and Engineering, Department of Industrial Engineering, Stellenbosch University, Private Bag X1, Matieland, 7602, South Africa, email: vuuren@sun.ac.za

ammunition) are effectively utilised to defend the DAs. The threat value fusion problem consists of acquiring a comprehensive overview of the level of threat posed by each aircraft in respect of the entire defended system of assets.

TE is achieved by employing aircraft-related data obtained from sensor systems and associated information obtained from pre-programmed data bases (*e.g.* threat-specific information and doctrinal procedures) in order to quantify the threat level posed by detected aerial threats in respect of the defended system. A major concern during this TE process, when different TE models are employed in conjunction with one another, is the fusion of the different threat values returned by these models into a single representative *system threat value*[1].

This paper is structured as follows: An overview of the processes of TE and weapon assignment is provided in §2 within the context of decision support. After introducing the type of *Decision Support System* (DSS) typically employed in this context and various levels of data fusion, the TE process typically implemented is described in §3. This is followed in §4 by an explanation of the proposed data fusion process, with an emphasis on the construction of the utility function and the method of fusion of the different types of threat values. A hypothetical example is used in §5 to illustrate these concepts. The paper closes in §6 with some ideas for future work.

2 Threat evaluation in context

The tasks of analysing aerial threats and assigning ground-based weapon resources to counter these threats in a GBAD environment are the responsibility of a *Fire Control Officer* (FCO). Generally, a *Threat Evaluation and Weapon Assignment* (TEWA) DSS is employed by the FCO to aid him with the processes of TE and weapon assignment. Such a TEWA DSS is, in essence, typically a hybrid DSS and expert system, because it usually employs both computerised analytical methods and heuristic rules[2] to aid the decision making processes of the operator. The functional architecture of such a DSS is depicted in Figure 1. The figure is interpreted in this section with reference to the various levels of information in the well-known (updated) JDL II data fusion model [10].

In Figure 1 it may be seen that the input information required by a TEWA DSS is a combination of real-time sensor data and pre-programmed domain expert knowledge. The real-time sensor data usually include the positional and kinematic data of the detected threats and normally have to be fused together from various sensor sources. This level 0 (source preprocessing) data fusion process, is generally performed within the sensors [10]. The knowledge base, on the other hand, typically includes pre-deployment data on enemy arsenals, threat types and electro-magnetic signatures of known threats.

The data processor unit is a level 1 (object assessment) data fusion process. This process is concerned with the estimation and prediction of relations between the entities (threats,

[1] A *system threat value* provides a holistic view of the level of threat that each aerial threat poses to the defended system as a whole and is, in turn, used within a weapon assignment objective function in an attempt to optimise the assignment of weapon systems.

[2] Heuristic rules are typically developed through experience, intuition and judgment [4].

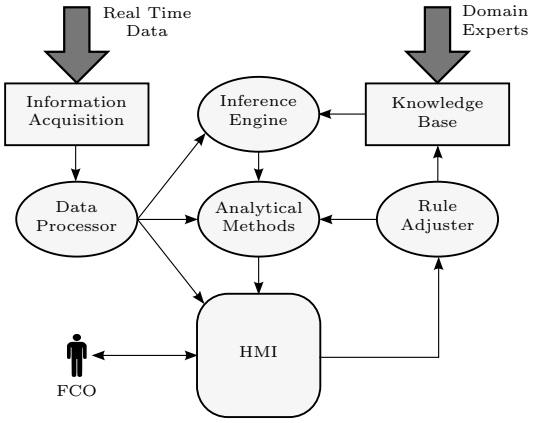

Figure 1: *Functional architecture of a typical TEWA DSS (adapted from [4]).*

DAs) and their relation to the environment, in order to develop the current situational picture from which further impact assessments can be performed. Typical functionality of this component may include triangulation and aircraft track extraction. The inference engine, on the other hand, is a level 2 (situation assessment) data fusion process. This process utilises a combination of the data from the data processor and pre-deployment data from the knowledge base to infer certain characteristics of the threats (threat type, weapon envelope, *etc.*) by using a combination of context-based reasoning, pattern recognition techniques and heuristic rules.

The analytical methods process is the focus area of this paper. This process includes the TE and weapon assignment processes; both are level 3 (impact assessment) data fusion processes. During these processes, the levels of threat of the different aircraft are determined and counter attacks devised [2]. Finally, the results of the TE and weapon assignment processes are displayed on the *Human Machine Interface* (HMI) and the FCO can interact with these solutions in order to select a suitable course of action.

The FCO can usually interact with the HMI through the rule adjuster component so as to configure certain analytical methods for the TE and weapon assignment processes, or update and modify the existing information in the knowledge base. This will ensure that the DSS complements the FCO's analysis style and enhances the FCO's confidence in the DSS.

3 The threat evaluation process

Roux and Van Vuuren [8] proposed three levels of TE models of varied complexity. In order of increasing complexity, they are flagging models, *Deterministic Models* (DMs) and stochastic models. Flagging models are binary in nature and are activated when certain threshold violations occur (*e.g.* sudden increases in altitude or dropping of paratroopers). Stochastic models are probability-based and require detailed information on enemy arsenals, threat types and doctrine. The focus in this paper is only on DMs.

DMs utilise the measured kinematic data from sensors, and calculate derived attributes

which are collectively used to estimate an aircraft's threat value. The estimation criteria used by DMs may include the time to weapon release, or any course, heading or distance-related measure. For the implementation of these models, basic pre-deployment information, such as DA positions, importance values of the different DAs and, in some cases, their orientations as well as the maximum turn radii of attacking aircraft, are required [9]. As a result, the exact input information required depends on the specific DM implemented. Heyns and Van Vuuren [3], as well as Roux and Van Vuuren [9], developed four very specific DMs with the help of domain experts. The principles on which these models rely are described in some detail in [8].

4 Proposed data fusion process

The purpose of the TE fusion component within the TEWA cycle is to combine the results from the various DMs. This fusion must be achieved in a manner that is not only mathematically tractable, but also practical for use in real-world military applications.

All DMs produce a threat value on the real interval $[0, 1]$. The aim of the fusion process should therefore be to construct a value-based prioritised list of threats, based on their system threat values. Value-based in this context refers to a cardinal prioritised list, as opposed to an ordinal list. Multiple techniques for this purpose exist in the field of *Multi-Attribute Utility Theory* (MAUT) [5]. These different techniques may be classified as *value measurement models*, *goal aspiration models* or *outranking models*.

Value-based measurement models are the only models in which a numerical preference score is calculated pertaining the degree to which a certain alternative may be preferred above another. The results are therefore quantitative in nature and the level of preference of one alternative to another is retained during fusion.

When utilising the DMs referred to in the previous section, a threat value is determined for each threat-DA-DM triple. If there are, for example, three incoming threats, two DAs to protect, and four different DMs, then a total of 24 different threat values will therefore be calculated. The output of the TE subsystem should, however, be a single system threat value for each threat in order for the weapon assignment subsystem to function effectively.

The purpose of our proposed data fusion process is to fuse together these different threat values — which are distinguished according to threat, DA and DM — so as to obtain a single system threat value per threat. Different hierarchies of threat values are shown in Figure 2. Since the DMs are typically configured differently, the first step should be to obtain a threat value with respect to each threat-DA pair (*i.e.* to fuse together the threat values obtained by the different DMs). After obtaining the theat-DA threat list thus fused, the importance weights of the DAs may finally be used to fuse together a single system threat value for each threat.

4.1 Computation of threat-DA pair threat values

Evaluation of threat values according to the DMs described in §3 is updated each time new information is received from the sensor systems, the duration of this update-cycle is

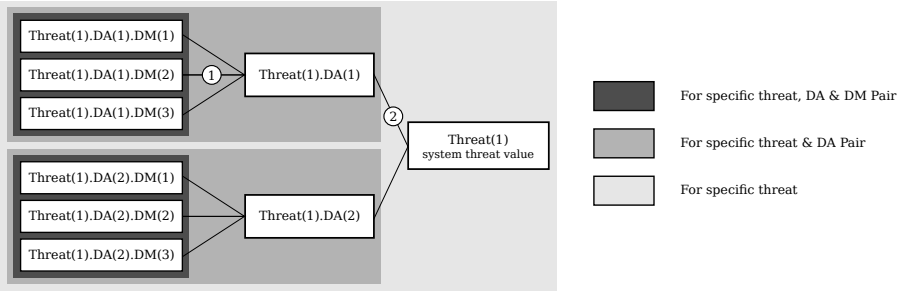

Figure 2: *Relationships between different threat values. Fusion process (1) involves multi-attribute utility functions within an aggregated value function tree in order to obtain an individual threat value per DA. Fusion process (2) involves the additive weighting method, where the weighting coefficients are the normalized importance values of the DAs.*

known as the TEWA *cycle time*. Consequently, the deterministic threat values are updated throughout the engagement as the threats approach the DAs.

This calls for a fusion model which is dynamic in nature. Furthermore, as threats approach the DAs, certain DMs become more accurate or relevant in estimating an aircraft's threat level. For fixed-wing aircraft, for instance, when threats are far from the DAs, the time-to-weapon-release may be a better predictor of threat level than distance-related threat measures. To illustrate, at long ranges when two threats are executing the approaching phases of their attack profiles at the same distance from the DAs, time should be a better predictor of threat level. Although they are the same distance from the DAs, the threat with the higher velocity poses a more imminent danger to the DAs, since it would be able to release its weapons earlier. In contrast, if threats are entering the manuevre phases of their attack profiles (in anticipation of weapon release), distance-related measures ought to be a better predictor of threat level, since time-related measures become increasingly difficult to predict accurately during these final phases of the attack profile.

It is therefore clear that a multi-attribute utility function is required in which the attributes are the DMs. The utility function should provide a single threat value for each threat-DM pair, where the fused threat value depends on the threat values of the DMs combined. For illustrative purposes, three spatial DMs are considered — a slant distance model, a passing distance model[3] and an altitude-related model. These three models were specifically chosen in order to adhere to the requirements of utility- and preferential independence when constructing a multi-attribute utility function.

In order to construct the utility function, it is first required to quantify the preferences of the end-users. To this end, the threat-value interval may be subdivided into three intervals; the midpoints of these intervals may then represent respectively high (0.83), medium (0.5) and low (0.16) threat values. This concept is illustrated in Figure 3.

The intervals in Figure 3 are suggested in order to facilitate effective elicitation of end-user

[3]The implemented passing distance model is generally referred to as the *Closest Point of Approach* (CPA) model in the literature. Passing distance is used here in order to aid understanding to a non-military readership.

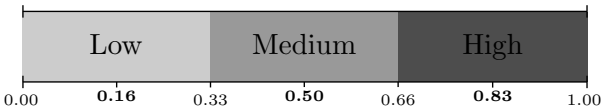

Figure 3: *Threat value intervals.*

preferences. It is anticipated that domain experts should be able to provide an appropriate or expected combined threat value when the threat value of an altitude DM and a passing distance DM are low, for instance, but that of a slant distance DM is high. This elicitation process may be repeated for all the different combinations of the DM threat levels in order to obtain a combined or characteristic threat value for each triple. This is required in order to serve as input for the construction of an accurate and robust utility function for the fusion process.

In an attempt to limit the amount of personal subjectivities of domain experts and to address the difficulties when aggregating individual preferences, it is advocated that a group of military experts attend a workshop and discuss the different alternatives for each of the criteria, with the goal of reaching group consensus in respect of input values for construction of the utility function.

Hypothetical threat values for the aforementioned combinations were selected for use in a proof-of-concept example. MATLAB was used to fit various functions through the resulting 27 data points. It was determined that a third degree, three-variable polynomial provides the best fit. The resulting function,

$$\Gamma(\gamma, \rho, \eta) = \sum_{i=0}^{3} \sum_{j=0}^{3} \sum_{k=0}^{3} a_{ijk} \gamma^i \rho^j \eta^k, \tag{1}$$

returns a fused characteristic threat value in the real interval $[0, 1]$ for a specific threat-DA pair. In (1), the symbols γ, ρ and η denote slant distance, passing distance and altitude DM threat values, respectively. The values of the coefficients a_{ijk} are shown in Table 1. All values not in the table assume a value of zero.

Table 1: *Coefficients for the multi-attribute utility function (1).*

$a_{000} = -0.12$	$a_{100} = 1.3$	$a_{200} = -1.2$	$a_{300} = -0.48$	$a_{110} = -0.74$	$a_{210} = 0.52$	$a_{101} = -1.8$
$a_{201} = 1.5$	$a_{010} = 0.45$	$a_{020} = 0.31$	$a_{030} = -0.21$	$a_{001} = 0.42$	$a_{002} = 0.8$	$a_{003} = -0.54$

4.2 Threat-DA threat value scaling

Another consideration in the fusion process, not described above, is the scaling of threat values. TE is typically conducted on all threats within an *Area of Responsibility* (AOR) which are identified as hostile or unknown. Doctrine often requires that if a threat enters a prespecified distance from a DA — here referred to as the *Keep-Out Boundary* (KOB) — the threat must be classified as highly threatening with respect to the DA considered. If the assumption is made that threats are classified according to three priority categories,

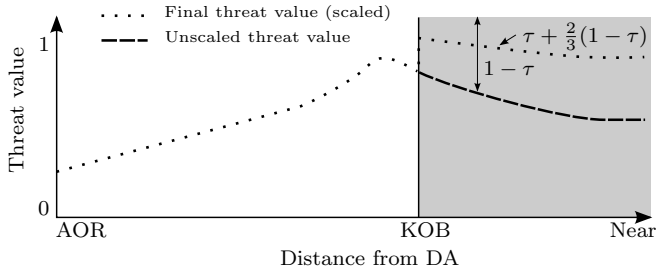

Figure 4: *Suggested threat value scaling method when threats cross the KOB.*

namely low, medium and high (as illustrated in Figure 3), then the scaling should ensure that any threat is classified as highly threating when it enters the KOB.

The scaling should therefore make provision for increasing the threat priority of low and medium threats to high priority when a threat crosses the KOB. It is advocated that the threat value τ of a threat crossing the KOB should be increased by $\frac{2}{3}(1-\tau)$, as illustrated in Figure 4. This scaling of the threat values will ensure that the low and medium threats are always classified as highly threatening threats when inside the KOB. This is true if the threat values τ of the classes of low, medium and high priority threats occupy the ranges $0-\frac{1}{3}$, $\frac{1}{3}-\frac{2}{3}$ and $\frac{2}{3}-1$, respectively. In practice, however, the scaling value (suggested here to be $\frac{2}{3}$) should be agreed upon by domain experts. The result of this process is a scaled threat-DA threat list.

4.3 Computation of system threat values

After calculating a single threat value for each threat-DA pair, it is required to fuse these values together in order to obtain a system threat value for each threat. One way to achieve this is to use the importance value of each DA as a linear weight applied within the additive weighted method. A linear weighting may be applied to all the criteria independently in order to obtain a system threat value for each threat.

The relative DA importance weights should be determined prior to system implementation and should therefore be stored in the knowledge base. Each DA usually has an importance value assigned to it by the defending force. This importance value quantifies the relative importance to the defending force of protecting the DA in question. Several variables may influence the importance of a specific DA, such as its repairability, vulnerability and vital importance [7].

Repairability of a DA refers to its ability to recover from damage inflicted to it, and is usually determined based on the manpower, equipment and time required to repair the asset to a functioning state. *Vulnerability*, on the other hand, refers to the extent to which an asset is susceptible to damage and surveillance during an attack. Armour, position, countermeasures and camouflage are factors which influence a DA's vulnerability. Finally, *vital importance* is the degree to which the mission's success relies on a specific DA. Assessing the impact that the destruction of an asset will have on the mission's success is one way of determining its vital importance value. A command centre, for example, is more important in respect of ensuring mission success (for maintaining command and

control superiority) than a redundant (backup) sensor system.

The DA importance values, together with the threat-DA threat values, may be fused together by an additive weighting function to obtain the system threat value

$$V_a = \sum_{k=1}^{n_D} v_{k,a} \cdot \psi_k$$

associated with threat $a \in \{1, \ldots, n_T\}$, where ψ_k denotes the normalised importance value of DA $k \in \{1, \ldots, n_D\}$. Furthermore, $v_{k,a}$ represents the (fused) threat value of threat a and DA k pair. The total number of DAs is denoted by n_D and the total number of threats by n_T.

5 Worked example

A worked example is provided in this section in order to illustrate and clarify the concepts of the preceding sections. A hypothetical ground-based air defense scenario is illustrated in Figure 5. In this figure the threat paths of three threats are indicated by the three lines, and the positions of two DAs are depicted by black dots. The differently colored domes represent the single-shot hit probability distribution volumes of two ground-based weapon systems which are indicated by the two crosses. The weapon systems are only included for the sake of completeness and their assignment does not form part of this worked example.

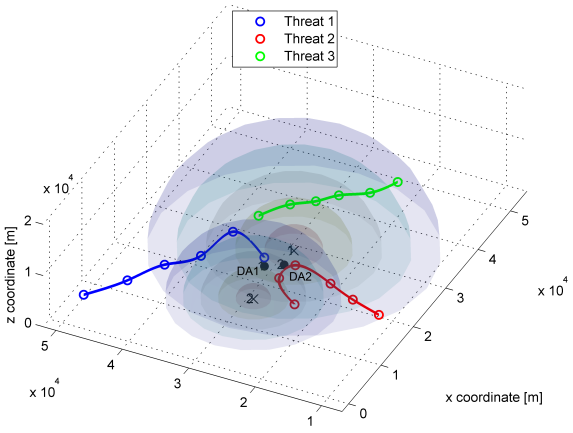

Figure 5: *Hypothetical ground-based air defense scenario.*

The threat tracks in Figure 5 correspond to a scenario spanning 120 seconds. For the purpose of this example, the TEWA cycle is repeated every second (*i.e.* the real-time data updates are assumed every second). Furthermore, only three spatial DMs are implemented — a slant distance model, a passing distance-related model and an altitude-related model. The resulting threat values are shown in Figure 6 as a function of time.

Although the DMs are unaware of this, Threat 1 is executing a pitch-and-dive attack manoeuvre in respect of DA 2. Threat 2, on the other hand, is executing a toss-bomb

attack manoeuvre in respect of DA 1. Finally, Threat 3 is a passenger aircraft passing over the conflict zone and therefore poses no real threat. Threat 3 is only present to ascertain the response of the TE algorithms in the case where an aircraft is not attacking the DAs.

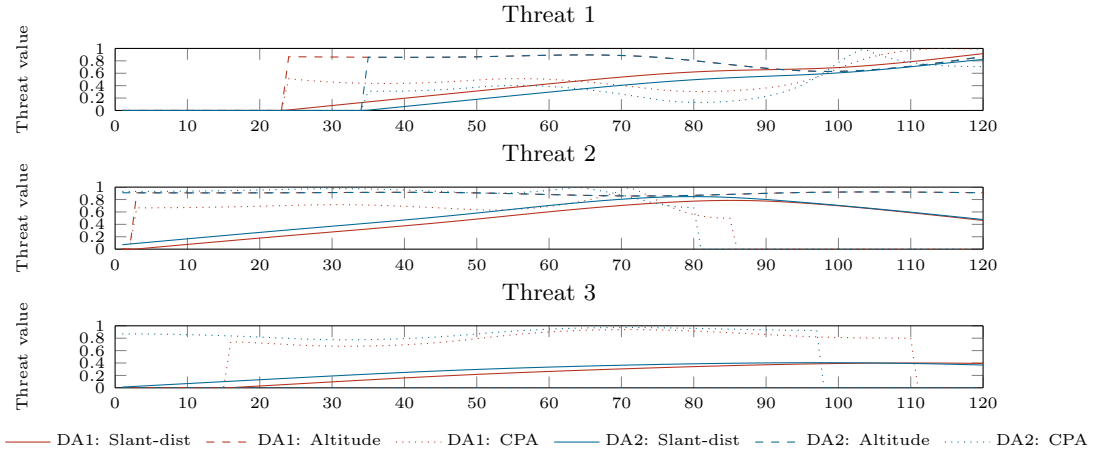

Figure 6: *Original threat values; distinguished in terms of threat, DA and DM.*

The threat values shown in Figure 6 were fused together in order to obtain a single threat value for each threat-DA pair. This fusion process was achieved using the aggregated value function approach described in §4.1. The $\frac{2}{3}$–KOB scaling referred to at the end of §4.3 was subsequently applied to the unscaled threat-DA threat list.

After obtaining the scaled threat-DA threat value list, these threat values were fused together using the normalised importance weights of the DAs. The additive weighting method described in §4.3 was used for obtaining the system threat values shown in Figure 7. These threat values may be used for ground-based weapon assignment purposes.

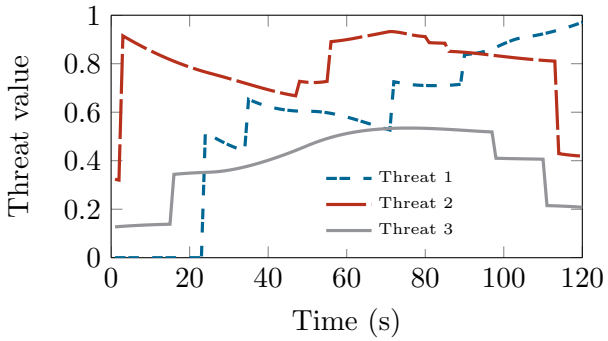

Figure 7: *System threat values as a function of time.*

From Figure 7 it is clear that the threat values provide realistic treat estimates of the various threats. The sudden rises and drops in threat values occur when certain models are "switched on" or "switched off." For example, a threat must be within the prespecified AOR radius before TE is conducted in respect of the threat. Similarly, the passing distance-related DM is also only active if the threat is heading towards a DA. It is worth mentioning that Threats 1 and 2 are scheduled to release their weapons at approximately times 90 and 60, respectively. It is therefore encouraging to note that the

fused threat values of these threats are at their highest levels close to the weapon release stage. Finally, it is heartening that the threat values associated with Threat 3 which is, in fact, not exhibiting threatening behaviour, is significantly lower than those of Threats 1 and 2.

Rapid changes in the threat values may be of concern to the effective functioning of the TEWA system, as described by Lötter and Van Vuuren [6]. The rapid changes in threat values, observed at times 3, 22, 37, 58, 72, 91 and 116 in Figure 7, may result in switching of weapon assignment recommendations. This switching is a typical emergent property of TEWA systems and is something that must be fully understood before implementing such systems. These switching recommendations may cause confusion on the part of the operator. An analysis of the extent of this switching behaviour is something that is an aspect of our current research. Several mitigation strategies are being investigated to alleviate this problem. Allouche [1] did similar work by implementing Kohonen's self-organising maps for the stabilisation of threat values. Threat value stabilisation was achieved by smoothing the observed real-time trajectory of the threats (anti-ship missiles in his case).

6 Conclusion and future work

The work reported in this paper forms part of a larger project which entails the performance evaluation of TEWA algorithms developed during the period 2006–2010 at Stellenbosch University, as described in [11]. Although the focus here is on higher level data fusion processes (levels 2–3 in the JDL fusion model), it is nevertheless important also to consider the effects that inaccurate, noisy input information may have on the output values of the TEWA algorithms. The performance evaluation of the system will therefore include an investigation into the sensitivity of various system parameters as well as the effects of uncertain input information on the system.

References

[1] Allouche MK, 2005, *Real-time use of Kohonen's self-organizing maps for threat stabilization*, Information Fusion, **6(2)**, pp. 153–163.

[2] Falzon L, 2006, *Using Bayesian network analysis to support centre of gravity analysis in military planning*, European Journal of Operational Research, **170(2)**, pp. 629–643.

[3] Heyns AM, 2008, *Measuring the threat value of fixed wing aircraft in a ground based air defense environment*, MSc Thesis, Stellenbosch University, Stellenbosch.

[4] Ignizio JP, 1991, *An introduction to expert systems*, 1st Edition, McGraw-Hill, New York (NY).

[5] Keeney RL & Raiffa H, 1993, *Decisions with multiple objectives: Preferences and value tradeoffs*, 1st Edition, Cambridge University Press, Cambridge.

[6] Lötter DP & Van Vuuren JH, 2014, *Implementation challenges associated with a threat evaluation and weapon assignment system*, Proceedings of the 43rd Annual Conference of the Operations Research Society of South Africa, pp. 27–35.

[7] Roux JN, 2010, *Design of a threat evaluation subsystem in a ground-based air defence environment*, PhD Thesis, Stellenbosch University, Stellenbosch.

[8] Roux JN & Van Vuuren JH, 2008, *Real-time threat evaluation in a ground based air defence environment*, ORiON, **24(1)**, pp. 75–101.

[9] Roux JN & Van Vuuren JH, 2007, *Threat evaluation and weapon assignment decision support: A review of the state of the art*, ORiON, **23(2)**, pp. 151–187.

[10] Steinberg AN & Bowman CL, 2004, *Rethinking the JDL data fusion levels*, National Symposium on Sensor and Data Fusion, **38**, pp. 39.

[11] Truter ML & Van Vuuren JH, 2014, *Prerequisites for the design of a threat evaluation and weapon assignment system evaluator*, Proceedings of the 43rd Annual Conference of the Operations Research Society of South Africa, pp. 54–61.