A Bayesian network approach to threat evaluation with application to an air defense scenario

Fredrik Johansson
School of Humanities and Informatics
University of Skövde
Box 408, SE-541 28 Skövde, Sweden
Email: fredrik.johansson@his.se

Göran Falkman
School of Humanities and Informatics
University of Skövde
Box 408, SE-541 28 Skövde, Sweden
Email: goran.falkman@his.se

Abstract—In this paper, a precise description of the threat evaluation process is presented. This is followed by a review describing which parameters that have been suggested for threat evaluation in an air surveillance context throughout the literature, together with an overview of different algorithms for threat evaluation. Grounded in the findings from the literature review, a threat evaluation system has been developed. The system is based on a Bayesian network approach, making it possible to handle imperfect observations. The structure of the Bayesian network is described in detail. Finally, an analysis of the system’s performance as applied to a synthetic scenario is presented.

Keywords: Bayesian networks, TEWA, threat assessment, threat evaluation, weapons allocation, weapons assignment.

I. INTRODUCTION

In a military environment it is often the case that decision makers in real-time have to evaluate the tactical situation and to protect defended assets against enemy threats by assigning available weapon systems to them [1]. In a situation with several potential threats, it is of importance to prioritize these according to the degree of threat they represent to friendly defended assets, since such a degree indicates in which order the threats should be engaged [2], [3]. The degree of threat, known as threat value, can also be used to support intelligent sensor management [4], by allocating more sensor resources to targets with high threat values. To determine which of several threats that represent the highest danger is of great importance, since errors such as prioritizing a lesser threat as a greater threat can result in engaging the wrong target, which often will have severe consequences [5]. A well-known example in which a misclassification of a non-threat as a threat resulted in tragic consequences is USS Vincennes shootdown of an Iranian commercial airliner in the late 1980s [6].

The process of calculating threat values will in this paper be referred to as threat evaluation, while the reactive assignment of weapon systems to identified threats will be referred to as weapons allocation. Threat evaluation is a high-level information fusion process that in relation to the JDL model of data fusion [7] belongs to level 3 [1], [4], [5], i.e. it is part of impact assessment. There are surprisingly few papers that have been written on the topic of threat evaluation, especially when it comes to systems for automatic or semi-automatic threat evaluation. An explanation to this is probably that the inner workings of threat evaluation systems typically are kept secret due to the high cost and extensive research required to develop them [1], and to avoid that weaknesses in developed threat evaluation systems are exploited. In this paper, we describe the threat evaluation process, give a classification of which parameters have been used for threat value calculation, and what kind of threat evaluation algorithms that have been described throughout the literature. Based on the findings from a literature review on parameters and algorithms for threat evaluation, an implementation of a threat evaluation system is described.

In contrast to threat evaluation, weapons allocation have been studied more thoroughly, especially within the field of operations research [1]. The weapons allocation process is heavily influenced by the output from the threat evaluation process, but will not be of any focus here. Some examples of work within the field of weapons allocation can instead be found in [8]–[10].

The remainder of this paper is organized as follows. In section II, a precise description of the threat evaluation process is presented. This is followed by a classification of parameters that throughout the literature are suggested for use in threat value calculation, and a summary of different algorithms and methods for threat evaluation that exist. In section III, a threat evaluation system based on the findings from the literature review is presented. The calculation of threat values in the system is performed by making inference in a Bayesian network. The structure of this Bayesian network is described, together with an analysis of the system’s behavior as applied to a synthetic scenario. Finally, in section IV the paper is concluded and thoughts regarding future work are presented.

II. THREAT EVALUATION

Consider a tactical situation where we have a set of defended assets $A = \{A_1, \ldots, A_n\}$ that we are interested in to protect (e.g. friendly forces, bridges, and power plants). There is also a set of targets $T = \{T_1, \ldots, T_m\}$, which have been detected in the surveillance area. Now, the first problem is to for each target-defended asset pair $(T_i, A_j)$, where $T_i \in T$ and $A_j \in A$, assign a threat value representing the degree of threat $T_i$ poses to $A_j$, i.e., to define a function $f : T \times A \rightarrow [0, 1]$, assuming numbers between 0 (lowest possible threat value) and 1 (highest possible threat value). Secondly, based on the
calculated threat values we will create a prioritized threat list, ranging from the most severe threat to the least. The above description is the essence of the threat evaluation process that we will study in this paper. This is consistent with the definition of threat evaluation given in [11], saying that “threat evaluation refers to the part of threat analysis concerned with the ongoing process of determining if an entity intends to inflict evil, injury, or damage to the defending forces and its interest, along with the ranking of such entities according to the level of threat they pose.”

So, how can we calculate threat values for target-defended asset pairs? To answer this question we must first define what we mean by threat. A threat is in [5] defined as an expression of intention to inflict evil, injury, or damage. These threats are according to Steinberg [12] modeled in terms of relationships between threatening entities and threatened entities. The threatening entities will be referred to as targets, while the threatened entities are referred to as defended assets. A threat is often assessed as a combination of its capability and intent (cf. [5], [13], and [14] (p.284)). A target’s capability is its ability to inflict injury or damage to defended assets, while intent refers to its will or determination to inflict such damage [11]. In [15], a third threat component is mentioned: opportunity. This is spatio-temporal states of affairs making it possible to carry out one’s intent given sufficient capabilities [15].

A. Parameters for threat evaluation

In order to evaluate the threat posed by a target $T_i$ on a defended asset $A_j$, there is a need to identify the parameters that control the threat value given a target-defended asset pair [16]. A large number of different parameters for threat value calculation have been suggested in the literature. However, many of these are closely related to each other. Based on an exhaustive literature survey over publications dealing with threat evaluation in the information fusion domain and related areas, the parameters have been classified as follows.

1) Proximity parameters: An important class of parameters for assigning threat values to target-defended asset pairs is proximity parameters, i.e., parameters measuring the target’s proximity to the defended asset. A key parameter that is used in many threat value evaluation techniques [2], [5] is the distance from the defended asset to the closest point of approach (CPA). The CPA is the point where the target eventually will be the closest to the defended asset, given current track estimates. Assuming stationary (non-moving) defended assets, this is the orthogonal projection of the position of the defended asset on the extension of the target’s velocity vector (see Figure 1). The distance between the position of the defended asset (known as threat reference point or point of interest) and the CPA is clearly a measure of the threat level: the larger the distance, the less the threat. This distance will in the following be referred to as range from CPA.

Parameters that are closely related to the distance from the defended asset to the CPA are time to CPA (TCPA), CPA in units of time (CPA IUOT), and time before hit (TBH).

If two targets of the same kind have the same CPA but different TCPA, the one with lowest TCPA will probably, at the moment, constitute a larger threat to the defended asset. TCPA is calculated as the distance between the CPA and the target’s current position, divided by the target’s current speed, i.e.,

$$TCPA = \frac{range\ from\ CPA}{\text{speed}}.$$

CPA IUOT is the time it would take the target to hit the defended asset after a 90° turn at its CPA, and is calculated as distance between the CPA and the position of the defended asset (referred to as range at CPA), divided by the target’s current speed:

$$CPA\ IUOT = \frac{range\ at\ CPA}{\text{speed}}.$$

Finally, TBH is an estimate of the time it would take the target to hit the defended asset. This is directly applicable for targets such as missiles, but can also be used as a proximity measure for weapon platforms. The TBH is calculated as:

$$TBH = TCPA + CPA\ IUOT.$$

Other proximity parameters that are suggested in the literature are the distance between the target and the defended asset and its rate of change. According to [16], the threat posed by a very distant target should be close to minimum and then increase gradually when the target approaches the defended asset. It should reach its maximum when the defended asset is within range of the target’s weapon systems. In the above calculations, we are assuming constant target velocities. This is an assumption that often is made when performing threat evaluation. For many platforms and conventional weapons this is a reasonable assumption, since they seldom make rapid maneuvers between two track updates [4]. However, for highly maneuvering targets such as missiles, the assumption is often unrealistic [2]. In such cases, the quick maneuvers of the target may cause large changes in the values of the above parameters.
B. Algorithms for threat evaluation

Also influences the likelihood of a hostile intent [19]. In order to handle the problem of highly maneuvering targets, there is sometimes a need for the use of smoothing techniques for the trajectory of targets in order to ensure only gradual changes in their threat values [5]. For more on this issue, see [2] and [3].

2) Capability parameters: The next class of parameters for threat evaluation is capability parameters. This refers to the target’s capability to threaten the defended asset. A central parameter here is target type, which can be identified from other parameters such as answer to IFF-interrogation, electronic support measures, speed, etc. Once the target type is known, parameters such as weapon type and weapon envelope can be inferred, given that the target carries weapons. These parameters are concerned with the lethality of the target and clearly are related to the proximity parameters, since a target is more threatening if it is able to overlay its weapon envelope over a defended asset than if it is outside the range of its weapon systems [16]. Fuel capacity is another capability parameter that is related to proximity. Given an identified target type it may be possible to have prior knowledge regarding the fuel capacity. Such information can be used to reason about the target’s maximum radius of operation. According to [4], the most important parameters for threat evaluation are the lethality of the target, the imminence of the target to the defended asset, and the geometry of the target’s weapon envelope relative to the defended asset.

3) Intent parameters: The class of intent parameters is a broad category, containing parameters that can reveal something about the target’s intent. An example of this is the target’s kinematics. According to [4], the target’s velocity (i.e. speed and heading) in combination with its altitude can be a good indicator of the target’s intent to attack a defended asset. Another kinematics parameter that can be used is the number of recent maneuvers [6].

Context parameters can also impact the threat value. A target classified as a commercial flight that all of a sudden stops to follow an air lane probably may be worth a closer look. Hence, the parameter following air lane can be of importance for threat ranking of air targets. This parameter is mentioned in [4], [6], and [17]. Another context parameter described in [6] is the feet wet parameter. This parameter is true for an air target flying over water. A final context parameter is coordinated activity [6], [18], indicating whether the target is nearby, or communicating with, other targets.

Other parameters that may indicate hostile intent is the use of radar jamming and deception, and whether the target’s fire-control radar is on or not [4], [19]. Finally, the political climate also influences the likelihood of a hostile intent [19].

B. Algorithms for threat evaluation

To our knowledge, only a few algorithms for threat value calculation are available in literature. In a series of experiments with U.S Navy officers summarized in [6], it is suggested that human operators perform threat evaluation on air targets by starting out with activation of a template corresponding to the target’s particular type. The activated template sets a baseline threat rating. Parameters relevant to the active template are then assessed and compared to expected values for the activated template. Depending on the degree of match between the actual value of a parameter and its expected value, the current threat rating is adjusted up or down (as an example given in [6], an aircraft in a littoral environment with a speed of 250 knots adds 0.2 to the current threat rating, while a speed of 500 knots adds 1.8). In [18], it is mentioned that the geopolitical situation influences the tolerance for deviations from expected values. In case of no unexpected data, the process is stopped after evaluation of the six most important parameters (for targets classified as military this corresponds to platform type, weapon type, weapon envelope, coordinated activity, distance, and course) [18]. Otherwise the evaluation process will continue with more parameters until there are no more parameters to process, or the fit of the expected values and the parameter values is good enough. From this naturalistic model a rule-based algorithm for threat evaluation was developed [6]. The same algorithm outline is described for threat evaluation of surface targets in [17]. A high-level description (adapted from [17]) of the rule-based algorithm follows:

1) Exception Score = 0
2) Threat = ID Threat Rating + Platform Threat Rating
3) FOR EACH critical parameter DO
   a) Get Value and Weight for the current parameter
   b) Threat = Threat ± Threat Change Rating
   c) IF Value is an exception
      THEN Exception Score = Exception Score - Weight
4) WHILE Exception Score < 0 AND more parameters exist DO
   a) Get Value and Weight for the current parameter
   b) Threat = Threat ± Threat Change Rating
   c) IF Value is an exception
      THEN Exception Score = Exception Score - Weight
      ELSE Exception Score = Exception Score + Weight

In [20], the threat evaluation module of a commercial air surveillance and defense system is described. For each defended asset a defended area, represented as a circle, has to be defined. This is accomplished by an operator specifying the position of the defended asset, together with its priority and the radius of the defended area. The parameters that are used for threat evaluation in the system are time, relative bearing, altitude, identity, number of engagements, speed, size, and aircraft type. The parameter time is the minimum time it will take the target to reach the defended area border (assuming constant speed), while identity is whether the target is identified as hostile or unknown. Number of engagements refers to the number of friendly weapon systems currently engaged to the target [20]. For each parameter the operator specifies rules, assigning a number of threat points depending on the parameter’s actual value (e.g. IF (Time < 1) THEN
For each target-defended asset pair, the points from the individual parameters are summed together and multiplied with a weight that is dependent on the priority of the defended asset. Finally, this value is divided by the maximum number of points, resulting in a normalized threat value between 0 and 1 to the target-defended asset pair.

In [21], another kind of rule-based algorithm is suggested, in which fuzzy inference rules are used to calculate the level of threat air targets pose to a navy combat ship, using altitude, speed, CPA, and range as input parameters. For each input parameter, three membership functions are defined (e.g. low, medium, and high for the altitude parameter). Such a membership function maps each point in the input space to a membership value between 0 and 1. Finally, fuzzy inference rules have been defined for how the input should affect the output parameter threat rating. The fuzzy inference rules that have been used in the implementation in [21] are the following:

1) IF (Altitude is low) AND (Speed is fast) AND (Range is close) AND (CPA is close) THEN (ThreatRating is high) (Weight: 1).
2) IF (Altitude is high) AND (Speed is slow) AND (Range is far) AND (CPA is far) THEN (ThreatRating is low) (Weight: 1).
3) IF (Altitude is medium) AND (Speed is medium) AND (Range is medium) AND (CPA is medium) THEN (ThreatRating is medium) (Weight: 1).
4) IF (Altitude is low) AND (Speed is fast) AND (Range is far) AND (CPA is close) THEN (ThreatRating is medium) (Weight: 0.5).
5) IF (Range is close) THEN (ThreatRating is medium) (Weight: 0.05).
6) IF (Range is far) THEN (ThreatRating is low) (Weight: 0.05).
7) IF (Range is medium) THEN (ThreatRating is low) (Weight: 0.05).

The last family of algorithms for threat evaluation that we have been able to identify in the literature is graphical models. In [16], a Bayesian network based algorithm using target state estimates for evaluation of the threat posed by a target on a defended asset is presented. The target’s capability to threaten a defended asset is measured by comparing the maximum range of the target’s weapon systems with the range between the target and the defended asset. In the same manner, the target’s intent to threaten the defended asset is measured by looking at the rate of change of the range between the target and the defended asset, together with the angle between the target’s velocity vector and the vector pointing from the target to the defended asset. The threat value is then calculated as the product of the capability and intent components. Another example of the use of graphical models for threat evaluation is presented in [19], where an evidential network (i.e. a valuation-based network using belief functions) is used to represent and reason about threat in the context of air surveillance. The evidence variables that are used in the network are: evasive maneuvers, fire control radar, countermeasures, political cli
date, IFF squawking, flight plan agreement, platform type, and imminence. Most of these variables are binary, while some can take on more states. Together with a few mediating variables, these evidence variables influences the intent and capability variables, which in turn have impact on the value of the threat variable.

III. IMPLEMENTATION

A long-term goal of this research is to develop a toolbox where different kinds of algorithms and models for threat evaluation can be tested and analyzed. As a first step, we have developed a threat evaluation model based on a Bayesian network. A reason for starting out with a Bayesian network approach is its abilities to handle uncertainty, which most often is a central aspect in an air surveillance environment.

A Bayesian network characterizes a problem domain consisting of a set of random variables \( U = \{X_1, ..., X_n\} \). These variables are in the Bayesian network represented as a set of corresponding nodes (vertices) \( V \) in an acyclic directed graph \( \mathcal{G} = (V, E) \), where the set of edges \( E \subseteq V \times V \) specifies (conditional) independence and dependence relations that hold between variables within the domain. Given the graph structure \( \mathcal{G} \), a joint probability distribution \( P \) over \( U \) can be calculated from a set of local probability distributions associated with each node\(^1\) \( X_i \), using the chain rule of Bayesian networks

\[
P(x_1, ..., x_n) = \prod_{i=1}^{n} P(x_i | pa_i),
\]

where the set of local probability distributions consists of the distributions in the product of Equation 4 (with \( pa \), we refer to an assignment of values to the parent set \( PA_i \) of node \( X_i \)). The joint probability distribution can be seen as a function assigning a number in the range \([0, 1]\) to each possible combination of states of variables describing the domain. A strength of Bayesian networks is their ability to represent joint probability distributions in a compact manner, due to their encoding of conditional independences between different variables in the domain.

A subset of the parameters for threat evaluation that we have discussed in Section II-A have been included as nodes in the developed Bayesian network. The parameters that have been used can be seen in Figure 2.

The dotted directed edges in Figure 2 are not part of the Bayesian network, but rather are calculated outside it, and hence, the structure of the actual Bayesian network looks like in Figure 3. The random variable (node) of main interest here is the query variable Threat, i.e., we want to calculate the posterior probability of Threat being in state true given some evidence on our information variables, which are the grey shaded nodes in Figure 3. This posterior probability \( P(\text{Threat} = \text{true} | z) \) is our assessed threat value of the pair \((T_i, A_j)\), for which the set of observations, \( z \), holds.

\(^1\)Since the nodes in \( \mathcal{G} \) are in one-to-one correspondence with the variables in \( U \), we use \( X_i \) to denote both variables and their corresponding nodes.
The threat variable is directly dependent upon the mediating variables Intent and Capability, which is consistent with the view that threat is a combination of capability and intent [5], [13]. Capability is in its turn dependent upon Target type and whether the defended asset is within the target’s weapon envelope or not (Within weapon envelope?). The target’s intent is according to the structure in Figure 3 the cause of the Euclidean distance between the target and the defended asset (Distance), as well as of the Time Before Hit.

Once the structure of the Bayesian network has been decided on, we also have to specify local probability distributions. These are given in the form of conditional probability tables (CPTs). Figure 4 illustrates how such a CPT may look like. To fill a CPT with appropriate numbers is often the hardest task when designing a Bayesian network manually [22], [23]. The task often becomes harder as a node’s number of parents and possible states grows. The numbers used for the CPTs in this research have not been assessed by domain experts and can most probably be improved on. However, the main focus here is on the approach rather than on specific numbers in the CPTs. Moreover, the threat value ordering is of higher importance than the threat values themselves, since we are searching for a way to prioritize the engagement of friendly weapon systems to the detected targets.

In the case of no evidence at all, our Bayesian network outputs the prior probability \( P(\text{Threat} = \text{true}) = 0.341 \), which thereby also becomes the threat value. For a high threat case with a B-2 bomber within range of its weapon systems, at very close distance and with very short time before hit, the threat value becomes 0.843. Similarly, for a low threat value with a Boeing 747 at very far distance with very long time before hit, the threat value becomes 0.0446. It should be noted that it is possible to adjust the prior probability of the node Intent in order to compensate for different political climates.

A. Test scenario

We have in Microsoft Visual C++ 2005 implemented a threat evaluation system that continuously reads scenario observations generated from the STAGE Scenario tool, calculates threat values for target-defended asset pairs by setting the observed values as evidence in the constructed Bayesian network, and plots the targets and the defended assets. To demonstrate the threat evaluation application, we have constructed a dynamic test scenario. The scenario consists of a defended asset and four air targets (two Boeing 747, one F-16, and one B-2 bomber). Figure 5 shows the initial heading of the targets (black arrows), together with their future trajectories (colored arrows). It also shows the location of the defended asset (the blue triangle). The speeds of the targets are close to constant, except for the F-16 which accelerates at the point where it starts to change its heading.

The diagram in Figure 6 shows the threat value as a function of time. One unit of time in the diagram corresponds to 50 observations, which is about ten seconds. An analysis gives that the first small change in threat values at Time = 2 for 747_2 and B2 occurs for different reasons. The decrease in threat value for 747_2 depends on a change in heading, which updates the position of its CPA. This in turn cause a state change for the node Intent through the mediating variable Intent. The increase in threat value for B2 at the same point in time depends on that the node Distance reaches a new state. Next change is at Time = 7, where the increased threat value for both B2 and 747_1 depends on changes in Distance. At Time = 9 a new change in heading for 747_2 results in an increase of the threat value. The target F16 have a changed threat value due to a speed change.
Figure 3. The structure of the Bayesian network used in the threat evaluation system.

Figure 5. Trajectories of the targets used in the test scenario (screen shot taken from STAGE Scenario). Black arrows show initial heading of targets.

acceleration at Time = 12, followed by a new increase at Time = 13 due to Distance reaching a new state. At Time = 15 target 747_1 reaches a new state for Time Before Hit. Finally, at Time = 16 the state for both Time Before Hit and Distance causes a higher threat value for F16.

IV. CONCLUSION AND DISCUSSION

In this paper, we have given a precise description of the threat evaluation process. A literature review has been carried out regarding which parameters that have been suggested for threat value calculation throughout the literature, together with an overview of different algorithms that exist for threat evaluation. Three main classes of parameters have been identified: capability parameters, intent parameters, and proximity parameters. A target’s proximity to a defended asset clearly is related to both capability and intent parameters. As an example, the range of a target’s weapon systems and the distance between the target and the defended asset are interrelated, since a target is more threatening to a defended asset if the defended asset is within the range of its weapon systems, than if it is outside it. Relations between capability parameters and proximity parameters can in fact be seen as an example of opportunities, which in [15] is described as spatio-temporal states of affairs that make it possible to carry out an intent, given sufficient capabilities.

Based on the findings from the literature review, we have implemented a system for threat evaluation in an air defense environment. The underlying mechanism for threat evaluation in this system is a Bayesian network. A subset of the identified
parameters for threat evaluation have been used as nodes in the implemented Bayesian network. The number of nodes, and thereby the complexity of the Bayesian network, have been limited in order to make it easier to analyze and validate the proposed model.

The implemented threat evaluation system has been applied to a synthetic air defense scenario. An analysis of the system’s threat value calculations shows that the proposed Bayesian network model works well for dynamically moving targets. An issue of interest is the need for discretization of continuous nodes in most inference algorithms for Bayesian networks. The discretization gets stable threat values as an effect, which changes only when a node’s value has changed much enough to pass into a new state. Stable threat values can be seen as a good thing, but it can also be argued that small continuous changes in the threat values are to be preferred, since such changes better indicates whether the threat are about to decrease or increase. Increasing the numbers of states a node can take on will lead to more frequent changes in threat value, but will also make it harder to set the values in the CPTs. Another interesting aspect with the use of Bayesian networks is the possibility to handle soft evidence. As an example, if we after object identification are certain that a target is either a F-16 or a MiG-21 but are uncertain of which of these are the correct classification, we can in the Bayesian network assign likelihoods reflecting this knowledge.

As future work, more nodes should be added to the Bayesian network. This in order to handle important parameters that currently are not part of the model. Examples of such parameters are the use of countermeasures and fire control radar, and whether the air target is classified as friend, foe, or neutral. Another interesting aspect is to investigate if the system’s calculated threat values on realistic scenarios agrees with human experts on air defense. Assessing the performance of a threat evaluation system is a hard task, since it exist no such thing as an objective threat value. Finally, the Bayesian network is only a first component in a toolbox of different algorithms for threat evaluation. Other threat evaluation algorithms are to be implemented and compared against the performance of the Bayesian network. It is also of interest to investigate whether an ensemble of threat evaluation techniques perform better than a single threat evaluation technique.

ACKNOWLEDGMENT

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). We would like to express our thankfulness to the other members of the ground situation awareness scenario for fruitful discussions and valuable feedback.

The core of the BN implementation in this project is based on Netica’s C++-API. Netica is a trademark of Norsys Software Corp. and can be downloaded from www.norsys.com. For the simulations we have used the STAGE Scenario tool from Presagis Inc. (see www.presagis.com).

REFERENCES