 ISSN: 2442-6571

Target threat assessment using fuzzy sets theory

Ehsan Azimirad[a,1,*], Javad Haddadnia[b,c,2]

[a] *Electrical and Computer Engineering Department, Hakim Sabzevari University, Sabzevar, Iran*
[b] *Associate Professor, Electrical and Computer Engineering Department, Hakim Sabzevari University, Sabzevar, Iran*
[1] *e.azimi@hsu.ac.ir*; [2] haddadnia@hsu.ac.ir;*

ARTICLE INFO

Article history:
Received April 07 2015
Revised May 02 2015
Accepted May 05 2015

Keywords:
Threat assessment
Military applications
Fuzzy sets theory
Dynamic air targets
Multi sensor data fusion

ABSTRACT

The threat evaluation is significant component in target classification process and is significant in military and non military applications. Small errors or mistakes in threat evaluation and target classification especial in military applications can result in huge damage of life and property. Threat evaluation helps in case of weapon assignment, and intelligence sensor support system. It is very important factor to analyze the behavior of enemy tactics as well as our surveillance. This paper represented a precise description of the threat evaluation process using fuzzy sets theory. A review has been carried out regarding which parameters that have been suggested for threat value calculation. For the first time in this paper, eleven parameters are introduced for threat evaluation so that this parameters increase the accuracy in designed system. The implemented threat evaluation system has been applied to a synthetic air defense scenario and four real time dynamic air defense scenarios. The simulation results show the correctness, accuracy, reliability and minimum errors in designing of threat evaluation system.

I. Introduction

Target threat assessment for air action is one of the most important processes in military command and control, since its result supports the commander making decisions and selecting alternative military actions. Many researchers have studied target recognition or threat assessment, however, the aerial target threat assessment is still an open issue. Obtaining an accurate threat assessment of adversarial targets requires combining large amounts of information from multiple sensors as different attributes creating different risks. The information provided by these multiple sensors is often incomplete or uncertain disturbed by nature or characterized by not only randomness but also fuzziness. In addition, it's quite difficult to achieve the exact threat degree because of the limitation of time and the jamming of the hostile target in the real complex warfare, and usually we just gain a fuzzy threat degree range[1],[2].

The various defended assets can be air bases, tourist places, bridges, camps, nuclear power plants, command post, harbors, radars, monuments, parliament's buildings, etc. In the war as well as peace keeping scenario it becomes critical to understand the possible enemy dynamic targets such as aircrafts (bomber, fighter, and transporter), missiles, helicopters, etc which can be manned or unmanned targets. 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 [3]. The dynamic targets are those targets which are mobile and exhibit change in their characteristic behavior. Various factors are considered for a decision making augmented with human cognitive intelligence.

An expert system built with help of fuzzy logic can play an important role in enhancing situation awareness and automated decision making. The protection of defended assets is the prime objective of threat evaluation modeling of dynamic targets. An assumption is made that defending targets act as potential threats, but targets may be friend or enemy which is decided by IFF (Identification, friend or foe). The IFF is designed by command and control system. In this situation, prioritization of potential threats is very important according to threat level (Degree of threat) of detected enemy

targets via multi resources. Battle space and intelligent sensors help in target classification. Threat value quantifies the possibility of threat or danger imposed by a potential target. In this situation of possible multiple targets, it becomes critical to prioritize the degree of threat involved with them to decide which target is more dangerous via predicting the threat value.

Threat value is directly proportional to the amount of danger a target produces towards the protected asset. The higher threat value implies more dangerous target. This analysis in turn will play a significant role in weapon allocation against suspicious targets. 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 [4], [5]. The degree of threat, known as threat value, can also be used to support intelligent sensor management [6],[7], 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 [8].

Threat evaluation is a high-level information fusion process that in relation to the JDL model of data fusion [9] belongs to level 3 [3], [6], [8], i.e. it is part of impact assessment. A grid of sensors produces large amount of heterogeneous data which can be used to evaluate the degree of threat of a target. Thus threat evaluation is a high level information fusion process. At times the threat evaluation becomes challenging in the presence of multiple parameters and processes. There is some amount of uncertainty involved in these parameters depending on the nature of targets and assets involved. It is difficult to formulate mathematical model by using selected parameters as inputs to generate the threat value as an output. The fuzzy inference system turns out to be one of the most efficient methods for the threat evaluation of dynamic targets under uncertain condition. In this paper, we describe the importance of threat evaluation in introduction section.

Data fusion has its roots in the defense research community of the early 1980's. As a result the first data fusion models were either adapted from existing military oriented process models or were designed with a distinctly military flavor [10]. More recently the use of data fusion has broadened to include industrial, medical and commercial applications. More recent models have acknowledged this migration by reducing the military terminology. However, this still exists to some extent (and needs to be changed). Sensor network configuration, the display information and feedback within the network integration, some of the major issues in the implementation of a process model are considered. In Fig. 1, a data fusion model is presented for use in various applications. The model in this paper is useful JDL data fusion systems are usually discussed in the context of the military.

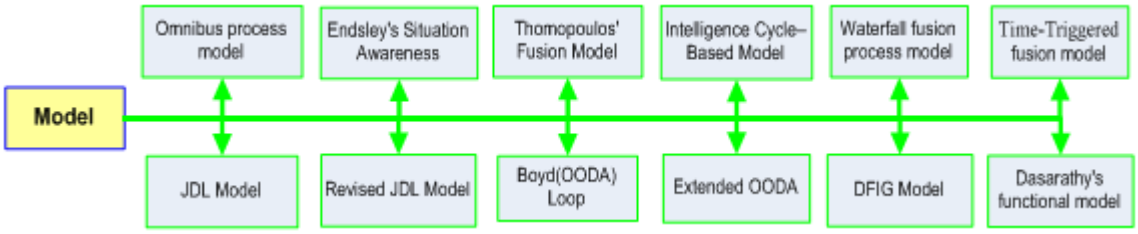


Fig. 1. Multi sensor Data Fusion Models

The remainder of this paper is organized as follows. In section II, a precise description of the threat evaluation consisting of definition, modeling and evaluation in JDL model with threat parameters is presented. In section III fuzzy based approach for designing a new fuzzy model in fuzzy sets theory is presented. In section IV, simulation and results are presented. In this section, case study is demonstrated in four scenarios for static and dynamic targets. The calculation of threat values in the system is performed by making inference in a fuzzy model. The structure of this fuzzy model is described, together with an analysis of the system's behavior as applied to a synthetic scenario. Finally, in section V the paper is concluded and thoughts regarding future work are presented.

II. Threat Evaluation in JDL Model

A. Threat Definition

The threat is an expression of intension to inflict evil, injury, or damage [4,8]. These threats are ac-cording to Steinberg [8] 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. The threat evaluation is significant component in target classification process. Small errors or mistakes in threat evaluation and target classification can result in huge damage of life and property. A threat is often assessed as a combination of its capability and intent ([8],[11]-[16]). 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 [17]. In [13], 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 [18]. Threat evaluation helps in case of weapon assignment, and intelligence sensor support system[19]-[21]. It is very important factor to analyze the behavior of enemy tactics as well as our surveillance. Disastrous situation in terms of loss of life and the valuable assets occur due to wrong evaluation of threat value. In this case we will suffer more as damages so it is important to evaluate more accurately. Threat evaluation is a process based on defending targets to defended asset; here an assumption is to protect one asset against several defending targets but consideration of more number of assets will give realistic feel towards threat evaluation.

B. JDL Model

It is a high level information fusion technique that belongs to third level data fusion model in Joint Directors of Laboratories (JDL) as seen in Fig. 2.

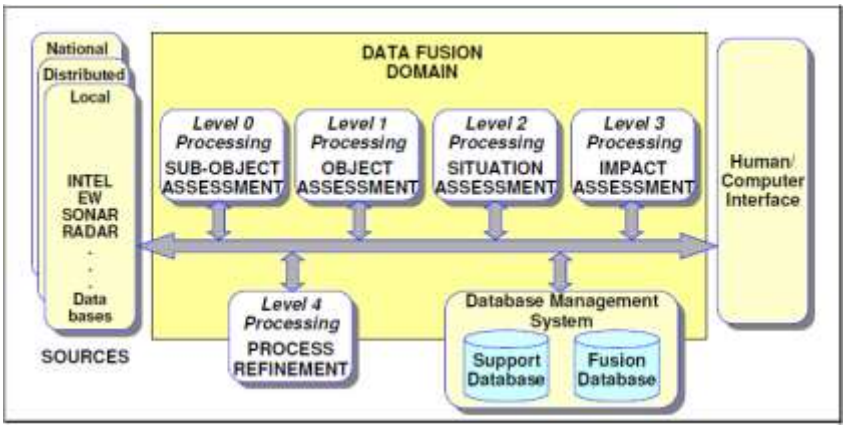


Fig. 2. The JDL Model.

The JDL model comprises different levels [22]-[26]:

Level 0: Sub-Object Data Assessment: At this level, data is accessed from different sources, which may be localized or distributed. The main task of this level is to pre-process data by correcting biases and standardizing the input before the data from variety of sources is fused.

Level 1: Object assessment: Assessment and prediction of entity states on the basis of observation-to track association for continuous state estimation (e.g. kinematics) and discrete state estimation (e.g. Target type and ID) is done in this level.

Level 2: Situation Assessment: Assessment and prediction of relations between the entities and relationship with the surrounding is focused in this level. This includes force structure, cross force relations, communications, perceptual influences, physical context, etc.

Level 3: Threat Assessment: Assessment and prediction of effects on situation of planned or estimated/predicted actions by the participants; to include interactions between action plans of multiple players is the main focus of this level.

Level 4: Process Refinement: This level focuses on the optimization of over all information fusion process that is an element of Resource Management.

C. Threat Modeling

Consider a tactical situation where we have a set of defended assets $A = \{A_1, A_2, ..., A_m\}$ that we are interested in to protect (e.g. friendly forces, ships, bridges, and power plants). There is also a set of targets $T = \{T_1, T_2, ..., T_n\}$, 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 $Th(i, j): T \times A \rightarrow [0,1]$, assuming numbers between 0 and 1. Threat value of i th available defended asset from j th attacking target is $Th(i, j)$. The threat evaluation model is proposed in Fig. 3.

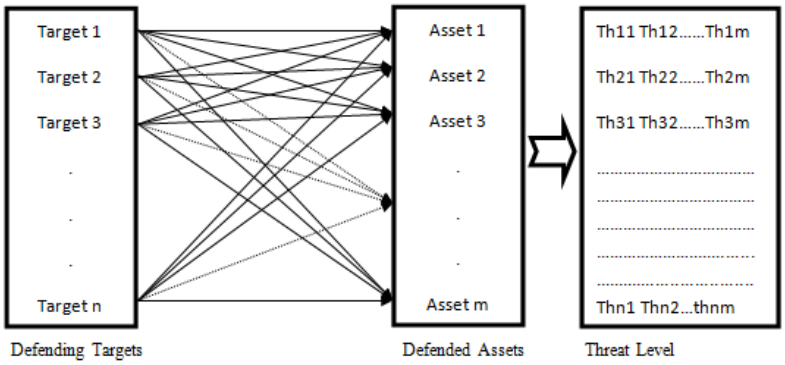


Fig. 3. Asset- target pairs

The numbers 0 is lowest possible threat value and 1 is highest possible threat value.

D. Parameters for Threat Assessment

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 [27]. 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.

The variety of parameters are proposed and used by researchers for threat evaluation [3],[4],[6],[22],[34],[28]-[33]. These parameters have varying degree of effect on the threat value. Some parameters for calculating threat value are dependent on other parameters. For example, the visibility and maneuvers parameters are dependent on other. If atmospheric conditions were bad then the target cannot be maneuvers and if atmospheric conditions were good then the target can be maneuvers. This dependence is considered in rule based fuzzy sets. A number of parameters [31] are discussed with their descriptions in Table 1. These parameters have been classified as follows.

Table 1. Target of parameters

Attribute	Description
Speed	Approximate air speed or an indication Of change (e.g., increasing).
Altitude	Approximate feet above ground or an indication of change (e.g., climbing).
Range/ Distance	The track's distance from own ship.
CPA	Closest Point of Approach Estimated distance that track will pass by own ship if the track and own ship remain On their current courses.
Weapon envelope	The track's position with respect to its Estimated weapons envelope.
Own Support	Availability of nearby friendly ships Or patrol aircraft.
Visibility	Approximate number of miles, or an indication of atmospheric conditions (e.g., haze).
Maneuvers	Indicates the number of recent maneuvers, or if the track is following The ship.
Fire	The Target Fire into Asset
IFF Mode	Identify Friend or Foe. Signals from a track that indicate if it is a friendly, or Perhaps neutral.
Target Support	Availability targets for assistance to enemy target

- Proximity parameters: An important class of parameters for assigning threat values to target-defended asset pairs, i.e. CPA parameter.

- **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. The several central parameters here are target type, weapon type and weapon envelope.

- **Intent parameters:** The class of intent parameters is a broad category, containing parameters that can reveal something about the target's intent. The several parameters here are speed, heading [35], altitude and maneuvers [36].

III. Fuzzy Sets Theory

Fuzzy inference based on fuzzy sets theory is the process of formulating the mapping from a given input to an output using fuzzy logic. The mapping then provides a basis from which decisions can be made, or patterns determined. The process of fuzzy inference involves all of the sections: Membership Function, Logical Operation, and If-Then Rules [30]. In this paper one kind of rule-based algorithm is suggested [37]-[41], in which fuzzy inference rules are used to calculate the level of threat air targets pose to a navy combat ship, using speed, altitude, range, CPA, weapon envelope, own support, visibility, maneuver, fire, target support and IFF as input parameters and threat value as output parameter. This matter is demonstrated in Fig. 4. For each input parameter, multiple membership functions are defined. 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 steps involved for threat value [5]:

1. Select target's information as inputs and threat rating as output.

   Threat Evaluation Fuzzy Model is presented in Fig. 4.

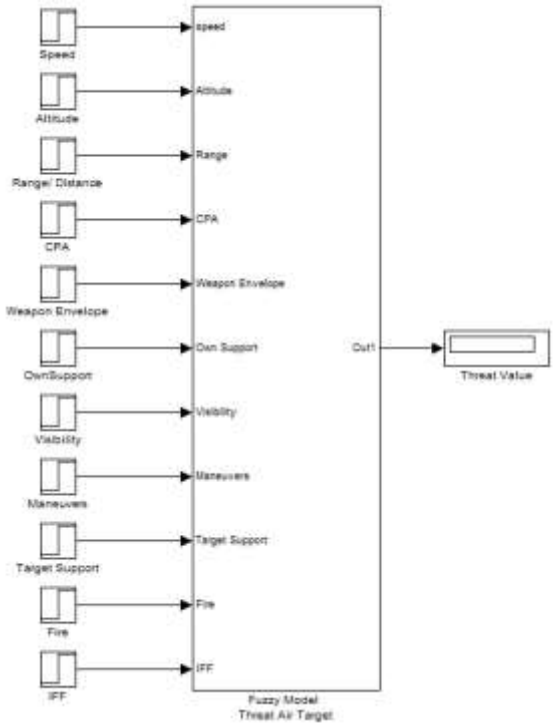


Fig. 4. TEFM (Threat Evaluation Fuzzy Model)

2. Decide membership functions for each input and output parameters.

Membership function of parameters is triangular. Each of the parameters was explained in following: Targets have maximum 1400 knot speed. The targets can achieve maximum 50000 ft Altitude but it depends on the type of target. Maximum range detected by the radar system will be 200 nautical miles but this range depends on the power of radar system. CPA can be calculated from velocity vector and position of asset. Maximum CPA is considered 200 feet. Weapon envelope can be calculated as distance. Maximum weapon envelope is considered 300km for every of targets. visibility is considered between 4 to 20 mA [9]. These parameters are demonstrated in Fig. 5:

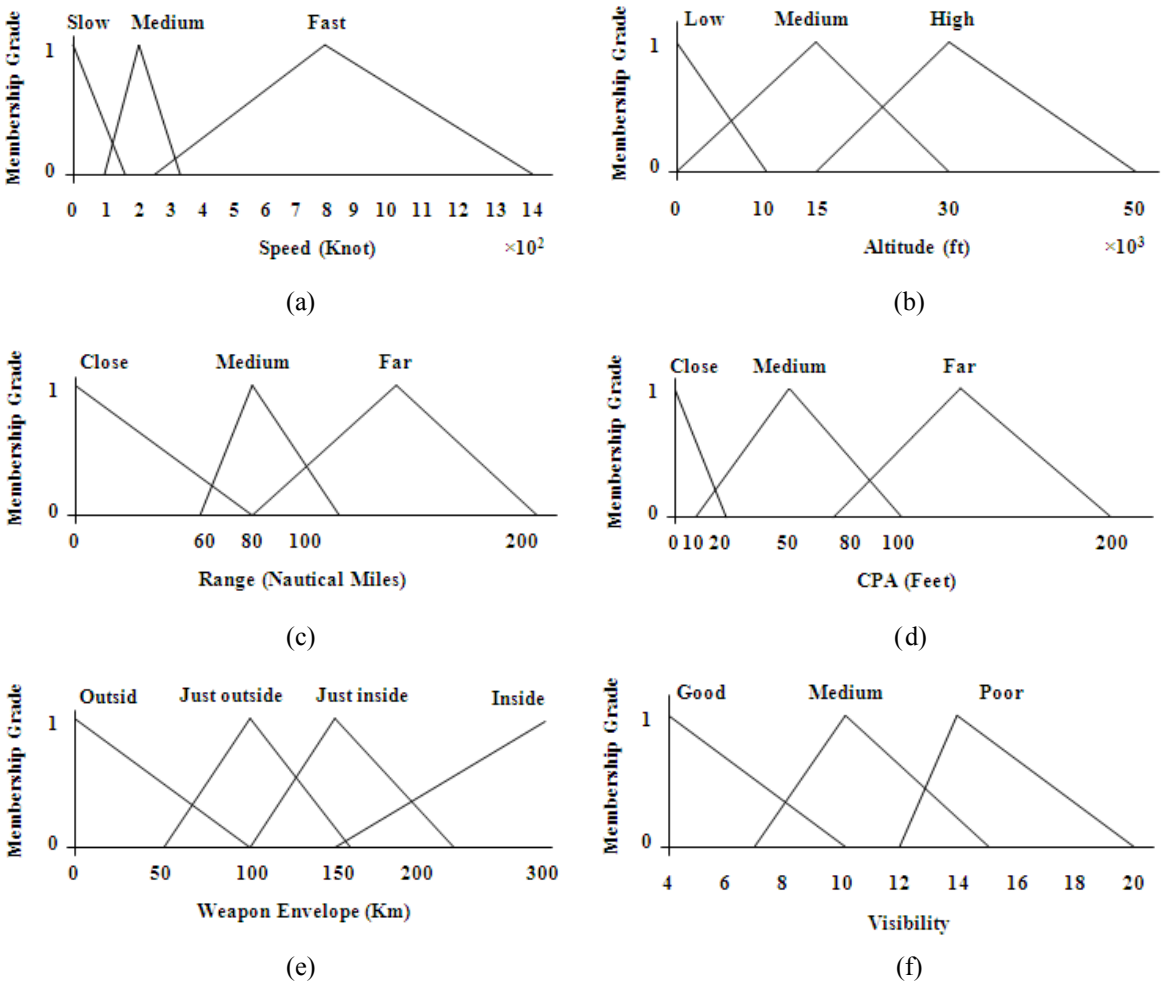
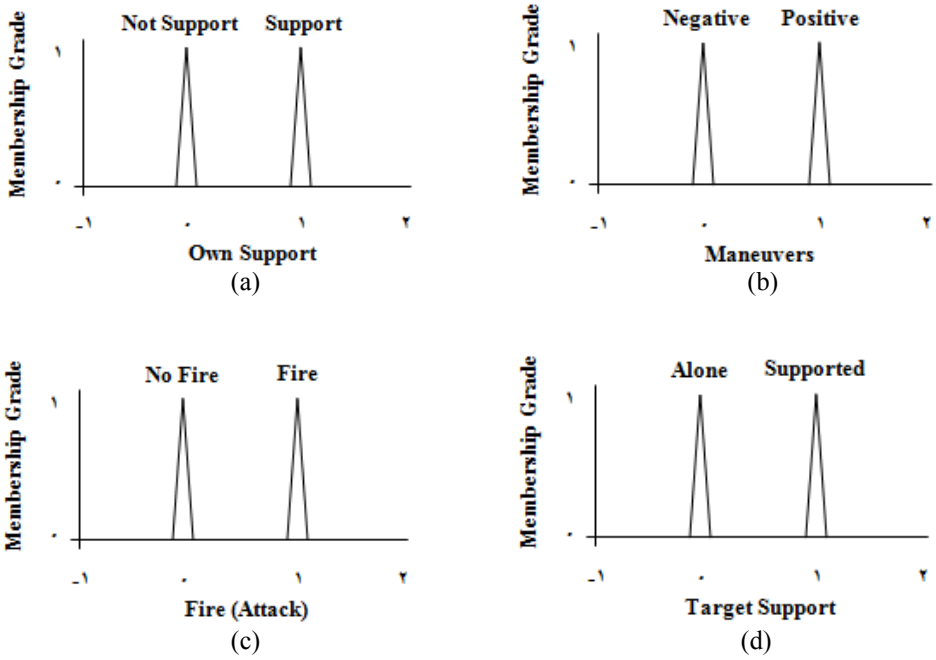
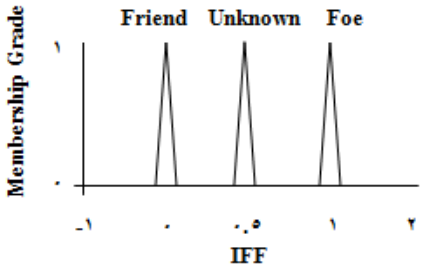


Fig. 5. Membership functions for input parameters: (a) Speed, (b) Altitude, (c) Range, (d) CPA, (e) weapon envelope, (f) visibility

The residue of input parameters consists of own support, maneuver, fire, target support and IFF are considered 0 and 1 as seen in Fig. 6. These are singleton.





(e)

Fig. 6. Membership functions for other parameters: (a) own support, (b) maneuvers, (c) fire, (d) target support, (e) IFF

The output parameter in threat evaluation of fuzzy model is threat rating that is between 0 and 1 as seen in Fig. 7.

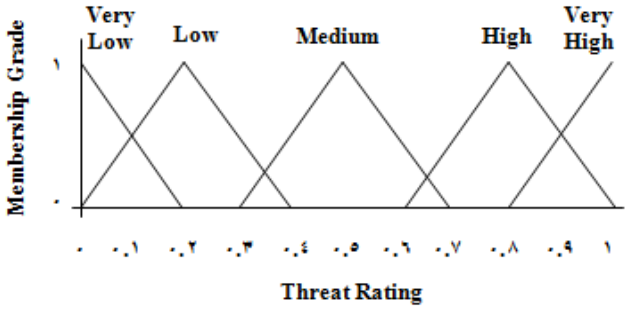


Fig. 7. Membership functions for threat rating

3. Determine fuzzy rules by using inputs and output.

Determine fuzzy inference rules using some standard data available and the expert's comments on the relation between the inputs and output. Some tentative rules are framed and the results are evaluated for the validity of the results with respect to the real time and synthetic scenario. These inputs change the threat rating via rules. In this paper is defined 331 rules that has caused the system is robust and efficient. A few of fuzzy inference rules that have been used in the implementation shown in Table 2.

Table 2. A few of fuzzy inference rules used in this paper

Rule Number	Description
Rule 1	IF (Altitude is low) AND (Speed is fast) AND (Range is close) AND (CPA is close) THEN (Threat Rating is very high) (Weight: 1).
Rule 2	IF (Altitude is high) AND (Speed is slow) AND (Range is far) AND (CPA is far) THEN (Threat Rating is very low) (Weight: 1).
Rule 3	IF (Altitude is medium) AND (Speed is medium) AND (Range is medium) AND (CPA is medium) THEN (Threat Rating is medium) (Weight: 1).
Rule 4	IF (Altitude is low) AND (Speed is fast) AND (Range is far) THEN (Threat Rating is medium) (Weight: 1).
Rule 5	IF (Altitude is high) AND (Speed is fast) AND (Range is far) THEN (Threat Rating is very low) (Weight: 1).
Rule 6	IF (Altitude is low) AND (Speed is slow) AND (Range is close) AND (weapon envelope is outside) THEN (Threat Rating is very low) (Weight: 1).
Rule 7	IF (Altitude is low) AND (Speed is slow) AND (Range is close) AND (Weapon Envelope is inside) THEN (Threat Rating is high) (Weight: 1).
Rule 8	IF (Own Support is Not Support) AND (Fire (attack) is Fire) AND (Target Support is supported) AND (IFF is foe) THEN (Threat Rating is high) (Weight: 0.9).

IV. Simulation and Results

To demonstrate the threat evaluation application, we have constructed a test scenario. The scenario consists of a four defended asset and three air targets (one Boeing 747, one F-16, and one B-2 bomber). This scenario is discussed in four case studies for dynamic targets and is discussed in twelve samples for static targets of parameters. Fig. 8 demonstrated battle environment.

Fig. 8. Combat environment in the test scenario

A. Static Scenario

Simulation of block diagram proposed fuzzy model is completed for threat evaluation of targets by using the MATLAB software as seen in Fig. 9. The figure shows a static scenario which is reads the input parameters as constant information in every time. This information is obtained from the radar system connected in the command and control unit. The underlying Fuzzy Inference System evaluates the value of threat for every one of the defended assets.

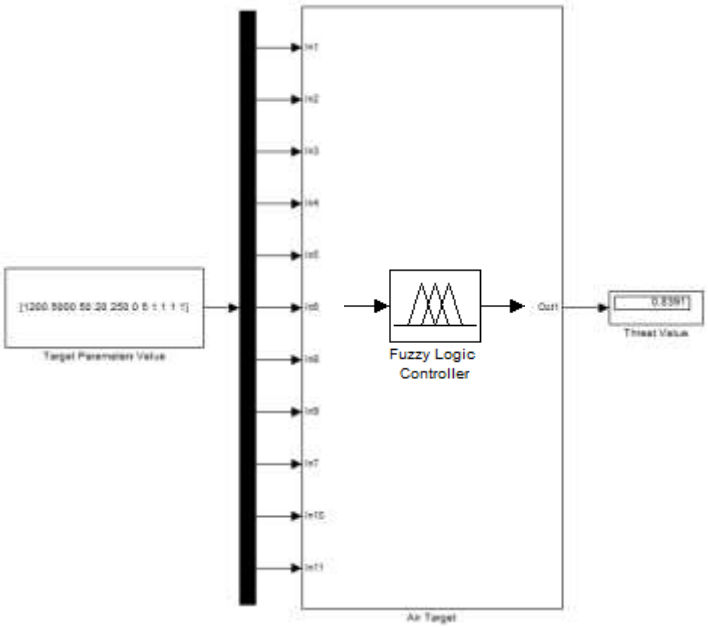


Fig. 9. Static fuzzy model of threat evaluation in MATLAB

Simulation of this fuzzy model is done for the multiple set of inputs for the various example targets in static scenario. For example: For the input information like Altitude 5000 ft, Speed 1200 knot, range 50 in nautical miles, CPA 20 in ft, weapon envelope 250 km, visibility 5mA, own support 0 and other parameters are 1, the output generated is the threat rating 0.8377 (which lies between 0 and 1). It will change when values of parameter change time to time. Higher the threat

rating identifies more dangerous target. The value of the threat rating will guide the decision making to engage the weapons in the process of protecting the assets from the targets. Simulation results in static test scenario for 10 instants are demonstrated in Table 3.

Table 3. Simulation results in 10 instants static test scenario

Static Scenario Numbers	Threat Values for T_1 Target in Static Scenarios											
	Speed	Altitude	Range	CPA	Weapon Envelope	Own Support	Visibility	Maneuver	Fire	Target Support	IFF	Threat Value
1	100	30000	180	80	50	1	5	0	0	0	0	**0.1665**
2	100	30000	180	80	50	0	5	0	0	0	0	**0.1187**
3	500	4000	180	150	50	0	5	0	0	0	0	**0.3134**
4	500	15000	120	80	50	1	5	1	1	0	0	**0.4743**
5	500	15000	120	80	50	1	5	1	1	1	1	**0.5784**
6	1000	10000	20	15	190	1	15	1	1	0	0	**0.8150**
7	1000	10000	20	15	190	1	15	1	1	1	1	**0.8321**
8	1200	5000	50	20	250	0	5	0	0	0	0	**0.4632**
9	1200	5000	50	20	250	1	5	1	1	0	0	**0.8032**
10	1200	5000	50	20	250	0	5	1	1	1	1	**0.8377**

B. Dynamic Scenario

In this section, several scenarios for simulation dynamic air targets and threat evaluation them are discussed. Then for evaluating of robustness and efficiency of fuzzy model is done the comparison between them. The Fig. 10 shows a dynamic scenario which is reads the input parameters as information in real time problems that vary on time.

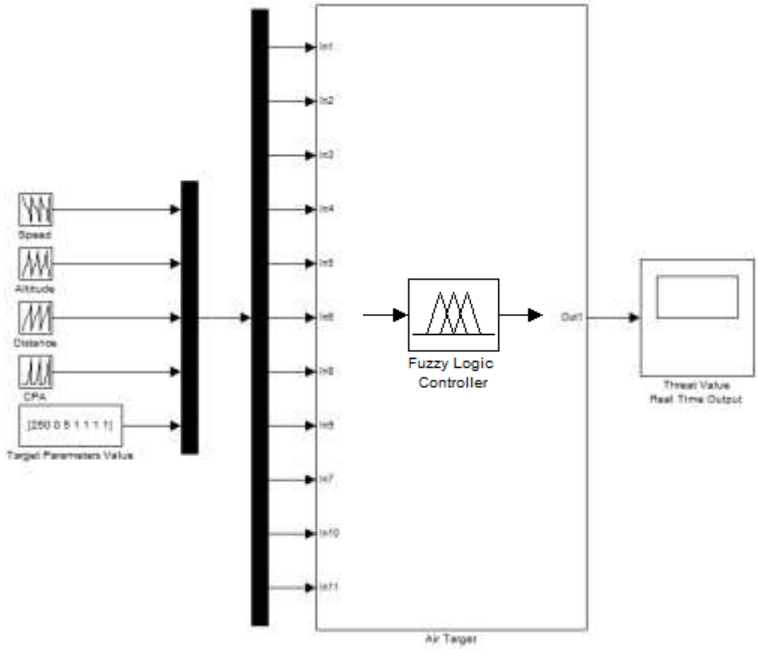


Fig. 10. Dynamic fuzzy model of threat evaluation in MATLAB

B.1 The First Scenario

In the all of scenarios, inputs of fuzzy model consist of speed, altitude, range and CPA are stated on real time information and the other inputs are constant information (static). In the first of scenario

(Fig. 11) has been assumed that enemy target (Target1) be closed to defended asset (Asset1). Every one of input parameters is varied as follow. The speed parameter of target with the increasing variable values is considered to be [153، 324، 564، 759، 900، 1040] knot in six different times. The altitude parameter of target with the decreasing variable values is considered to be [42830، 30025 ،21203، 17000، 10210، 5296] ft in six different times. The range and CPA parameters of target with the decreasing variable values respectively are considered to be [180، 143، 125، 100، 80، 30] nautical miles and [173، 125، 90، 60، 40، 10] feet in six different times. Also, weapon envelope is 250 km, visibility is 5mA, own support is 0 and the rest of the parameters are 1. The projection of combat environment and the time variation of each of the four parameters speed, altitude, range and CPA used in the first of scenario is demonstrated in Fig. 12.

Fig. 11. Projection of combat environment used in the one scenario

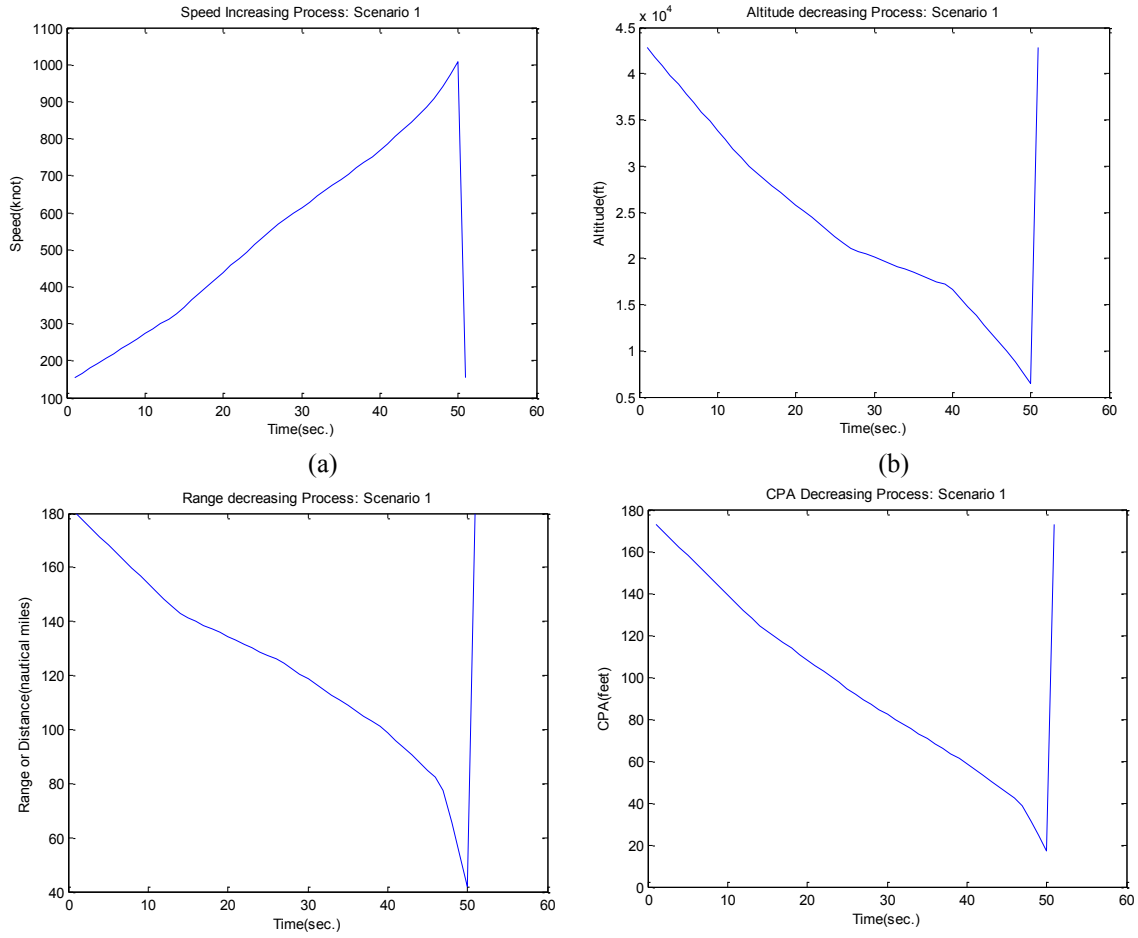


Fig. 12. The time variation of the target: (a) Speed, (b) Altitude, (c) Range, (d) CPA

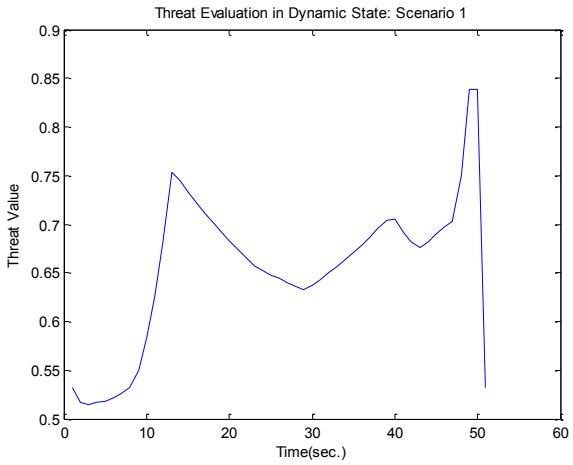


Fig. 13. The output of threat fuzzy model in first scenario

Fig. 13 shows the output of the fuzzy system threat assessment. By considering the amount of above, threat value increase significantly because the speed parameter is increased and three other parameters are decreased. The final threat value in the first scenario is got 0.8391. It shows that the threat is very high.

B.2 The Second Scenario

In the second of scenario (Fig. 14) has been assumed that enemy target (Target2) be fared from the defended asset (Asset2). Every one of input parameters is varied as follow. The speed parameter of target with the decreasing variable values is considered to be [1300، 950، 764، 259، 190، 40] knot in six different times. The altitude parameter of target with the increasing variable values is considered to be [2000، 3153، 7000،10000، 15000، 19000] ft in six different times. The range and CPA parameters of target with the increasing variable values respectively are considered to be [15 ،22، 36، 78، 112، 140] nautical miles and [2، 5، 12، 15، 20، 35] feet in six different times. Also, weapon envelope is 150 km, visibility is 5mA, own support is 0 and the rest of the parameters are 0. The projection of combat environment and the time variation of each of the four parameters speed, altitude, range and CPA used in the second of scenario is demonstrated in Fig. 15.

Fig. 14. Projection of combat environment in the second scenario

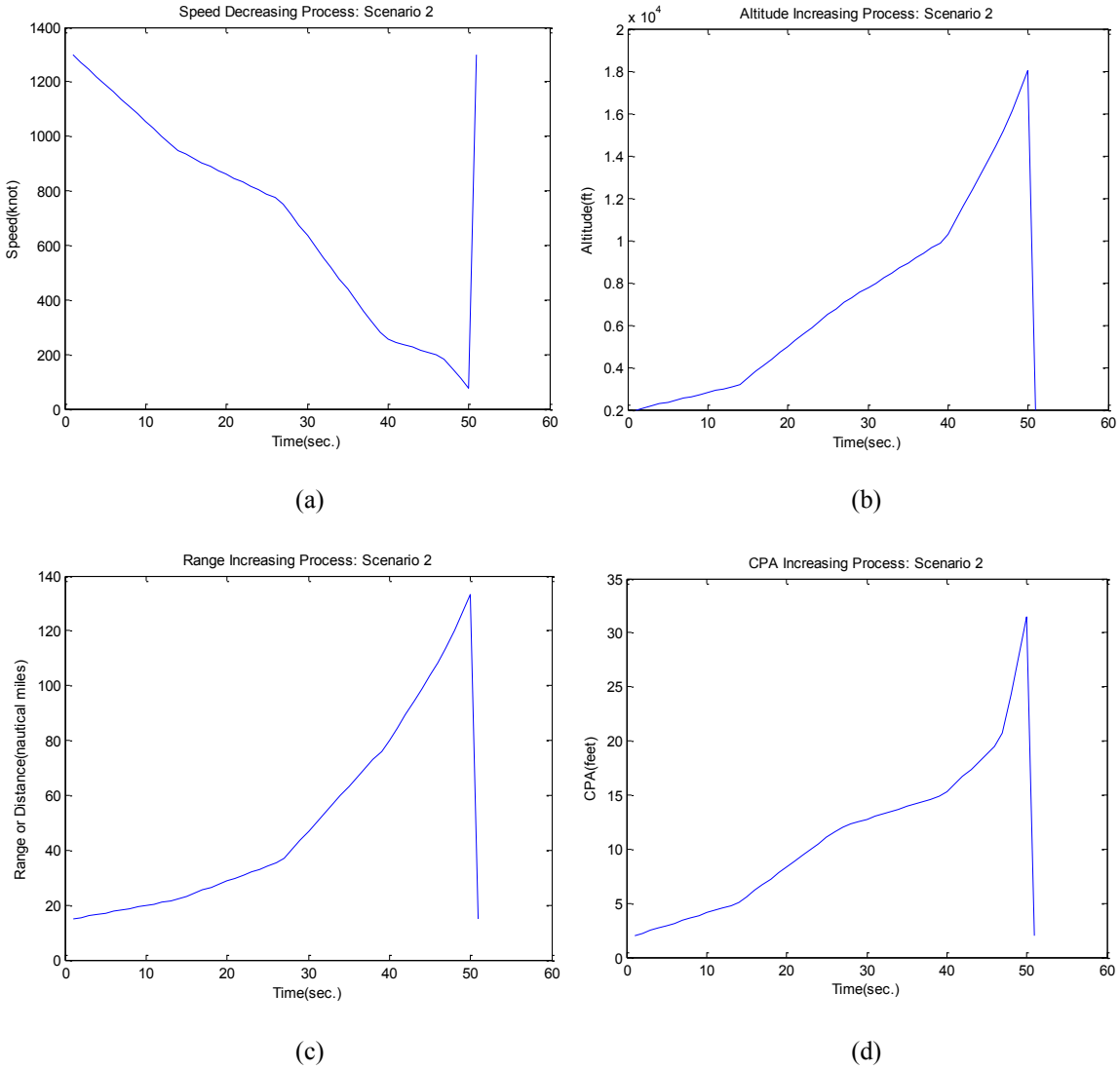


Fig. 15. The time variation of the target: (a) Speed, (b) Altitude, (c) Range, (d) CPA

Fig. 16 shows the output of the fuzzy system threat assessment. By considering the amount of above, threat value decrease significantly because the speed parameter is decreased and three other parameters are increased. The final threat value in the second scenario is got 0.1164. It shows that the threat is very low

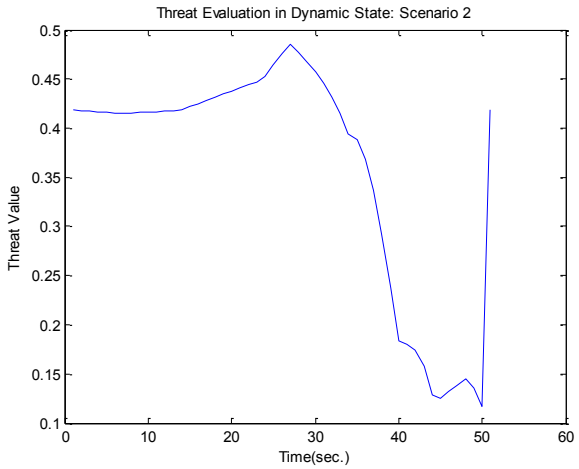


Fig. 16. The output of threat fuzzy model in second scenario

B.3 The Third Scenario

In the third of scenario (Fig. 18) has been assumed that enemy target (Target3) the first be fared and then be closed to defended asset (Asset3). Every one of input parameters is varied as follow. The speed parameter of target with the increasing, decreasing and then increasing variable values is considered to be [250، 600، 764، 600، 890، 1150] knot in six different times. The altitude parameter of target with the increasing and then decreasing variable values is considered to be [3500، 8100، 15000، 12000 ،6000 ،1000] ft in six different times. The range and CPA parameters of target with the increasing and then decreasing variable values respectively are considered to be [15، 82، 166 ،148، 122، 40] nautical miles and [160، 168، 190، 140، 90، 15] feet in six different times. Also, weapon envelope is 250 km, visibility is 5mA, own support is 0, maneuvers and fire is 1 and the rest of the parameters are 0. The projections of used in this scenario and the time variation of each of the four parameters are demonstrated in Fig. 17.

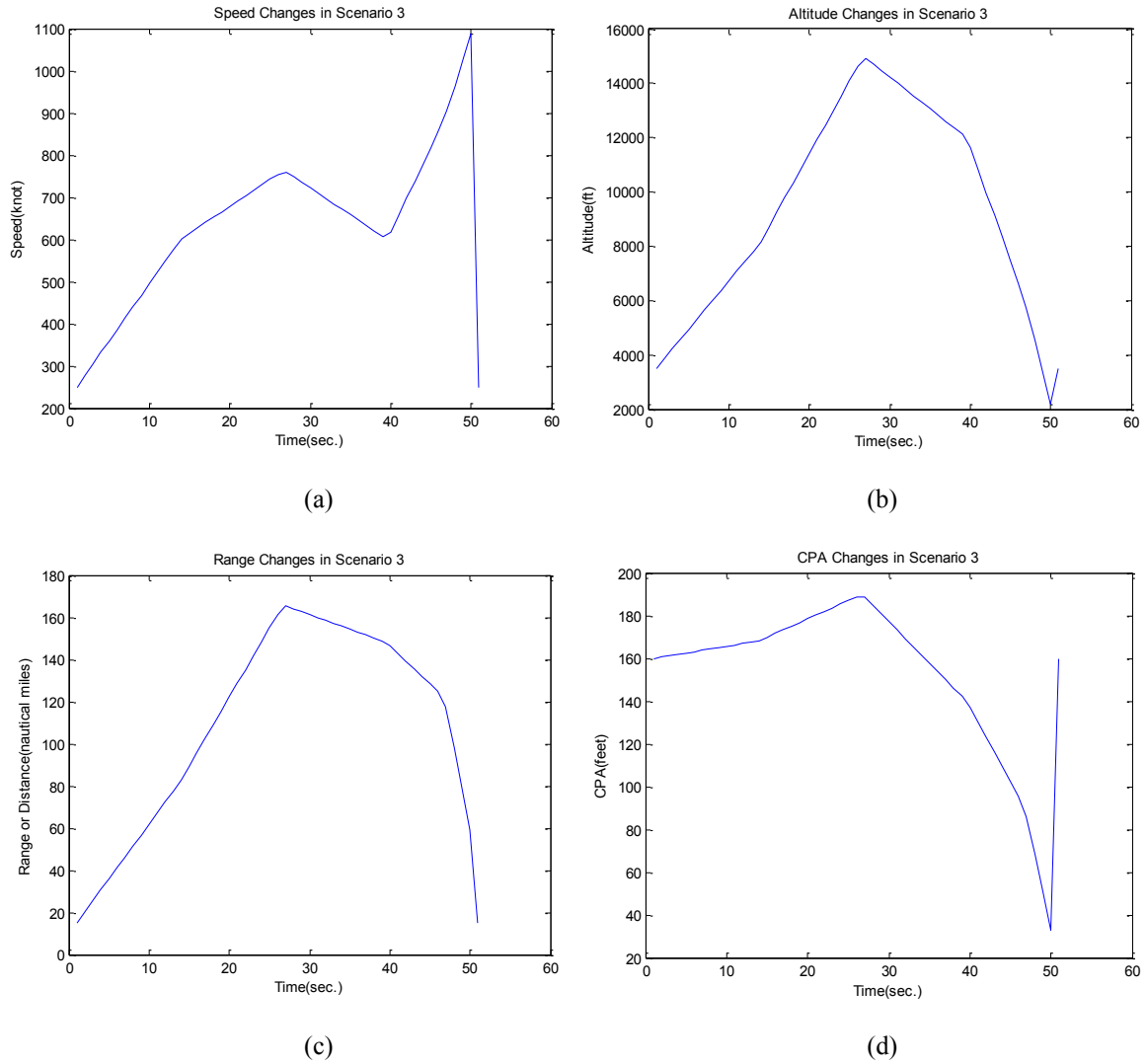


Fig. 17. The time variation of the target: (a) Speed, (b) Altitude, (c) Range, (d) CPA

Fig. 18. Projection of combat environment in the third scenario

Fig. 19 shows the output of the fuzzy system threat assessment. By considering the amount of above, threat value increase significantly because of the speed parameter is increased and then decreased and increased. Also, three other parameters are increased and decreased. The final threat value in the third scenario is got 0.8087. It shows that the threat is very high.

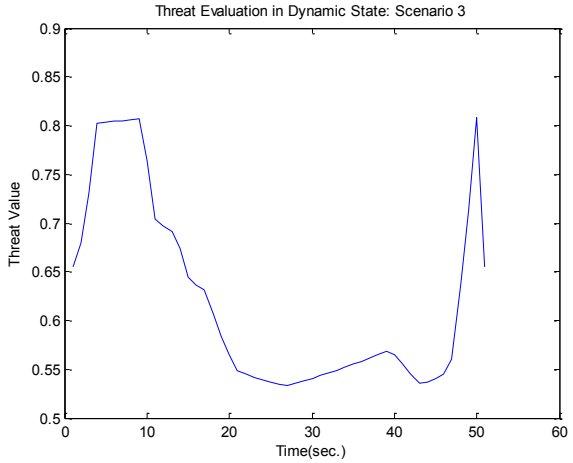
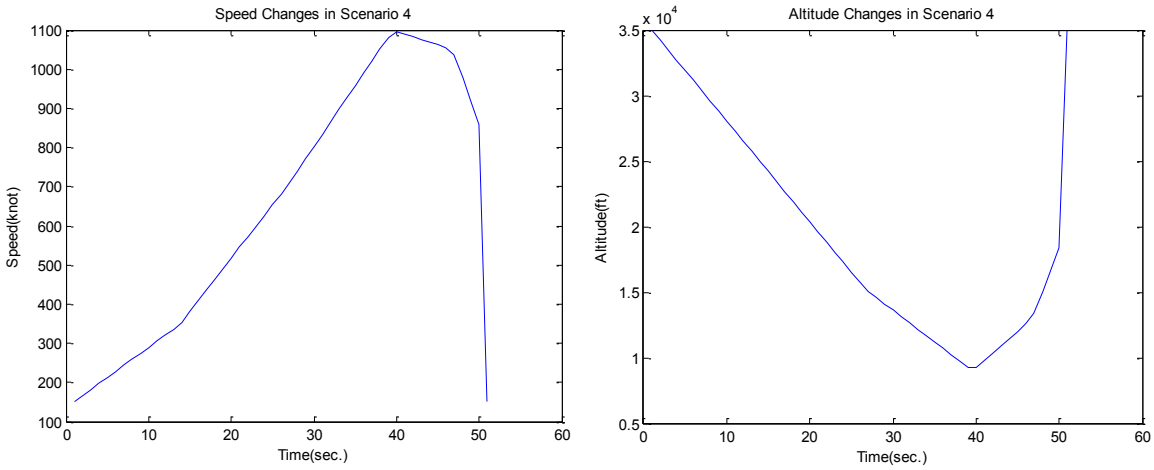


Fig. 19. The output of threat fuzzy model in third scenario

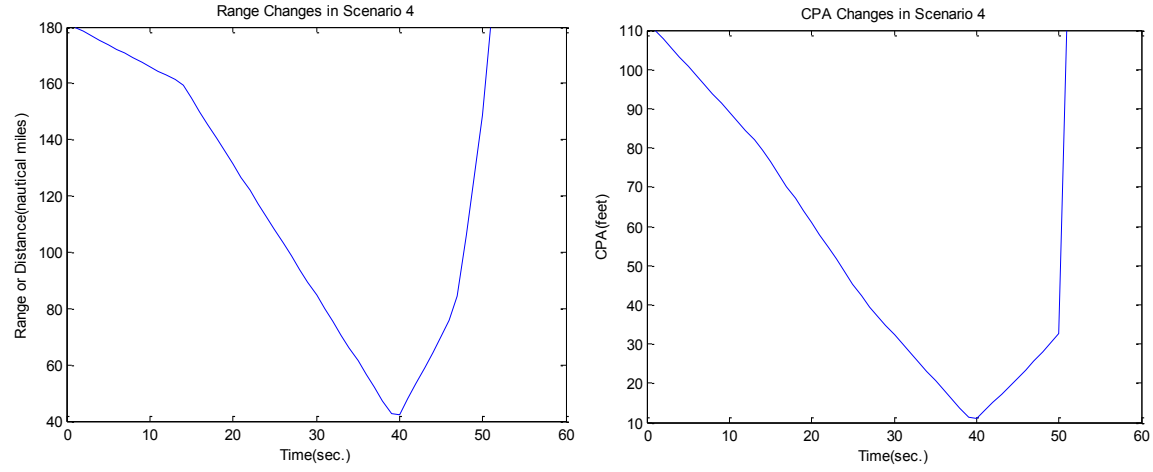
B.4 The Four Scenario

In the four of scenario (Fig. 20) has been assumed that enemy target (Target4) the first be closed and then be fared from the defended asset (Asset4). Every one of input parameters is varied as follow. The speed parameter of target with the increasing and then decreasing variable values is considered to be [150، 350، 700، 1100، 1050، 800] knot in six different times. The altitude parameter of target with the decreasing and then increasing variable values is considered to be [35000، 25100، 15200، 9000 ،13000 ،20000] ft in six different times. The range and CPA parameters of target with the decreasing and then increasing variable values respectively are considered to be [180، 160، 100 ،40، 80، 170] nautical miles and [110، 80، 40، 10، 25، 35] feet in six different times. Also, weapon envelope is 100 km, visibility is 10mA and the rest of the parameters are 1. The projections of used in this scenario and the time variation of each of the four parameters are demonstrated in Fig. 21.

Fig. 20. Projection of combat environment in the fourth scenario



(a) (b)



(c) (d)

Fig. 21. The time variation of the target: (a) Speed, (b) Altitude, (c) Range, (d) CPA

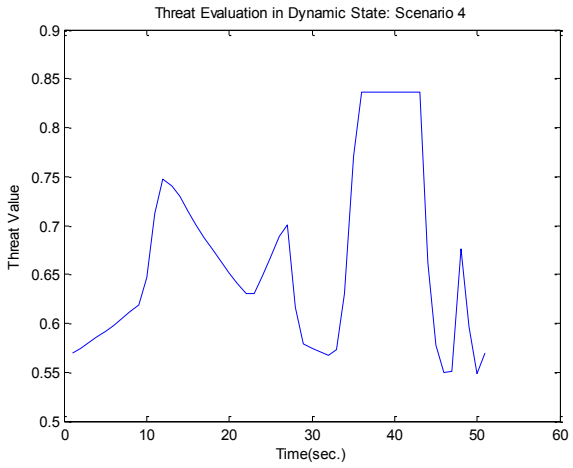


Fig. 22. The output of threat fuzzy model in fourth scenarios

Fig. 22 shows the output of the fuzzy system threat assessment. By considering the amount of above, threat value is averaged because of the speed parameter is increased and then decreased. Also, three other parameters are decreased and increased. The final threat value in the four scenarios is got 0.5483. It shows that the threat is medium. Table 4 is demonstrated the comparison of the results of four real time scenarios.

Table 4. The Final Threat Value in Four Scenarios

scenario	Target Position	Final Threat Value	Output Type
1	Target be closed to Asset	0.8391	Very High
2	Target be fared the Asset	0.1164	Very Low
3	Target be fared and then closed to Asset	0.8087	Very High
4	Target be closed and then fared the Asset	0.5483	Medium

V. Conclusions

The threat evaluation is significant component in target classification process and is significant in military and non military applications. Small errors or mistakes in threat evaluation and target classification especial in military applications can result in huge damage of life and property. Threat evaluation helps in case of weapon assignment, and intelligence sensor support system. It is very important factor to analyze the behavior of enemy tactics as well as our surveillance. Threat evaluation is a process based on defending targets to defended asset so that an assumption is to protect one or multiple assets against several defending targets that will give realistic feel towards threat evaluation. This matter is an open problem in literature and the many researchers are done it yet.

This paper represented a precise description of the threat evaluation process using fuzzy sets theory. A review has been carried out regarding which parameters that have been suggested for threat value calculation. In this paper, we have implemented a system for threat evaluation in an air defense environment by considering of better parameters. For the first time in this paper, eleven parameters are introduced for threat evaluation such as altitude, speed, range, CPA, weapon envelope, own support, visibility, maneuver, fire, target support and IFF as input in fuzzy inference system. This parameters increase the accuracy in designed system. The underlying mechanism for threat evaluation in this system is based on fuzzy logic. The fuzzy logic based multi objective decision making system is an excellent tool available to deploy a decision support system. It simplifies the task of human decision maker to a great deal. Each target has different threat value at different time. In this paper, threat rating of targets is effectively estimated between 0 and 1 by using fuzzy inference system which is giving accurate result. The implemented threat evaluation system has been applied to a synthetic air defense scenario and four real time dynamic air defense scenarios.

The simulation results in table 3 related to static targets are adapted with the results of table 4 related to dynamic targets in different scenarios. The results show the correctness, accuracy, reliability and minimum errors in the system is designed.

The future work includes: 1- updating of target attribute parameters, 2- modeling of surface and under surface targets for determine them threat value and 3- updating of membership functions in input parameters system and designing of a new threat evaluation fuzzy model. Another interesting task is to investigate if the system's calculated threat values on realistic scenarios agree with human experts on air defense. The threat evaluation system can contribute significantly in the process of the improvement of situational awareness in peace and the battlefield scenarios in a network centric operation setup. This will add value to the battle space entity in a network centric platform operations with respect to the automated decision making support.

References

[1] Y. Deng, X. Y. Su, D. Wang, Q. Li, Target Recognition Based on Fuzzy Dempster Data Fusion Method, Defence Science Journal, 2010, 60 (5): 525 – 530.

[2] H. Durrant-Whyte, "Multi Sensor Data Fusion", Australian Centre for Field Robotics the University of Sydney, January 2001.

[3] J. N. Roux, J. H. Van Vuuren, "Threat evaluation and wea-pon assignment decision support: A review of the state of the art, Orion", vol. 23, pp. 151–186, 2007.

[4] J. Roy, S. Paradis, M. Allouche, "Threat evaluation for impact assessment in situation analysis systems", In: Kadar, I. (ed.) Proceedings of SPIE: Signal Processing, Sensor Fusion, and Target Recognition XI, vol. 4729, pp. 329–341, 2002.

[5] S. Kumar, A. M. Dixit, "Threat Evaluation Modelling for Dynamic Targets Using Fuzzy Logic Approach", International Conference on Computer Science and Engineering, 2012.

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

[7] G. A. McIntyre, K. J. Hintz, "A Comprehensive Approach to Sensor Management, Part I: A Survey of Modern Sensor Management Systems", IEEE Transactions on SMC, April 1999.

[8] J. Roy, S. Paradis, M. Allouche, "Threat evaluation for impact assessment in situation analysis systems", in Proceedings of SPIE: Signal Processing, Sensor Fusion, and Target Recognition XI (I. Kadar, ed.), vol. 4729, pp. 329–341, July 2002.

[9] Visibility Sensor Model 6000, "The Standard of Measure-ment", Belfort Instrument Company, USA.

[10] P. Valin, E. Bosse, A. Jouan, "Airborne application of information fusion algorithms to classification", Technical Report TR 2004-282, Defense Research and Development Canada – Valcartier, May 2006.

[11] A. Steinberg, "An approach to threat assessment", in Proceedings of the 8th International Conference on Information Fusion, 2005.

[12] X. Nguyen, "Threat assessment in tactical airborne environ-ments", in Proceedings of the Fifth International Conference on Information Fusion, 2002.

[13] E. L. Waltz, J. Llinas, "Multisensor Data Fusion", Artech House, 1990.

[14] Kehe Wu, Shichao, "An Information Security Threat Assessment Model based on Bayesian Network and OWA Operator", Applied Mathematics & Information Sciences, Vol. 8, No. 2, pp. 833-838, 2014.

[15] Haixin ZHANG, Bingyi KANG, Ya LI, Yajuan ZHANG, Yong DENG, "Target Threat Assessment Based on Interval Data Fusion", Journal of Computational Information Systems 8: 6 2609–2616, 2012.

[16] G. S. Malik, S. K. Das, "A METHOD OF RISK ANALYSIS AND THREAT MANAGEMENT USING ANALYTIC HIERARCHY PROCESS: AN APPLICATION TO AIR DEFENSE", International Symposium of the Analytic Hierarchy Process 2014, Washington, U.S.A, 2014.

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

[18] E. Little, G. Rogova, "An ontological analysis of threat and vulnerability", in Proceedings of the 9th International Conference on Information Fusion, 2006.

[19] S.J. Yang, J. Holsopple, M. Sudit, "Evaluating Threat Assessment for Multi-Stage Cyber Attacks", In Proceedings of the 2006 Military Communications Conference, Washington, DC. Oct. 23-25, 2006.

[20] R. Chinchani, A. Iyer, H.Q. Ngo, S. Upadhyaya, "Towards a theory of insider threat assessment", In Proceedings of the 2005 International Conference on Dependable Systems and Networks, 2005.

[21] F. BOLDERHEIJ, PHD thesis, "Mission Driven", Netherlands Defense Academy and the Centre for Automation of Mission Critical Systems (CAMS), Force Vision, 2007.

[22] F. Johansson, "Evaluating the performance of TEWA Sys-tem", Orebro University, 2010.

[23] F. White, "A Model for Data Fusion", Proceedings 1st National Symposium on Sensor Fusion, 1988.

[24] A. Steinberg, C. Bowman, F. White, "Revisions to the JDL Data Fusion Model", SPIE, Vol. 3719, pp. 430-441, 1999.

[25] L. Klein, "Sensor and Data Fusion Concepts and Applications", SPIE Volume TT14, 1993.

[26] M. Bedworth, J. O'Brien, "The Omnibus Model: A New Model of Data Fusion?", 1999.

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

[28] F. Johansson, G. Falkman, "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.

[29] T. Lampinen, J. Ropponen, T. T. Laitinen, "Joint Threat Assessment with Asset Profiling and Entity Bayes Net", In Proceeding of the 12th International Conference on Information Fusion, Seattle, WA, USA, 2009.

[30] Y. Liang, "A fuzzy knowledge based system in situation and threat assessment", Journal of Systems Science & Information, 4, 791–802, 2006.

[31] M. Liebhaber, B. Feher, "Air threat assessment: Research, model, and display guidelines", in Proceedings of the Command and Control Research and Technology Symposium, 2002.

[32] Y. Liang, "An approximate reasoning model for situation and threat assessment", in Proceedings of the 4th International Conference on Fuzzy Systems and Knowledge Discovery, 2007.

[33] X. Nguyen, "Threat assessment in tactical airborne environ-ments", in Proceedings of the Fifth International Conference on Information Fusion, 2002.

[34] T. J. Ross, "Fuzzy Logic with Engineering Applications", Second Edition, John Wiley and Sons, 628.

[35] M. Oxenham, "Enhancing situation awareness for air defence via automated threat analysis", in Proceedings of the Sixth International Conference on Information Fusion, vol. 2, pp. 1086–1093, 2003.

[36] M. Liebhaber, B. Feher, "Air threat assessment: Research, model, and display guidelines", in Proceedings of the 2002 Command and Control Research and Technology Symposium, 2002.

[37] Chen Dongfenga, Feng Yua, Liu Yongxuea, "Threat Assessment for Air Defense Operations Based on Intuitionistic Fuzzy Logic", International Workshop on Information and Electronics Engineering (IWIEE), 2012, pp. 3302-3306.

[38] A. Berrached M. Beheshti A. de Korvin R. Aló, "Applying Fuzzy Relation Equations to Threat Analysis", Proceedings of the 35th Hawaii International Conference on System Sciences – 2002.

[39] Athar Kharal, "Predicting Suicide Attacks: A Fuzzy Soft Set Approach", 2010.

[40] S.H Nasaruddin, Lily Marlia Abdul Latif, "Information System Risk Analysis Using Fuzzy Techniques", International Symposium on Mathematical Sciences and Computing Research 2013 (iSMSC 2013) 6-7 December 2013, Perak, MALAYSIA.

[41] Rahul Choudhary, Abhishek Raghuvanshi, "Fuzzy Based Evaluation Model of a Systems Security", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, No. 9, September 2012, pp. 413-416.