

# A survivability-based testbed for comparing threat evaluation algorithms

Fredrik Johansson  
 School of Humanities and Informatics  
 University of Skövde  
 Skövde, Sweden  
 Email: fredrik.johansson@his.se

Göran Falkman  
 School of Humanities and Informatics  
 University of Skövde  
 Skövde, Sweden  
 Email: goran.falkman@his.se

**Abstract**—Threat evaluation is the process in which threat values are assigned to detected targets, based upon the inferred capabilities and intents of the targets to inflict damage to blue force defended assets. This is a high-level information fusion process of high importance, since the calculated threat values are used as input when blue force weapon systems are allocated to the incoming targets, a process often referred to as weapon allocation. Threat values can be calculated from a number of different parameters, such as the position of the closest point of approach (CPA) with respect to blue force defended assets, time required to reach the CPA, the target’s velocity, and its type. A number of algorithms for calculating threat values have been suggested throughout literature, however, criteria to evaluate the performance of such algorithms seem to be lacking. In this paper, we discuss different ways to assess the performance of threat evaluation algorithms. In specific, we describe how threat evaluation algorithms can be compared to each other, using a survivability criterion. Survivability is measured by running the threat evaluation algorithms on simulated scenarios and using the resulting threat values as input to a weapon allocation module. Depending on how well the threat evaluation is performed, the ability of the blue force weapon systems to eliminate the incoming targets will vary (and thereby also the survivability of the defended assets).

## I. THREAT EVALUATION AND WEAPON ALLOCATION

Consider a tactical air defense situation consisting of a set  $\mathbf{W} = (W_1, \dots, W_M)$  of weapon systems, a set  $\mathbf{T} = (T_1, \dots, T_N)$  of air targets, and a set  $\mathbf{A} = (A_1, \dots, A_P)$  of defended assets. The task of the air defense is to evaluate the tactical situation in real-time, and to protect the defended assets by allocating available weapon systems to threatening enemy targets [1]. In an air defense situation, such threats are mainly comprised of aircrafts and missiles [2].

For each target-defended asset pair  $(T_i, A_j)$ , where  $T_i \in \mathbf{T}$  and  $A_j \in \mathbf{A}$ , a threat value  $V_{ij} \in [0, 1]$  is assigned, representing the degree of threat that the target  $T_i$  poses to the defended asset  $A_j$ . These can be combined into a single threat value  $V_i$  for each target  $T_i$ , by applying the equation

$$V_i = \frac{\sum_{j=1}^P V_{ij} S_j}{|\mathbf{A}|}, \quad (1)$$

where  $S_j$  is a user-defined parameter, denoting the protection value of a defended asset  $A_j$ , and  $|\mathbf{A}|$  is the total number of defended assets. The process of threat value calculation is known as threat evaluation. The results from the threat

evaluation can be used for weapon allocation, i.e. the reactive assignment of weapon systems to engage identified threats [3]. From a static perspective, the weapon allocation problem can be seen as an optimization problem (shown to be NP-complete [4]) in which we would like to find a solution that minimizes the total expected value of the surviving targets [5]:

$$F^* \equiv \min_{x_{ik} \in \{0,1\}} F = \sum_{i=1}^N V_i \prod_{k=1}^M (1 - P_{ik})^{x_{ik}}, \quad (2)$$

$$\text{subject to } \sum_{i=1}^N x_{ik} = 1, \quad k = 1, \dots, M. \quad (3)$$

In the above equations,  $P_{ik}$  (often referred to as a kill probability) is the probability that weapon  $k$  destroys target  $i$  if it is assigned to it, while  $x_{ik}$  is a decision variable with two possible states (1 if weapon  $k$  is assigned to target  $i$ , and 0 otherwise). The constraint in equation 3 indicates that each weapon system must be allocated to exactly one target. This static problem is a simplification, since it assumes that all weapon systems are allocated and fired simultaneously. In the real world, threat values and kill probabilities change over time. Hence, threat evaluation and weapon allocation should not be performed at a single point in time, but rather in an iterative way. This can be illustrated using Boyd’s famous Observe-Orient-Decide-Act (OODA) loop (see figure 1). In

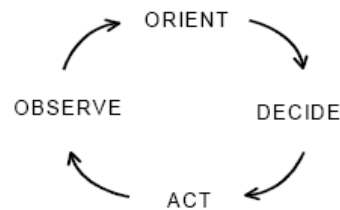


Figure 1. Simplified version of Boyd’s OODA loop

the Observe phase, data are gathered via different types of sensors in order to establish target tracks, etc. The situation is assessed in the Orient phase, using information from the Observe phase as input. In a context of air defense, this is the phase in which threat evaluation is performed. Based on

the resulting threat values, weapon systems are allocated to targets in the Decide phase. These decisions are executed in the Act phase, whereupon a damage assessment is done as a first step in the next cycle of the OODA loop, and so on. In this dynamic version of the weapon-target allocation problem the defense will not waste as many resources to targets that already have been engaged, since it can use a shoot-look-shoot strategy [5].

Since we in both the static and dynamic version of the weapon-target allocation problem strive to minimize the total expected value of the surviving targets, a question becomes how to calculate threat values,  $V_{ij}$ , for target-defended asset pairs (which later on can be summed together using equation 1). The threat of a target should according to literature [6], [7] be assessed as a combination of its capability and intent to damage the defended assets. Examples of parameters that can be used for threat evaluation are target type, position of the closest point of approach (CPA) with respect to blue force defended assets, time required to reach the CPA, and the target's velocity [8]. The values of the chosen parameters are then to be used as input for the computation of a threat value for each target-defended asset pair. Available algorithms for calculating threat values are sparse, at least in the open literature [8]. The two main approaches for threat evaluation that can be found in literature are rule-based algorithms and graphical models (e.g. Bayesian networks) [8], [9].

## II. COMPARISON AND PERFORMANCE EVALUATION OF THREAT EVALUATION ALGORITHMS

We have in an earlier paper [9] compared the resulting threat values from two different threat evaluation implementations tested on a simulated air defense scenario. In the same paper, we have compared the characteristics of the methods which the two implementations are built upon (Bayesian networks and fuzzy inference rules). To our knowledge, there are no other comparisons between algorithms for threat evaluation within open literature (even though such comparisons have been suggested [10], [11]). The question of how to compare threat evaluation algorithms to each other is closely related to the question of how to evaluate the performance of a single threat evaluation algorithm. The usual way to do this seems to be to construct a scenario with a number of targets, run the scenario, and let the threat evaluation algorithm calculate threat values for the different targets. The changes in threat values over time are then analyzed and, in some cases, the calculated threat values are compared to human expert knowledge [10], [12], [8], [13].

A problem with the approach described above is that the evaluation becomes very limited to the specific scenario, i.e. it is hard to say something about how the threat evaluation algorithm generalizes to other (real-world) scenarios. Simply analyzing threat value deviations are quite meaningless, since we do not only want to know if and why the threat value changes, but also if the threat values are "correct". However, correctness here assumes knowledge of an objective threat value, which the calculated threat values can be compared

to. This is problematic, since it is far from obvious that two experts would assign similar threat values for a specific situation. Even though this would be the case, it still would be impossible to apply the evaluation method on more than a few scenarios at most, since a human expert would need to create the scenarios, specify threat values and how they change over time, etc.

Clearly, if threat evaluation algorithms are to be evaluated or compared on a larger scale than just a few scenarios, another evaluation method is needed. Looking at evaluation criteria of importance, we can identify factors (based on findings in [9] and discussions with experts from industry) such as:

- Sensitivity
- Adaptivity
- Transparency
- Computational complexity (time-, memory-, and CPU-consumption)
- Correctness

What we are searching for is another way to measure the correctness of threat evaluation algorithms. Our suggestion is to create simulated scenarios and calculate threat values as before. However, this time we use the calculated threat values as input to a weapon allocation module. When the scenario is over, we count the number of surviving defended assets and use this as a measure of how well the threat evaluation algorithm performed. This survivability measure is not to be confused with the minimization of the total expected value of the surviving targets, illustrated in equation 2. Survivability of the defended assets is dependent upon the complexity of the scenario (e.g. the number of targets and the number of available weapon systems), the threat evaluation and the weapon allocation. However, by keeping the weapon allocation algorithm fixed, the idea is that the conditions for different threat evaluation algorithms will be the same, when run on the same scenario. Hence, the suggested survivability criterion is a relative measure for comparison between threat evaluation algorithms. In the case where the defended assets are assigned different protection values we are not interested in counting the number of surviving defended assets, but rather the normalized total protection value of the surviving defended assets, i.e.

$$H = \frac{\sum_{j=1}^P S_j u_j}{\sum_{j=1}^P S_j}, \quad (4)$$

where  $\vec{u} \in \{0, 1\}^P$  is a binary vector defined as

$$u_j = \begin{cases} 1 & \text{if defended asset } j \text{ survived;} \\ 0 & \text{otherwise.} \end{cases}$$

A similar approach have been used earlier for comparing weapon allocation algorithms, but the measures used there have been the percentage of threats destroyed and the percentage of defended assets alive [14]. Also, in their experiments the threat evaluation has been fixed, while the weapon allocation algorithms have been changed (since they have evaluated weapon allocation algorithms and not threat evaluation algorithms).

By using our suggested survivability measure, we have removed the need for elicitation of subjective threat values from human experts. However, we still have the problem of a limited amount of scenarios. This problem can be solved if we are able to generate a large number of scenarios automatically. This would not have been possible if we compared the output of threat evaluation algorithms to expert-based threat values, but now the performance criterion is part of the simulation, and hence, no expert involvement is needed for each generated scenario. Instead, what is needed is a way to make sure that the generated scenarios are realistic. This is part of ongoing work.

#### ACKNOWLEDGMENTS

This research has been supported by a grant from the Knowledge Foundation (project number: 2003/0104) to the Information Fusion research program at the University of Skövde ([www.infofusion.se](http://www.infofusion.se)).

#### REFERENCES

- [1] Roux, J. N. and van Vuuren, J. H., "Threat evaluation and weapon assignment decision support: A review of the state of the art," *ORION* **23**, 151–186 (2007).
- [2] Joint Chiefs of Staff, "Joint publication 3-01: Countering air and missile threats," (Feb 2007).
- [3] Paradis, S., Benaskeur, A., Oxenham, M., and Cutler, P., "Threat evaluation and weapons allocation in network-centric warfare," in [*Proceedings of the 8th International Conference on Information Fusion*], (2005).
- [4] Lloyd, S. and Witsenhausen, H., "Weapon allocation is NP-complete," in [*Proceedings of the 1986 Summer Conference on Simulation*], (1986).
- [5] Hosein, P. A., *A class of dynamic nonlinear resource allocation problems*, PhD thesis, Massachusetts Institute of Technology, Dept. of Electrical Engineering and Computer Science (1990).
- [6] Nguyen, X., "Threat assessment in tactical airborne environments," in [*Proceedings of the Fifth International Conference on Information Fusion*], (2002).
- [7] Roy, J., Paradis, S., and Allouche, M., "Threat evaluation for impact assessment in situation analysis systems," in [*Proceedings of SPIE: Signal Processing, Sensor Fusion, and Target Recognition XI*], Kadar, I., ed., **4729**, 329–341 (July 2002).
- [8] Johansson, F. and Falkman, G., "A Bayesian network approach to threat evaluation with application to an air defense scenario," in [*Proceedings of the 11th International Conference on Information Fusion*], (2008).
- [9] Johansson, F. and Falkman, G., "A comparison between two approaches to threat evaluation in an air defense scenario," in [*Proceedings of the 5th International Conference on Modeling Decisions for Artificial Intelligence*], (2008).
- [10] Liang, Y., "A fuzzy knowledge based system in situation and threat assessment," *Journal of Systems Science & Information* **4**, 791–802 (Dec 2006).
- [11] Liang, Y., "An approximate reasoning model for situation and threat assessment," in [*Proceedings of the 4th International Conference on Fuzzy Systems and Knowledge Discovery*], (2007).
- [12] Benavoli, A., Ristic, B., Farina, A., Oxenham, M., and Chisci, L., "An approach to threat assessment based on evidential networks," in [*Proceedings of the 10th International Conference on Information Fusion*], (2007).
- [13] Elfström, M., "Hotutvärderare för luftvärn - automatiska algoritmer för beslutsstöd och beslutsfattande," C-uppsats, Swedish National Defence College (in Swedish) (2005).
- [14] Benaskeur, A., Bossé, E., and Blodgett, D., "Combat resource allocation planning in naval engagements," Tech. Rep. TR 2005-486, Defence R&D Canada - Valcartier (2007).