A Threat Evaluation Model for Small-Scale Naval Platforms with Limited Capability

Mustafa Çöçelli
Defense Systems Technologies
Aselsan A.Ş.
Ankara, TURKEY
mcocel@aselsan.com.tr

Ethem Arkın
Defense Systems Technologies
Aselsan A.Ş.
Ankara, TURKEY
earkin@aselsan.com.tr

Abstract— **Naval command and control (C2) systems guide the operators to fulfill combat actions under time-constrained circumstances. Selecting proper targets among hundreds is an important decision making process with no compensation. Hereby, threat evaluation is a critical fusion operation to accelerate this process and increase situational awareness level in military domain services. However, combat management system could suffer from small-scale platforms supplying insufficient inputs that allow only limited foresight of common tactical picture. In this paper we present an experience on deriving threat evaluation value by pruning general approaches to meet operational needs of small-scale naval platforms along decision making process. We represent a method to obtain tactical information from only kinematics of target in two dimensional space. In the meanwhile, there is no knowledge about characteristics and identification of target which are strategically very important. Threat evaluation model is composed of the extraction of threat assessment cues, threat selection step supported by Bayesian Inference and the calculation of threat assessment rating. We have analyzed performance of proposed threat evaluation model simulating a set of synthetic scenarios and observed real-life results on functioning naval platform.**

Keywords— Threat Evaluation, Decision-Making, Situational Awareness, Information Fusion, Command and Control (C2)

I. Introduction

In the defense domain, significant portion of operational systems simply give assistance to operators through the pictorial representation of the current tactical situation. Operators benefit from the data on the identity and kinematics of assets while making judgement about current martial situation. This tactical aspect carry a certain value of precious information for operators. Nevertheless, there is no prominent aid to understand the meaning and the relationship of entities [1]. There is a necessity of recognition, identification and prioritization for surrounding entities to display clear and obvious tactical picture because of the possibility of combat risk in the field [2]. Categorizing an asset as harm intended object is a difficult and stressful task for tactical operators due to the presence of large amount of instant variable data, the uncertainty of environment, error-prone atmosphere and biases. Therefore, assistance of machine power is inevitable for operators along OODA (Observe-Orient-Decide-Act) loop [3] of C2 processes. There are lots of efforts spent on modeling and simulation studies for the decision cycle of operators while developing military systems [4, 5]. These efforts indicates the crucial role of decision support systems in modern military systems.

Threat evaluation is the ongoing process of systematically interpretation of the information collected through situational awareness phase. The motivation behind this process is to determine if an entity intends to damage the defending assets. As a result of this process, the most appropriate policy of action to protect defended forces is detected [6]. Hereby, threat evaluation methods become important to reduce the amount of time that requires cognitive process of operator understanding and accelerate response time of operator through decision-making process. Threat evaluation phase analyzes, interprets and compiles output of sensor data processing. Data operations should have been accomplished in the situational awareness phase [7]. Resulting information varies depending on the sensor capability.

Threat level of a potential target is measured by benefiting from different techniques, such as, rule based techniques, fuzzy logic based techniques, neural networks and graphical models [8]. Inputs of all of these techniques are called the threat assessment cues. These cues are determined as a result of progressive in-depth researches through years. Liebhaber and Feher give list of mostly used 17 cues, namely, airlane, altitude, coordinated activity, course heading, closest point of approach (CPA), ESM/Radar Electronic Support, feet wet/dry IFF mode, maneuvers, origin/location, own support, range/distance, speed, visibility, weapon envelope, wings clean/dirty in their air assessment study [9].

Threat assessment cues are categorized as capability, proximity and intent parameters in accordance with the aspect of a different research [8]. Capability parameter of target is mostly related to characteristic of this asset. Proximity parameters, mainly, represents the proximity of defended asset to potential target. Capability parameters are related to the measure of the target's lethality for own asset. Intent parameters are cues that measure behaviors of the potential target to perceive the actual purpose of this object on defended entity [8].

The categorization of the threat evaluation measurements fulfills the purpose of separation among cues with respect to their characteristic and kinetic information. While proximity and intent parameters are arising from the kinematic data of target, capability parameters of target are generally related to identification and classification of potential target. Small-scale naval vessels could be deprive of IFF or ESM ability that defines target's decisive characteristics for the level of danger. In this paper, we present a threat evaluation model that firstly extracting threat assessment cues from kinematics of track, then making threat selection operation through tracks by using cues and finally allowing defense system to reach threat assessment ratings of potential targets after fusion operation among cues.

The remainder of this paper is organized as follows. In section II, the motivation behind the implemented threat evaluation model is introduced and the formal definition of the threat evaluation problem is presented. In section III, entire steps of the implementation for the presented threat evaluation model is presented. In section IV, the model is evaluated by three synthetic scenarios and collected input and output data from these scenarios are interpreted. In section V, related works for the threat evaluation problem are given. Finally, in section VI, the summary of this paper is presented and last words about this study are stated.

II. MOTIVATION

Threat evaluation is not a completely defined and solved process due to the complexity of estimating C2 operator actions in response to a developing situation during military operation [10]. It is still open issue due to the necessity of fusing large amount of uncertain data from various sensors [11]. The issue becomes more compelling when the platform has limited capability for the collection of surrounding information. In this regard, small-scale platforms suffer from the state of insufficient information arising from inadequate equipment. The absence of the crucial equipment and competent sensors causes lower estimation performance for the threat level of targets. In this study, we experience such scenario and evaluate a method to make the best of C2 system of small-scale platforms by benefiting from existing data.

Any content word connected with threat evaluation process is called factor, characteristic or specifically cue [10, 12]. The main source of the threat rating value is threat assessment cues. Origin, IFF Mode, Intelligence Report, Altitude, Proximity to an Airlane and ESM (Radar Signature) are the most crucial parameters utilized by air defense system in US Navy while performing threat evaluation [9]. These parameters, particularly, point out the characteristics of target and enter the category of capability parameters. Because these cues determine the capability of target's lethality in battlefield. However, small-scale vessels could be not equipped with high technological systems performing electronic warfare which separates friendly or enemy communication. Moreover, small-scale naval platform could suffer from absence of identification systems that detect aircraft or friendly forces. These disadvantages bring the platform to the state without any signature of familiarization about external forces. Consequently, the platform is deprived of the awareness of target's capability which generates needed data for the capability branch of the threat evaluation phase. If threat evaluation process does not take into consideration the operator initiative as a feedback, kinematics information of external forces is only instrument to apply while measuring the threat level for foreign assets.

Meanwhile, threat evaluation process can defined formally as follows. $\mathbf{T} = \{T_1, \dots, T_n\}$ symbolizes set of targets and $\mathbf{A} = \{A_1, \dots, A_m\}$ symbolizes set of friendly assets requiring protection. V_{ij} describes the threat evaluation value of target-defended asset pair (T_i, A_j), where $T_i \in$ T, $A_j \in$ A. V_{ij} takes normalized values between 0 and 1 for simplicity. Predictably, while 0 defines safe force, 1 stands for dangerous one. A function is designed based on the information arises from threat assessment cues as follows [13]:

$$f: \mathbf{T} \text{ x } \mathbf{A} \rightarrow [0,1] \tag{1}$$

If there is no possibility to separate friends from hostile forces in the field, then only asset to defend against dangerous force will be our own ship. At that time, group of assets (A) in the description of threat evaluation process are downgraded to one asset (A_1). Johansson's formula is reduced to following version with respect to this condition:

$$f: \mathbf{T} \text{ x } A_1 = \mathbf{V} \rightarrow [0,1] \tag{2}$$

In (2), $\mathbf{V} = \{V_1, \dots, V_n\}$ symbolizes the corresponding threat value of targets with respect to A_1 which signifies the own ship platform. The calculation of threat evaluation value is changing according to various types of techniques. Details of our approach will be introduced in method section of this paper.

III. METHOD

Threat evaluation process without any indication of objects' identity is a complicated task since it should separate dangerous and safe forces from each other by only investigating kinematic behaviors of those objects. The interpretation of the information derived from position, speed, and course of assets establishes the basis of the threat evaluation model.

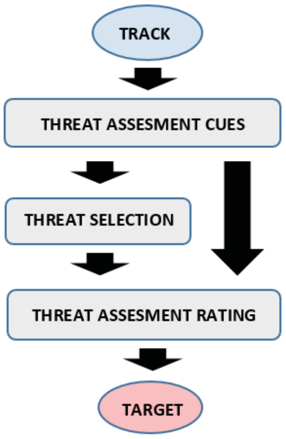


Fig. 1. Threat Evaluation Model

We have defined a three phase method for the management of the threat evaluation process. In the first phase, we have extracted scores of threat assessment cues from the kinematics of targets and own ship. In the second phase, threat selection algorithm is applied by benefiting from these scores to filter potentially dangerous assets. In the last phase, threat assessment rating is calculated by using scores of threat assessment cues again as an input to reveal danger level of targets.

Fig.1 depicts fundamental phases of the threat evaluation model. In the beginning of the process, kinematics of tracks are used as input for the extraction of the threat assessment cues. In this phase, the model also utilizes from kinematics of defended asset to calculate cue scores. The scores generated from this phase is firstly directed to threat selection algorithm to classify tracks as dangerous or assumed friend. The calculation of the threat assessment rating phase accepts this classification and the cue scores as input. Targets classified as dangerous are prioritized for the calculation of threat rating. The classification of target is also used to reveal danger level of target for the use of the operator. As a result, the track turns into target with a classification and danger level indicated by threat rating within the model.

A. Threat Assessment Cues

In order to derive threat level of a target on a defended asset, it is necessary to associate correct parameters that produce the threat value given a target-defended asset pair closely with each other [14]. Various parameters have been proposed to calculate threat assessment rating for years. However, there is no possibility to make use of whole suggested parameters in the threat evaluation algorithm of combat management systems. Because this algorithm shall be limited to sensors' capability of the ship platform where the software is installed. Consequently, the threat evaluation algorithm ends up with being deprived of some useful parameters due to the limited capability of the vessel. In such cases, it is inevitable to use remaining useful parameters with their full strength. In our case, available information about the target and own ship are course, speed and location (latitude-longitude) without any altitude data. Kinematic information of suspicious and friendly assets turns to threat assessment cues contributing the threat selection algorithm and the calculation of threat assessment rating. While determining the resulting values of threat evaluation model, there is a need to find mathematical correspondence of threat assessment cues. Following sections describes the approaches to obtain scores using threat assessment cues from sensor current data.

1) Speed: Speed is one of the most important capability parameter to determine the classification of asset and foresee the potential danger behind this asset [9, 10, 12, 15]. While speed of a mid-range surface-to-surface missile could have high speed which indicates great danger, an ordinary boat could reach 30 knots which means lesser danger. It is inevitable to take into account speed factor due to its indicator dynamic while measuring threat level. Since speed information of target and own ship is present and ready to use in our scenario, the threat evaluation model takes advantage of this valuable data. Speed value makes contribution to threat evaluation phase linearly as indicated follows.

$$s_i = \frac{s_c}{s_{max}} \tag{3}$$

Particularly, current speed of target is divided by theoretical maximum value of a moving object to find the contribution of target's speed to resulting threat rating.

2) Distance: Since the position of target and own ship on earth sphere is known in our case, the distance between two objects could be calculated easily by use of the haversine formula [16]. Despite the shortage of the altitude information for the target, the distance between potential target and own ship on sea level is still another essential factor that affects the threat rating value directly. Closer target is interpreted as more dangerous than farther target [9, 10, 12, 15]. Therefore, weighted contribution of this cue to threat evaluation model is changing linearly with respect to the measured distance between two assets. Score is determined by the division of the current distance to the maximum distance. This maximum value could be described as the target detection range of the friend asset as follows:

$$d_i = \frac{d_c}{d_{max}} \tag{4}$$

3) Course-Position Relation: The orientation of target asset's course with respect to defended asset position is another cue that contributes the threat rating [9, 10, 12]. If course of a target is pointed directly to defended asset, this indicator is interpreted as dangerous for the friend asset and threat rating is affected more by means of its value. If target's orientation is not related with the current position of friend asset, then this particular condition is not read as critical situation for defended asset and threat rating score is not influenced very much. The measurement of this cue is performed by firstly calculating the angle (α) that is formed between velocity vector of target asset and the imaginary line between two objects. Then, the magnitude of this angle is normalized by dividing it to π which is the maximum value in this sense.

$$h_i = \frac{\alpha}{\pi} \tag{5}$$

As a result, calculation gives the score generated from the relation of target's course and defended asset' position. Fig. 2 explains the angle used to calculate course-position score. In order to measure α angle, firstly, virtual line is drawn from target to own ship. The angle between this line and target's course forms α angle as shown below.

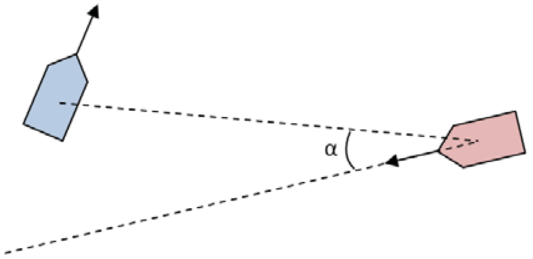


Fig. 2. Course-Position Angle

4) Maneuver: Calculating the number of maneuver is an option while determining the contribution of maneuver behavior of target to threat evaluation model [9, 10, 12]. However, it is difficult to determine which behavior could be counted as maneuver. There should be a significant threshold value between current course of target and previous course value of the target. Moreover, periodicity of feeding data to system is changing this threshold value. Instead of this method, alteration of target's course value plays key role while calculating the maneuver score of target.

$$m_i = \frac{c_i - c_{i-1}}{c_{max}}\text{, where } c_{max} = \frac{\pi}{2} \qquad (6)$$

Maneuver angle is simply the difference between target's current course value and target's course value belonging to previous iteration. Maneuver score is produced by dividing this angle to maximum maneuver angle which is semicircle.

5) Time Before Hit: The closes point of approach (CPA) between two assets is another important proximity parameter to measure threat level of attacking asset. By using this CPA position, the speed and course direction of assets, it is possible to bring out other cues evaluate the threat level of hostile asset. Johnson and *Falkman* come up with time before hit (TBH) cue that benefit from those parameters [8]. In their scenario, there are one mobile object and one stationary object. In this study, their approach of calculation of TBH is adapted to two mobile objects.

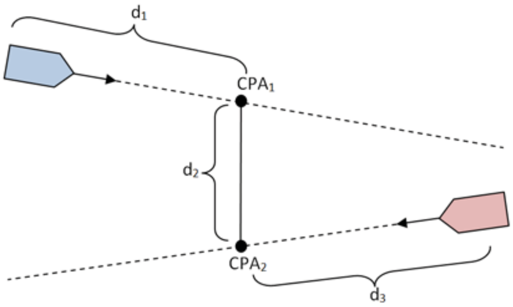


Fig. 3. The distance between two objects, which is passing through CPA points

Fig. 3 illustrates the three marked paths connecting two assets to each other. Details of these links are given as follows:

- d_1: The distance between defended asset and its CPA to the other object.
- d_2: The distance between two CPA points.
- d_3: The distance between unidentified object and its CPA to defended asset.

TBH is simply calculated by benefiting from the distances shown in Fig. 3 and the speed of the unidentified object. Moreover, contribution of TBH to threat evaluation algorithm is calculated as follows:

$$t_i = \frac{TBH_i}{TBH_{max}}\text{, where } TBH = \frac{d_1 + d_2 + d_3}{s_o} \qquad (7)$$

B. Bayesian Inference for Threat Selection Process

Threat evaluation problems absolutely host uncertainty in its nature. Even the algorithm concludes with the highest rank of threat level, there is still a chance of mistaken outcome. It is a beneficial practice from operator's point of view to observe the threat level of target by covering existing outcome with alternative layer to reduce uncertainty of existing problem.

Bayesian Inference is a beneficial method to simply answer the question whether a target is threat or not which is distinct from expressing threat rating of assets [17]. Threat assessment rating gives the operator the level of danger and threat ranking information among suspected assets. In order to simplify the tactical picture in front of the user, engage the operator's attention to particular candidates and facilitate to perform prioritization process, there is a practical option to highlight risky targets that have threat rating larger than reasonable certain threshold. In contradistinction to this approach, extended method based on Bayesian Inference seems to be more proper to determine that if target is a threat since Bayes' formula is more convenient to test truth of a hypothesis. We named this approach as threat selection process among all targets. After elimination of low-rated targets with the help of proposed method, user could concentrate more on threat ranking of marked targets in shortened list.

Bayesian Inference is an effective method indicating the procedure learning uncertain status of the world from known data [17]. Simply, Bayes' rule allows us find out the posterior probability (the posterior) of a hypothesis with given prior probability (the prior) and compatibility of the observed evidence with the hypothesis (the likelihood) [18]. Bayes' formula points out the way to alter probability statements using data [11]. Formally, Bayes' theorem is formulized as follows [17]:

$$P(H \mid E) = \frac{P(E \mid H).P(H)}{P(E)} \qquad (8)$$

Explanation of each term in Bayes' theorem and the corresponding instances of these expressions inside the threat selection problem can be described as follows:

- H denotes the hypothesis that we are trying to confirm or deny in Bayes' rule. Basically, our problem's hypothesis is whether given target is threat or not threat.
- E denotes the evidence which is the data to compute the posterior probability from prior probability for Bayes' formula. In our problem, scores of each threat assessment cues are equivalent form of evidences, namely data, of our hypothesis.
- P(H) denotes the prior probability of the hypothesis before the evidence is observed. Simultaneously, in our case, threat selection score that is result of previous iteration of threat selection phase is interpreted as the prior probability of hypothesis.
- P(H | E) denotes the posterior probability of a hypothesis (H) after observing the evidence (E). Meanwhile, it corresponds the actual score of the target at current time. This score is generated after applying

the effect of threat assessment cues over the result of previous iteration. This score is considered as fundamental indication for marking a target as a threat at that time.

- The remaining term in the formula, $\frac{\mathrm{P(E \mid H)}}{\mathrm{P(E\ )}}$, is the impact of evidence on the prior probability. Similarly, the combination of threat assessment cues' scores is determinant factor for the threat selection process.

Bayes' formula takes the following form after interpretation of terms according to threat selection process:

$$P(T_i \mid \mathbf{C}) = \frac{P(\mathbf{C} \mid T_{i-1}).P(T_{i-1})}{P(\mathbf{C})} \tag{9}$$

Similarly, explanation of each term in (9) as follows:

- T symbolizes the threat selection hypothesis that if a target is threat.
- $\mathbf{C}$ nearly stands for cues which are evidences of hypothesis *T.*
- $P(T_{i-1})$ is the prior probability of the hypothesis before evidences are observed, namely, the value generated at previous iteration of threat selection algorithm.
- $P(T_i \mid \mathbf{C})$ denotes the posterior probability of the threat selection hypothesis (*T*) after observing cues ($\mathbf{C}$).
- The remaining term in (9) is $\frac{P(\mathbf{C} \mid T_{i-1})}{P(\mathbf{C})}$ and it is the impact of the fusion of cues on previous result of the threat selection algorithm.

The group of threat assessment cues used in threat selection algorithm is same as the ones used in the calculation of threat assessment rating except one difference. The distance passing through CPAs of two assets in (7) is used instead of TBH. Since speed and TBH cues are dependent to each other, they couldn't take part at the same group. Therefore, this necessary adaptation is applied while determining threat selection score. Because, the assumption of conditional independence [18, 19] does not allow the fusion of evidences dependent to each other.

Threat assessment cue scores reference multiple evidences in Bayes' rule. These evidences are combined to take a place in Bayes' formula together. Therefore, there is a need to redefine (9) according to combination of these evidences. Equation (9) is turned to following form after taking account multiple evidences:

$$P(T_i \mid \ \wedge_{\mathrm{j=1}}^{\mathrm{n}} C_j) = \frac{P(T_{i-1}) \prod_{\mathrm{j=1}}^{\mathrm{n}} P(C_j \mid T_{i-1})}{P(T_{i-1}) \prod_{\mathrm{j=1}}^{\mathrm{n}} P(C_j \mid T_{i-1}) + P(N_{i-1}) \prod_{\mathrm{j=1}}^{\mathrm{n}} P(C_j \mid N_{i-1})}$$

where $P(N) = 1 - P(T)$ and $1 \leq n \ \leq 5$
n : number of threat assessment cue
N : opposite hypothesis of T (10)

In (10), $P(T)$ stands for the probability of target for being a threat while $P(N)$ denotes the probability of a target to not being a threat. After the calculation of probability of T hypothesis, decision making process of this hypothesis is simply performed as follows:

$$f(t) = \begin{cases} P(T_i \mid \mathbf{C}) \ \geq \ \beta, \ t \ is \ threat \\ otherwise, \ \ t \ is \ not \ a \ threat \end{cases} \tag{11}$$

Judgment of the threat selection problem is performed by comparing hypothesis's probability value with certain reliable threshold found by experience.

C. The Calculation of Threat Assesment Rating

The danger level of potential target is calculated by taking account the subset of threat cues proposed in the literature due to limited capability of small-scale vessels. These cues are listed as speed, distance, heading, maneuver and time before hit which are described in cues section. Each cue forms its own score and contributes the total score with different weights. Roughly speaking, eventual threat rating is the total of these cues scores. The fundamental of the mechanism is given formulas below. $\mathbf{C} = \{C_1, C_2, C_3, C_4, C_5\}$ is the group of the scores produced by considering listed five threat assessment cues.

$$w_1 + w_2 + w_3 + w_4 + w_5 = 1 \tag{12}$$

$$V_a = \sum_{k=1}^{5} w_\mathrm{k} C_\mathrm{k} \ \ , \mathbf{C} \rightarrow [0, 1], V_a \in \mathbf{V} \tag{13}$$

$$V_i = w_1 s_i + w_2 d_i + w_3 h_i + w_4 m_i + w_5 t_i \tag{14}$$

Equation (12) shows the coefficients multiplied by each cues scores. The sum of these coefficients is equal to 1 to satisfy closed interval between 0 and 1 for threat assessment rating. (13) represents that the total of each weighted cues scores generates ultimate threat rating value of each target. (14) is the opened version of (13) that showing each cues separately and specialized interpretation of (13) for each iteration over time while calculating threat rating value. Weights of terms belonging to these equations are determined as a result of test scenarios of algorithms. It can be evaluated as empirical method to reach final results.

Threat selection process is another input of this phase as shown in Fig. 1. The priority is given to tracks classified as dangerous at selection phase. They are calculated in front and marked with different sign for attracting operator's attention. Threat assessment rating of those classified as assumed friend are also calculated, however, they do not require priority and listed below the dangerous ones.

IV. EVALUATION

To evaluate the threat evaluation model, we have created synthetic scenarios and measured the threat assessment cues for these scenarios. After the evaluation using synthetic scenarios, we have experienced the method on the real environment and compared with evaluation scenarios. In this paper we do not present the real environment results because of confidential manner. But the results are correlated with our synthetic scenario results.

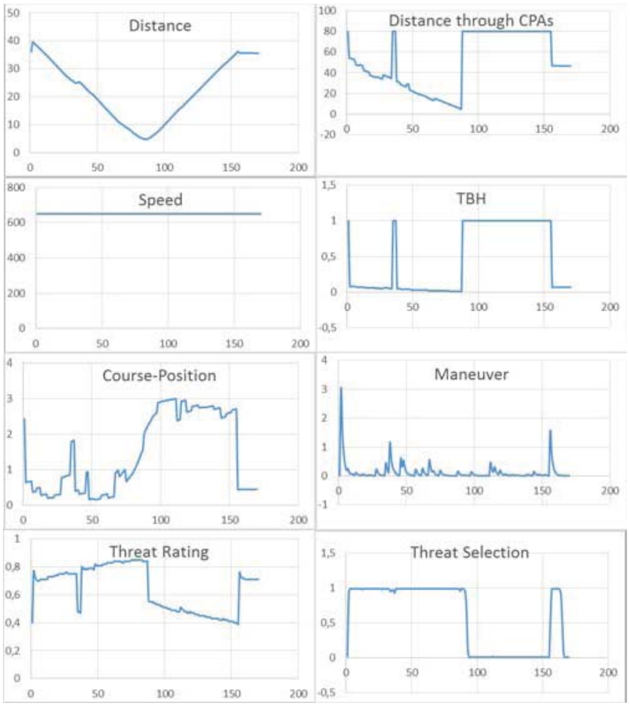


Fig. 4. Threat Assessment Parameters Scores and Resulting Threat Selection Probability and Threat Assesment Rating for Synthetic Scenario 1

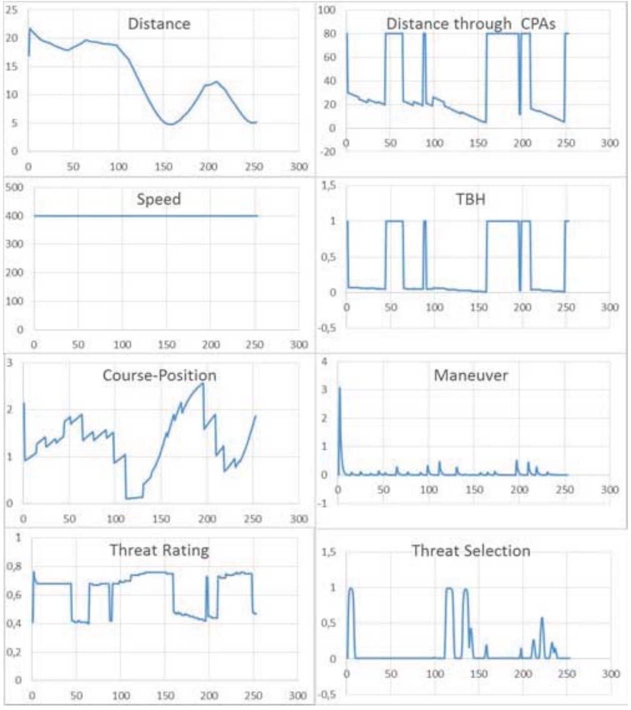


Fig. 6. Threat Assessment Parameters Scores and Resulting Threat Selection Probability and Threat Assesment Rating for Synthetic Scenario 3

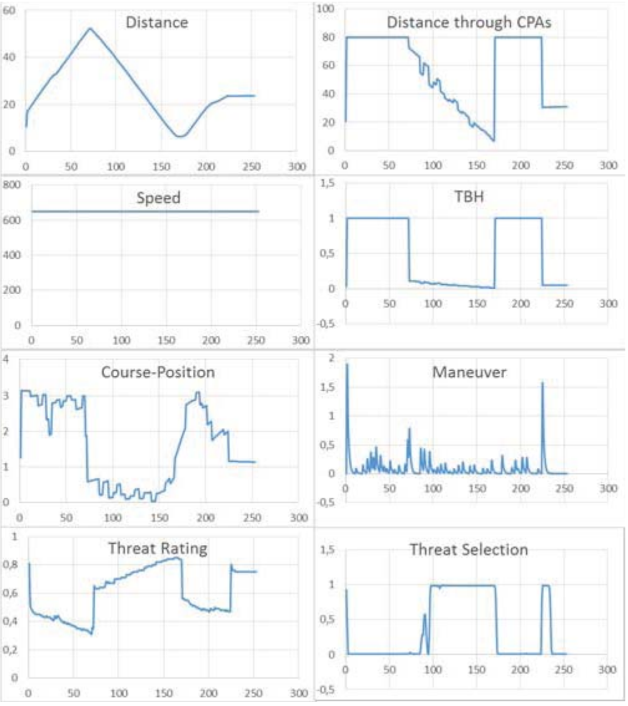
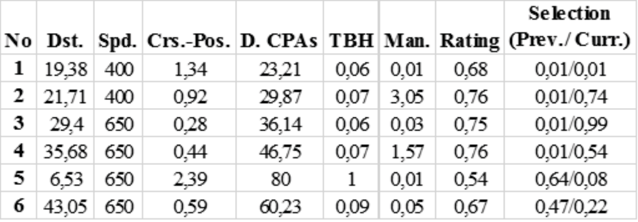


Fig. 5. Threat Assessment Parameters Scores and Resulting Threat Selection Probability and Threat Assesment Rating for Synthetic Scenario 2

Simulation of proposed solution to threat evaluation problem are fulfilled with synthetic scenario generator tool developed in purpose of feeding tracks data to combat management system. The tool is capable of defining user-specified routes for tracks by selecting waypoints over tactical display and defining own ship asset with its user-specified route and stationary speed. Three synthetic scenarios are chosen to present in this paper to reveal the behaviors of the algorithms in different circumstances. In the first scenario, suspicious object aims its heading in the direction of defended asset at the beginning. Then, it rotates far from own ship when it becomes closer. This scenario simulates dangerous behavior for own ship firstly. Target becomes non-hazardous in the end. The second scenario is the opposite version of the first scenario. While the object does not show any unfriendly behavior initially, it poses danger for defended asset toward the end of the scenario. The last scenario characterizes the behavior of random movements of an asset. The algorithms' outcomes are recorded to examine behaviors of these methods throughout iterations. Furthermore, direct distance of track from target, speed of suspected asset, course and position relation between track and target, distance of track from target by passing through CPA, TBH, maneuver score for target are recorded to investigate the effect of these cues over resulting threat selection outcome and threat assessment rating. Whole recorded values are transferred to line charts in order to facilitate the investigation process of results. It is practical and straightforward to examine the relationship of cues with resulting values visually. Before examining overall results, Table 1 gives example of random records that builds line charts in the end. In Table 1, it is possible to investigate the inputs of the algorithms and resulting outputs of algorithms from these inputs numerically. After the fusion of threat assessment cues according to threat evaluation model as described, resulting values are obtained for threat rating value and threat selection value in the end.

TABLE I. SAMPLES FOR INPUTS AND OUPUTS OF ALGORITMHS



No	Dst.	Spd.	Crs.-Pos.	D. CPAs	TBH	Man.	Rating	Selection (Prev./Curr.)
1	19,38	400	1,34	23,21	0,06	0,01	0,68	0,01/0,01
2	21,71	400	0,92	29,87	0,07	3,05	0,76	0,01/0,74
3	29,4	650	0,28	36,14	0,06	0,03	0,75	0,01/0,99
4	35,68	650	0,44	46,75	0,07	1,57	0,76	0,01/0,54
5	6,53	650	2,39	80	1	0,01	0,54	0,64/0,08
6	43,05	650	0,59	60,23	0,09	0,05	0,67	0,47/0,22

Fig. 4 shows the charts generated from the records of first synthetic scenario. In substance, firstly, the target roughly points its heading to the own ship and closing the distance from own ship. After a while, the target turns its heading to outside of own ship and move away from the defended asset as can be seen in Fig. 4.

In beginning of the first scenario, threat evaluation algorithm produces higher threat rating since the target's behavior is riskier for the defended target. Similarly, threat selection algorithm marks this behavior as potential threat activity over own ship. Second part of the target's movement reduces the tension and target quits being risky for own ship. Threat evaluation algorithm produces lower values after this move. However, threat selection method based on Bayesian Inference does not count the target as safe asset immediately. After couple of iterations is passed, the method is convinced about own ship' safety against the existence of the moving object.

Fig. 5 displays the line charts constructed from second scenario data storing parameters information and resulting threat rating and threat selection score from these parameters values. Transition from harmless situation to dangerous situation is observed when analyzing typical motion of track belong to this scenario. The target firstly moves away from the own ship, then, aims to own asset and becomes closer in course of time.

In the second scenario, the first stage of the run generates threat rating values lower than 0.5 in the interval between 0 and 1, which is convenient harmless movement of the target around own ship. Bayesian threat selection method is compatible with this outcome. The method does not interpret the target as dangerous object until the suspicious asset changes its direction to own ship. After this change on the motion of the target, threat rating sharply increases from 0.3 to 0.65. However, threat selection algorithm does not reflect this behavior to its conclusion instantly and remains to interpret target as safe for a while. The continuation of the motion brings the threat selection algorithm to outcome that classifies the object as dangerous.

Fig. 6 gives an example of a target that changes its route excessively and the response of the threat algorithms to this type of behavior. It is possible to observe the effect of this unstable attitude of the target on the results of threat algorithms. There is a fact that random threat motion results sudden change in threat rating algorithm and spikes in threat selection method. This scenario shows the necessity of improvement in algorithms to handle such situations. In this case, operator would receive many false alarms and blinking display in front.

As can be seen in whole figures, threat rating is a changing value for each cycle of sensor's target data supply since it is calculated with the current cue scores for that iteration. Threat history is an important feature for operators to interpret the evaluation of dangerousness [9]. Instant cue score could be different from the cue score belonging to previous iteration because of momentary faulty sensor reports and unbalanced information. As a result, indication of these line charts to user, also, could be another support for decision-making process.

V. RELATED WORK

There are various threat evaluation algorithms mainly based on rule based, fuzzy logic and Bayes network in the literature as follow:

A rule based threat evaluation algorithm is proposed by making use of inferences arising from questionnaires conducted with U.S. Navy officers [12]. Threat assessment parameters are discovered by benefiting from experiences of U.S. Navy personnel and these parameters become fundamental inputs of suggested rule based algorithm.

A fuzzy knowledge-based system brings alternative rule based approach by using calculate the values of threats, using altitude, speed, CPA, and range as threat assessment cues to calculate threat values of targets [20].

Threat evaluation process using fuzzy sets theory is introduces in another study [11]. Eleven parameters are effective factors for the calculation of threat posed by surrounding units. The design of the algorithm is tested with a synthetic air defense scenario and four real-time air defense scenarios.

Okello and Thoms present a Bayesian Network based threat evaluation algorithm that uses estimations of target state and their uncertainty measurements arising from a tracking and data fusion module in order to evaluate the threat level of a given unfriendly entity on a defended asset [14].

Another threat evaluation system based on Bayesian Network is developed in Johansson's study [8]. Mainly, target type, weapon range, speed, TBH and distance are used as threat assessment cues. These parameters become the nodes of Bayesian Network while constructing the relationship among them.

Threat evaluation domain is still open to discussion and expects for new approaches carrying current works one more step further. The process turns into more challenging problem when experiencing it on the platform with limited capability. Since small-scale vessels could not have high technological equipment providing more details about battle area, the right use of existing information becomes more critical within threat evaluation procedure as a matter of course.

VI. CONCLUSION

In this paper, we have presented the definition of threat evaluation process along C2 processes and the importance of threat evaluation in military defense domain. Existing threat evaluation methods provide solution to generic problem. However, directly adapting existent threat evaluation methods to the platform with limited capability is not applicable due to limitations of small-scale platforms that affect inputs of the threat evaluation algorithm excessively. Therefore, a literature review is performed to determine the threat assessment cues convenient for the intruder and the defended asset whose speed, course and position are known. Speed, distance, maneuver, heading-position relation and TBH are selected cues that utilize the capacity of kinematic parameters effectively.

We present method named as threat selection method accepting cores of threat assessment cues to increase decision making support for the operator. This information is somehow alternative evaluation of kinematic parameters with Bayesian Inference. Entire threat assessment cues except TBH is used in the process of threat selection. Instead of TBH, distance between the intruder and defended asset and passing through CPAs of these assets is used to fulfill the conditional independence precondition for Bayesian Inference since TBH and speed cue are tightly related with each other.

After the selection phase, threat assessment rating is calculated by using scores prepared from mentioned threat assessment cues under certain conditions. Targets classified as dangerous are prioritized for the threat rating calculation and marked with recognizable sign to grab operator's attention.

The implemented Bayesian threat selection algorithm and the method of the threat rating calculation have been tested with synthetic scenarios and results of methods are given for the further investigation of readers. Threat selection method gives definite answer to the question whether target should be as threat after evaluation of mentioned cues. In other words, numerical results of threat selection algorithm are mostly very close to 0 or 1, which facilitate to reach conclusion that conducted hypothesis is true or false. Threat rating changes logically with respect to scores arising from threat assessment cues.

In this paper, threat evaluation model described in Fig.1 produces separate tactical information completely independent of one another for the use of operator. As a future work, the combination of threat selection algorithm and the calculation phase of threat assessment rating could serve weapon assignment problem directly. Additionally, a modern surface platform should take care of all threats owning different environmental types. There is no such classification in current model since the system is deprived of this information. A preliminary phase can be performed before threat evaluation process to detect the environment of targets. Speed data seems to be key factor while performing this preliminary phase. As a result, speed and maneuver cues of the model will be heavily affected from this update. Furthermore, this design does not include any interaction with the operator. Operator input could improve performance of the system. Category and identification information coming from operator perspective provide valuable feedback to system and threat selection and threat rating algorithm can take into count these operator's feedback while determining final results. Moreover, weight values used in threat selection algorithm can be determined by a survey conducted with experienced C2 operators. Besides, the use of smoothing signal techniques can be investigated in order to solve spike problems discovered in third synthetic scenario. Moreover, each processes could be improved by benefiting from unused threat assessment cues in case of the use of the system in better equipped platforms than small-scale ones. These improvements will shorten decision cycle of operator and make them executes rapidly in the end.

REFERENCES

[1] Irandoust, H., A. Benaskeur, F. Kabanza, and P. Bellefeuille. "A mixed-initiative advisory system for threat evaluation". in *Proceedings of the 15th International Command and Control Research and Technology Symposium: The Evolution of C*. 2010.

[2] Riveiro, M., T. Helldin, M. Lebram, and G. Falkman. "Towards future threat evaluation systems: user study, proposal and precepts for design". in Information Fusion (FUSION), 2013 16th International Conference on. 2013. IEEE.

[3] Boyd, J.R., "The essence of winning and losing". Unpublished lecture notes, 1996.

[4] Park, S.C., Y. Kwon, K. Seong, and J. Pyun, "Simulation framework for small scale engagement". Computers & Industrial Engineering, 2010. **59**(3): p. 463-472.

[5] Mury, B.N., Bao, "A Recursive Engagement Simulation Tree (REST) For Use in Maritime Defence". 2007, Defence R&D Canada – Atlantic.

[6] Paradis, S., A. Benaskeur, M. Oxenham, and P. Cutler. "Threat evaluation and weapons allocation in network-centric warfare". in *Information Fusion, 2005 8th International Conference on*. 2005. IEEE.

[7] Bolderheij, F. and P. Van Genderen. "Mission driven sensor management". in *Proceedings of the 7th International Conference on Information Fusion*. 2004.

[8] Johansson, F. and G. Falkman. "A Bayesian network approach to threat evaluation with application to an air defense scenario". in *Information Fusion, 2008 11th International Conference on*. 2008. IEEE.

[9] Liebhaber, M.J. and B. Feher, "Air threat assessment: Research, model, and display guidelines". 2002, DTIC Document.

[10] Liebhaber, M.J. and C. Smith, "Naval air defense threat assessment: Cognitive factors and model". 2000, DTIC Document.

[11] Azimirad, E. and J. Haddadnia, "A New Data Fusion Instrument for Threat Evaluation Using of Fuzzy Sets Theory". International Journal of Computer Science and Information Security, 2015. **13**(4): p. 19.

[12] Liebhaber, M.J., D. Kobus, and B. Feher, "Studies of US Navy air defense threat assessment: Cues, information order, and impact of conflicting data". Studies, 2002.

[13] Johansson, F., "Evaluating the performance of TEWA systems". 2010.

[14] Okello, N. and G. Thorns, "Threat assessment using Bayesian networks". Information Fusion, 2003: p. 1102-1109.

[15] Liebhaber, M.J. and B. Feher, "Surface warfare threat assessment: Requirements definition". 2002, DTIC Document.

[16] Robusto, C., "The cosine-haversine formula". The American Mathematical Monthly, 1957. **64**(1): p. 38-40.

[17] Box, G.E. and G.C. Tiao, "Bayesian inference in statistical analysis". Vol. 40. 2011: John Wiley & Sons.

[18] de Vos, A.F., "A primer in Bayesian Inference". preprint, 2004.

[19] Russell, S. and P. Norvig, "AI a modern approach". Learning, 2005. **2**(3): p. 4.

[20] Liang, Y. "An approximate reasoning model for situation and threat assessment". in *Fuzzy Systems and Knowledge Discovery, 2007. FSKD 2007. Fourth International Conference on*. 2007. IEEE.