A new model for threat assessment in data fusion based on fuzzy evidence theory

Ehsan Azimirad\textsuperscript{a1,*}, Javad Haddadnia\textsuperscript{b2}

\textsuperscript{a} Assistant Professor, Eqbal Lahoori Institute of Higher Education, Mashhad, Iran
\textsuperscript{b} Associate Professor, Electrical and Computer Engineering Department, Hakim Sabzevari University, Sabzevar, Iran
\textsuperscript{1}azimi@eqbal.ac.ir; \textsuperscript{2}haddadnia@hsu.ac.ir; \textsuperscript{*} corresponding author

ARTICLE INFO

Article history:
Received May 1, 2016
Revised June 5, 2016
Accepted June 6, 2016

Keywords:
Threat Assessment
Fuzzy Evidence Theory
Evidence Theory
Imperfect Information
Uncertainty Measures

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]. 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.

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 [2]. Threat evaluation is a high-level information fusion process that in relation to the JDL model of data fusion [5] belongs to level 3 [1], [2], [4], 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. At times the threat evaluation becomes challenging in the presence of multiple parameters and processes. There is some amount of uncertainty involved in this information that depending on the nature of targets and assets involved. It is difficult to formulate mathematical model by using selected information as inputs to generate the threat value as an output. Klir and Wierman (1999) defined three types of uncertainty of information [6]:

- Fuzziness: resulting from the imprecise boundaries of fuzzy sets.
- Nonspecificity: associated with the sizes or cardinalities of various sets of alternatives.
Discord: which describes conflicts among the sets of alternatives.

Since the information provided is always imperfect and several kinds of imperfection may be encountered (imprecision, uncertainty, incompleteness, vagueness, etc.), several theories have been developed to deal with this variety of imperfect information. Each theory aims to model real situations more accurately. Many theories have been developed to deal with uncertainty that consisting of [7]: (1) Probability theory, (2) Evidence theory, (3) Fuzzy sets theory, (4) Possibility theory, (5) Rough sets theory and (6) Random sets theory. One difficult aspect of modeling information in these theories is quantifying the confidence levels that someone has for the events considered [7].

As seen above, each of the theories is well suited to one particular kind of imperfect information. In practice, complex situations involve the processing of several pieces of information, each exhibiting one or more types of imperfection. In this paper has been represented a new theory for modeling of types of imperfection information which is important in calculating the amount of threat.

The remainder of this paper is organized as follows. In section 2, a precise description of the fuzzy evidence theory is presented. In section 3 the proposed method is presented. In section 4, simulation and results are presented. Finally, in section 5 the paper is concluded and thoughts regarding future work are presented.

II. Fuzzy Evidence Theory

As seen in introduction section, in complex situations particular military problems for example threat assessment; must designed a new method for data fusion under uncertainty. This method is gotten as fusion of theories. Fusion between the different theories is sometimes necessary; but they should be performed with care to minimize information loss. Therefore, no single theory can deal alone with these complex situations.

Fuzzy Evidence Theory (FET) is a theoretical framework for representing uncertain information allowing capturing all three types of uncertainty. FET is based on two basic theories: Dempster-Shafer theory and fuzzy set theory [6].

A. Evidence Theory

Dempster-Shafer theory (Dempster, 1968; Shafer, 1976), or evidence theory, is based on the concept of evidence, which represents all available information about the state of a certain system in terms of a collection of crisp sets and beliefs associated with them [6]. Evidence theory is often presented as a generalization of probability theory. As such, unlike probability theory, it is able to represent both imprecision and uncertainty.

Let us assume that we are concerned with the value of a certain quantity \( x \) and the set of all possible values is \( X \) (i.e., \( X \) is the frame of discernment).

A proposition specifies that \( x \in A \subseteq X \). In other words, a proposition is a piece of information about \( x \) in the form “the value of \( x \) is in \( A \)” for some \( A \subseteq X \). In the DST, the uncertainty over propositions is reflected by the function called basic probability assignment (BPA) or mass function that is stated in (1).

\[
m: P(X) \rightarrow [0,1]
\]  
(1)

Where \( P(X) \) denotes the power set of \( X \), and the following two properties hold (2).

\[
\begin{align*}
    m_{x}(\phi) &= 0 \\
    \sum_{A \subseteq X} m_{x}(A) &= 1
\end{align*}
\]  
(2)

Given several propositions about \( x \), BPA reflects our uncertainty over them. In other words, \( m(A) \) represents the belief exactly committed to \( A \) that is the exact evidence that the value of \( x \) is in \( A \). If for a certain \( A \) \( m(A) > 0 \) then \( A \) is called a focal element [6].

The totality of focal elements and the associated BPA define a body of evidence. More formally, a
body of evidence is the following collection: \( \{ A_i, m_x(A_i) \}_{i=1}^n \) such that \( A \subseteq X \), \( m(A) > 0 \) and \( m \) is a BPA. The definition of the basic probability assignment form one of the major cores of the DST [6]. DST is a theory of uncertainty. More precisely, in the framework of this theory it is possible to represent and measure two types of uncertainty: nonspecificity and discord [7].

**B. Fuzzy Sets Theory**

A fuzzy set [8]-[11] is a collection of homogeneous elements whose members have a degree of membership. In the classical set theory (also known as crisp set theory, or, simply, set theory), an element \( x \in X \) can either be a member of a certain set \( A \subseteq X \) or not be a member of this set. Here, \( X \) is the universe of all elements, which the set \( A \) is part of. The concept of fuzzy set, in turn, assumes that \( x \) can be a member of a fuzzy set \( \tilde{A} \) with a certain grade of membership \( \mu_\tilde{A}(x) \).

This grade of membership is defined by the membership function \( \mu(x): X \rightarrow [0,1] \). Thus, the quantity \( \mu(x) \) defines the grade of membership of the element \( x \) in the fuzzy set \( \tilde{A} \). A classical set \( A \) can be seen as a special form of a fuzzy set whose membership function is Boolean, i.e. \( \mu(x): X \rightarrow \{0,1\} \).

The support of a fuzzy set \( \tilde{A} \) is the crisp set that contains all such points \( x \in X \) for which \( \mu(x) > 0 \). For every \( \alpha \in [0,1] \), a given fuzzy set \( \tilde{A} \) yields a crisp set \( \tilde{A} = \{ x \in X : \mu(x) \geq \alpha \} \), which we call \( \alpha \)-cuts (\( \tilde{A}_\alpha \)). Triangular fuzzy number \( A = [a, b, c] \) can be represented in (3).

\[
\mu(x) = \begin{cases} 
\frac{x-a}{b-a}, & a \leq x \leq b \\
\frac{c-x}{c-b}, & b \leq x \leq c 
\end{cases}
\]  

(3)

The \( \alpha \)-cuts for this fuzzy number are (4).

\[
\alpha - \text{cut}(\tilde{A}) = [a + \alpha(b-a), c - \alpha(c-b)]
\]  

(4)

Fuzzy evidence theory combines the concepts of the DST with fuzzy sets in order to reflect all three types of uncertainty within one framework.

**C. Combination Rule in FET**

In the DST, in order to combine two pieces of information, represented in the form of two different bodies of evidence, the following equation can be used. Let \( m(A) \) and \( m(B) \) be BPAs of two bodies of evidence and let \( m(C) \) denote the BPA of the combined body of evidence. Then \( m(C) \) is defined as (5).

\[
m(C) = \sum_{\tilde{A}, \tilde{B} \subseteq C} \frac{m_\tilde{A}(A)m_\tilde{B}(B)}{1 - \sum_{\tilde{A}, \tilde{B} \subseteq C} m_\tilde{A}(A)m_\tilde{B}(B)}
\]

(5)

The above equation is called Dempster’s rule of combination, and it is the most usual way to combine multiple bodies of evidence into one aggregate body of evidence. This rule is used for fuzzy sets \( \tilde{A} \) and \( \tilde{B} \) defined as (6).

\[
m(\tilde{C}) = \sum_{\tilde{A}, \tilde{B} \subseteq C} \frac{m_\tilde{A}(A)m_\tilde{B}(B)}{1 - \sum_{\tilde{A}, \tilde{B} \subseteq C} m_\tilde{A}(A)m_\tilde{B}(B)}
\]

(6)

**D. Uncertainty Measures in FET**

The quality of an additional piece of information about \( x \) can be measured in terms of the uncertainty decrease this piece of information provides. To do that, a certain uncertainty measure has to be defined. A first uncertainty measure recently proposed in the framework of the fuzzy evidence theory is called General Uncertainty Measure [6]. Given a fuzzy body of evidence \( FBoE = \{ \tilde{A}, \mu_\tilde{A}(x), m(\tilde{A}) \} \), the General Uncertainty Measure (GM) associated with it is
defined as in (7).

\[
GM (FBoE) = - \sum_{x \in X} \left[ BetP(x) \log_2 \frac{BetP(x)}{\overline{BetP}(x)} + BetP(x) \log_2 \overline{BetP}(x) \right]
\]  

(7)

Where

\[
BetP(x) = \sum_{i=1}^{n} m_x (\tilde{A}_i) \mu_x (x)
\]

(8)

\[
\overline{BetP}(x) = \sum_{i=1}^{n} m_x (\tilde{A}_i) (1 - \mu_x (x))
\]

(9)

An alternative uncertainty measure for the fuzzy evidence theory is called Hybrid Entropy and was proposed by its authors as an “information measure which quantifies the overall uncertainty contained in a fuzzy evidence structure”. Hybrid Entropy is defined as in (10) [6].

\[
FH (FBoE) = - \sum_{i=1}^{n} m_x (\tilde{A}_i) \log_2 (m_x (\tilde{A}_i) (1 - F(\tilde{A}_i)))
\]

(10)

With

\[
F(\tilde{A}) = \frac{1}{|S_{\tilde{A}}|} \sum_{\tilde{A}_j \in S_{\tilde{A}}} \mu_{\tilde{A}(\tilde{A}_j)} (x)
\]

(11)

According to [12] the two above metrics reflect all three types of uncertainty.

### III. Proposed Method

The threats of different attributes are from different sensors. In this proposed method, the targets different attributes that are to membership function are firstly transformed into fuzzy numbers. Then the \(\alpha\)-cuts and focal elements of them are earned. Next, the focal elements are transformed to BPAs and then combined into a comprehensive BPA by the Dempster combination rule. Finally the comprehensive BPAs are ranked based on TOPSIS at last. In order to confirm the proposed model we calculated the maximum behavior of the two aggregate uncertainty measures, GM (7) and FH (10). The proposed method has been stated in following steps:

#### Step 1: The Determination of Target Attributes

The variety of parameters are proposed and used by researchers for threat evaluation in [13]-[20]. A number of parameters that are used in this paper are discussed in Table 1.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed</td>
<td>Approximate airspeed or an indication Of change</td>
</tr>
<tr>
<td>Altitude</td>
<td>Approximate feet above ground.</td>
</tr>
<tr>
<td>Range</td>
<td>The track’s distance from own ship.</td>
</tr>
<tr>
<td>CPA</td>
<td>Closest Point of Approach (CPA) Estimated distance.</td>
</tr>
<tr>
<td>Weapon envelope</td>
<td>The track’s position with respect to its Estimated weapons envelope.</td>
</tr>
<tr>
<td>Own Support</td>
<td>Availability of nearby friendly ships Or patrol aircraft.</td>
</tr>
<tr>
<td>Visibility</td>
<td>An indication of atmospheric conditions.</td>
</tr>
<tr>
<td>Maneuvers</td>
<td>Indicates the number of recent maneuvers.</td>
</tr>
<tr>
<td>Fire</td>
<td>The Target Fire into Asset</td>
</tr>
<tr>
<td>IFF Mode</td>
<td>Identify Friend or Foe or Perhaps neutral.</td>
</tr>
<tr>
<td>Target Support</td>
<td>Availability targets for assistance to enemy target</td>
</tr>
</tbody>
</table>

According to [12] the two above metrics reflect all three types of uncertainty.

Fig. 1 illustrated the general process of this model based on fuzzy evidence theory.
Step 2: The Determination of Membership Functions

In this paper one kind of rule-based algorithm based on fuzzy evidence theory is suggested. In this step, the membership functions of fuzzy inference system are proposed related to input and output parameters. Membership functions of parameters are triangular and singleton. These functions are demonstrated in Fig. 2 and Fig. 3.

Fig. 2. Membership functions for triangular input parameters: (a) Speed, (b) Altitude, (c) Range, (d) CPA, (e) weapon envelope, (f) visibility
Fig. 3. Membership functions for singleton input parameters: (a) own support, (b) maneuvers, (c) fire, (d) target support, (e) IFF

The output parameter in fuzzy model is threat rating that is between 0 and 1. It demonstrated in Fig. 4.

**Step 3: The Determination of BPA**

In this step we calculated fuzzy numbers in (3) and $\alpha$-cuts (or focal elements) in (4) and produced BPA related to membership functions of input parameters. Next, we calculated comprehensive BPAs that got in (6). The BPAs related to membership functions of input parameters are produced as (12) [21].

$$m(A_i) = \frac{\int_{\bar{A}_i,\text{lower}}^{\bar{A}_i,\text{upper}} \mu_A(x)dx}{\sum_{i}^{\bar{A}_i,\text{upper}} \int_{\bar{A}_i,\text{lower}}^{\bar{A}_i,\text{upper}} \mu_A(x)dx} \quad (12)$$

Where $A_{\text{lower}}$ and $A_{\text{upper}}$ are lower and upper bounds in (4).

**Step 4: The Classification of Targets**

In this step we used on TOPSIS algorithm for ranking between targets. The TOPSIS stands for technique for preference by similarity to the ideal Solution [22]-[24]. TOPSIS is attractive in that.
limited subjective input is needed from decision makers. The only subjective input needed is weights [22]. TOPSIS is based on the concept that the chosen alternative should have the shortest distance from the positive ideal solution and the longest distance from the negative ideal solution. The output of algorithm that is result of proposed model determined threatens targets and nonthreatening targets. The idea of TOPSIS can be expressed in a series of stages [22].

1. **Determine the decision matrix.** This matrix has m row and n column. M is alternatives number and n is attributes number.

2. **Construct the normalized decision matrix.** This step transforms various attribute dimensions into non-dimensional attributes. This stage is done as in (13).

\[
r_{ij} = \frac{x_{ij}}{\left(\sum_{r=1}^{m} (x_{rj})^2\right)^{1/2}}
\]

3. **Determine ideal and negative-ideal solutions** as \(V^*_i\) and \(V'_i\).

4. **Calculate the separation measures.** Ideal separation and negative Ideal are gotten in this stage as in (14) and (15).

\[
S_{ij} = \left[\sum_{j=1}^{n} (V_{ij}^* - V_{ij})^2\right]^{1/2}, i = 1, 2, ..., m
\]

\[
S'_{ij} = \left[\sum_{j=1}^{n} (V'_{ij} - V_{ij})^2\right]^{1/2}, i = 1, 2, ..., m
\]

5. **Calculate the relative closeness to the ideal solution.** This stage is gotten as in (16).

\[
C_{ij} = \frac{S_{ij}'}{S_{ij}^* + S_{ij}'}, 0 < C_{ij} < 1
\]

6. **Rank order alternatives** by maximizing the ratio \(C_{ij}^*\).

**Step 5: The Calculation of Uncertainty**

In this step we first studied the maximum behavior of the two aggregate uncertainty measures, GM (7) and FH (10) and calculated the value of them in any input parameters only and total parameters (total uncertainty).

For validate of new proposed model, we compared the uncertainty values in fuzzy evidence theory and fuzzy sets theory. The uncertainty measures in fuzzy sets theory are \(U\)-uncertainty (17) and fuzziness (18). These measures are shown as in (17) and (18) [6].

\[
U(A) = \frac{1}{h(A)} \int_{0}^{h(A)} \log_2 \left[1 + \mu^u(A)\right] d\alpha
\]

\[
f(A) = \int_{a}^{b} \left(1 - \frac{x - a}{b - a}\right) dx + \int_{b}^{e} \left(1 - \frac{x - e}{b - c}\right) dx
\]

IV. **Simulation and Results**

In this section we stated the results of simulation for fuzzy sets theory and fuzzy evidence theory. These theories are not enough used in military applications in literatures. For this reason, there is no case study for comparing of results. Therefore, we compared the accuracy and reliability of proposed method by the results of them simulation. For start simulation we defined four scenarios in Fig. 5.
Fig. 5. The scenarios related to dynamic targets in combat environment

In Fig. 6 and Fig. 7, the output of fuzzy model and the result of uncertainty measures in it are shown for the all of scenarios.
In Table 2, the output of proposed method is shown. Also, in Fig. 8 the result of uncertainty measures are shown.

Table 2. the target threat ranking in proposed method

<table>
<thead>
<tr>
<th>Target Number</th>
<th>( C_i^* = S_i^<em>/(S_i^</em> + S_i') )</th>
<th>( S_i' )</th>
<th>( S_i^* )</th>
<th>( C_i^* )</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>( T_1 )</td>
<td></td>
<td>0.0152</td>
<td>0.0158</td>
<td>0.4903</td>
<td>3</td>
</tr>
<tr>
<td>( T_2 )</td>
<td></td>
<td>0.0259</td>
<td>0.0067</td>
<td>0.7944</td>
<td>1</td>
</tr>
<tr>
<td>( T_3 )</td>
<td></td>
<td>0.0129</td>
<td>0.0148</td>
<td>0.4657</td>
<td>4</td>
</tr>
<tr>
<td>( T_4 )</td>
<td></td>
<td>0.0137</td>
<td>0.0128</td>
<td>0.5170</td>
<td>2</td>
</tr>
</tbody>
</table>

According to the results, the larger the similarity the higher the threat is, so the target threat order is \( T_2 > T_4 > T_1 > T_3 \), the threat of \( T_1 \) is the highest while that of \( T_4 \) is the lowest.

Fig. 8. The uncertainty value in fuzzy dempster-shafer theory

Now, for comparing of the two theories, we assumed the results of this paper compared to the results of paper [20].

Table 3. Comparison between two theories for threat ranking

<table>
<thead>
<tr>
<th>Target Number</th>
<th>Fuzzy Sets Theory</th>
<th>Fuzzy Evidence Theory</th>
<th>Target Ranking (Fuzzy Set Theory)</th>
<th>Target Ranking (Fuzzy Evidence Theory)</th>
</tr>
</thead>
<tbody>
<tr>
<td>( T_1 )</td>
<td>0.5505</td>
<td>0.4903</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>( T_2 )</td>
<td>0.6100</td>
<td>0.7944</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( T_3 )</td>
<td>0.5698</td>
<td>0.4657</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>( T_4 )</td>
<td>0.5462</td>
<td>0.5170</td>
<td>4</td>
<td>2</td>
</tr>
</tbody>
</table>
According to the results of Table 3, the threat of $T_1$ is the highest. This means that the both of theories are fine for distinguish the greatest threat targets ranking. In Table 4, we compared the efficiency both of theories based on their uncertainty measures. We also stated the percentage improvement any uncertainty measures.

Table 4. The comparison of total uncertainty in two theories

<table>
<thead>
<tr>
<th>Uncertainty Models</th>
<th>Methods</th>
<th>Total Uncertainty</th>
<th>The Best Uncertainty</th>
<th>The Percentage Improvement of Uncertainty in Proposed Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model Based on Fuzzy Sets Theory</td>
<td>Fuzziness (F)</td>
<td>37935.3</td>
<td>111.41</td>
<td>%98.01</td>
</tr>
<tr>
<td></td>
<td>Non Specificity (U)</td>
<td>111.41</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Model Based on Fuzzy Evidence Theory</td>
<td>General Uncertainty (GM)</td>
<td>2.217</td>
<td>2.217</td>
<td></td>
</tr>
<tr>
<td>(Proposed)</td>
<td>Fuzzy Entropy (FH)</td>
<td>9.35</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

According to the results of Table 4, we can result that total uncertainty in fuzzy evidence theory (proposed method) is the better than total uncertainty in fuzzy sets theory. Also, the percentage improvement of uncertainty in proposed model based on fuzzy evidence theory is 98.01% that is the better than fuzzy sets theory.

V. Conclusions

Evidence theory models uncertain and imprecise information. Vague information cannot be modeled in probability theory or evidence theory. Fuzzy sets theory is the appropriate framework for this kind of information. Therefore the fusion of two theories can be effective for modeling of imperfect information.

In this paper, a new method of target threat assessment using of Fuzzy evidence theory (FET) theory and TOPSIS is proposed. FET solved two key problems; one is how it allowing capturing all three types of uncertainty in information and the other is how to rank the threat level of all targets. FET combines the concepts of the DST with fuzzy sets in order to reflect all three types of uncertainty within one framework. The new proposed method applied to a designing of real time scenario to air threat assessment, the result in Table 3 and Table 5 shows that this method is reasonable, effective, accuracy and reliability.

The future work can be done in updating of targets attributes and the better of membership functions, improvement and decreasing of uncertainty information and uncertainty model, representation of an intelligent algorithm for determining of TOPSIS weights and implementation FET for target threat assessment in surface and under surface applications.

References

Ehsan Azimirad and Javad Haddadnia (A New Model for Threat Assessment by Fuzzy Evidence Theory)


