Evaluating E-Commerce System Security Using Fuzzy Multi-Criterion Decision-Making

Wen Jiang, Zhenjian Li, Jia Jia

School of Electronics and Information,
Northwestern Polytechnical University,
Xi'an, China
jiangwen@nwpu.edu.cn

Dianting Liu

Department of Electrical and Computer Engineering
University of Miami,
Coral Gables, FL 33124, USA
d.liu4@umiami.edu

Abstract—In the development of E-Commerce, security has always been the core and key issue. To aim at the assessment of E-Commerce security, in order to efficiently handle uncertain information in the process of decision making, a new fuzzy multi-criteria decision-making (MCDM) method is presented based on fuzzy sets theory (FST) and Dempster-Shafer evidence theory (DST). First, a hierarchical structure of E-Commerce security is established. Second, the ratings of the third level criteria and the importance weights of the first level criteria, given by the experts, are expressed in trapezoidal (or triangular) fuzzy numbers. The ratings can be transformed into basic probability assignments (BPA) based on an improved similarity measure of generalized fuzzy numbers we proposed, combining the BPAs from bottom to top using Dempster's combination rule. At last, the importance weights can be transformed into discounting coefficients and the BPAs of the first level criteria can be fused using the discounting rule to obtain the final assessment decision. An illustrative example is given to show that the proposed method can be applied to the security evaluation for the complex E-Commerce system and provides the scientific and consensus evaluated results as well.

Keywords—E-Commerce security; Dempster-Shafer evidence theory; fuzzy sets theory; multi-criteria decision-making

I. INTRODUCTION

With the rapid development of information technology and communication technology, E-Commerce as a new economic and industrial model makes all round impact on social and economic aspects. But because of the virtuality of E-Commerce and the openness of the Internet, security issues are emerging and have become the bottleneck of E-Commerce development [1].

Due to the driving of application, many measures and methods have been proposed to improve the security of E-Commerce system [2-4]. However, because of the limitations of security technology at present and the complexity of security issues, it is very difficult to build an absolutely secure E-Commerce system. Therefore, it is very necessary to assess the security of an E-Commerce system [5,6], which can help the E-Commerce enterprise to build security policy, to implement safe management, and to provide some valuable reference for the development and use of E-Commerce system.

However, with the development of E-Commerce systems, they have more function, and their structure becomes more

complex. Safety evaluation system becomes a multi-level, multi-criterion, integrated process and becomes more complicated. Fusion is an interesting solution to obtain more relevant information, and Dempster's combination rule can be used to aggregate individual preferences into a collective preference in the group aggregation. Furthermore, in the practical evaluation process, the evaluation object is affected by various uncertain criteria, in which the fuzziness is the main. Hence, it is reasonable to assess E-Commerce system security in FST and DST.

II. PRELIMINARIES

A. Fuzzy sets theory

1) The basic concepts of fuzzy numbers [7]

Definition 2.1 (Fuzzy set). Let X be a universe of discourse, $\tilde{A}$ is a fuzzy subset of X if for all $x \in X$, there is a number $\mu_{\tilde{A}}(x) \in [0,1]$ assigned to represent the membership of x to $\tilde{A}$, and $\mu_{\tilde{A}}(x)$ is called the membership of $\tilde{A}$.

Definition 2.2 (Generalized trapezoidal fuzzy number) A generalized trapezoidal fuzzy number can be defined as $\tilde{A} = (a_1, a_2, a_3, a_4; w)$, where $a_1 \leq a_2 \leq a_3 \leq a_4$, $0 \leq w \leq 1$, and the membership function is defined by

$$\mu_{\tilde{A}}(x) = \begin{cases} 0 & x < a_1 \\ \frac{x-a_1}{a_2-a_1} & a_1 \leq x \leq a_2 \\ w & a_2 \leq x \leq a_3 \\ \frac{x-a_3}{a_4-a_3} & a_3 \leq x \leq a_4 \\ 0 & x > a_4 \end{cases} \quad (1)$$

If $a_2 = a_3$, then $\tilde{A}$ is a triangular fuzzy number. If $a_1 = a_2 = a_3 = a_4$, then $\tilde{A}$ is a crisp value.

2) Linguistic variable

The concept of linguistic variable is very useful in dealing with situations that are too complex or ill-defined to be reasonably described in conventional quantitative expressions.

In this paper, the importance and the ratings of the criteria are considered as linguistic variables. Due to the uncertainty, we prefer to express these linguistic variables in trapezoidal (or triangular) fuzzy numbers. Table I. shows the linguistic variables of the ratings of criteria. Table II shows the linguistic variables of the importance.

TABLE I. LINGUISTIC VARIABLES OF THE RATINGS

Very poor (VP)	(0,0,1,2)
Poor (P)	(1,2,2,3)
Medium poor (MP)	(2,3,4,5)
Fair (F)	(4,5,5,6)
Medium good (MG)	(5,6,7,8)
Good (G)	(7,8,8,9)
Very good (VG)	(8,9,10,10)

TABLE II. LINGUISTIC VARIABLES OF THE IMPORTANCE WEIGHT

Very low (VL)	(0,0,0.1,0.2)
Low (L)	(0.1,0.2,0.2,0.3)
Medium low (ML)	(0.2,0.3,0.4,0.5)
Medium (M)	(0.4,0.5,0.5,0.6)
Medium high (MH)	(0.5,0.6,0.7,0.8)
High (H)	(0.7,0.8,0.8,0.9)
Very high (VH)	(0.8,0.9,1,1)

3) Arithmetic operations

Assume that $\tilde{A}$ and $\tilde{B}$ are two generalized trapezoidal fuzzy numbers where $\tilde{A} = (a_1, a_2, a_3, a_4; w_{\tilde{A}})$ and $\tilde{B} = (b_1, b_2, b_3, b_4; w_{\tilde{B}})$. Some arithmetic operations between $\tilde{A}$ and $\tilde{B}$ are shown as follows [10]:

Generalized trapezoidal fuzzy numbers addition $\oplus$:

$$\begin{aligned} \tilde{A} \oplus \tilde{B} &= (a_1, a_2, a_3, a_4; w_{\tilde{A}}) \oplus (b_1, b_2, b_3, b_4; w_{\tilde{B}}) \\ &= (a_1 + b_1, a_2 + b_2, a_3 + b_3, a_4 + b_4; \min(w_{\tilde{A}}, w_{\tilde{B}})) \end{aligned} \quad (2)$$

Generalized trapezoidal fuzzy number multiplied by the real number $\times$:

$$\begin{aligned} m \times \tilde{A} &= m \times (a_1, a_2, a_3, a_4; w_{\tilde{A}}) \\ &= (m \times a_1, m \times a_2, m \times a_3, m \times a_4; w_{\tilde{A}}) \end{aligned} \quad (3)$$

4) Defuzzification

Defuzzification is an important step in fuzzy modeling and fuzzy multi-criteria decision-making. The defuzzification converts the fuzzy value into a crisp value, and determines the ordinal positions of n-fuzzy input parameters vector.

Definition 2.3 For a trapezoidal fuzzy number $\tilde{A} = (a_1, a_2, a_3, a_4)$, its defuzzification value [11] is defined as

$$c = (a_1 + a_2 + a_3 + a_4) / 4. \quad (4)$$

5) Similarity measure of generalized fuzzy numbers

We proposed an improved similarity measure of generalized in [15]. Assume fuzzy numbers

$\tilde{A} = (a_1, a_2, a_3, a_4; w_{\tilde{A}})$ and $\tilde{B} = (b_1, b_2, b_3, b_4; w_{\tilde{B}})$, $0 \leq a_1 \leq a_2 \leq a_3 \leq a_4 \leq 1$ and $0 \leq b_1 \leq b_2 \leq b_3 \leq b_4 \leq 1$. Then the degree of similarity $S(\tilde{A}, \tilde{B})$ between the generalized trapezoidal fuzzy numbers $\tilde{A}$ and $\tilde{B}$ is calculated as follows:

$$\begin{aligned} S(\tilde{A}, \tilde{B}) &= \left[1 - \left| x_{\tilde{A}}^* - x_{\tilde{B}}^* \right| \right] \times \left[1 - \left| w_{\tilde{A}} - w_{\tilde{B}} \right| \right] \\ &\times \frac{\min(P(\tilde{A}), P(\tilde{B})) + \min(A(\tilde{A}), A(\tilde{B}))}{\max(P(\tilde{A}), P(\tilde{B})) + \max(A(\tilde{A}), A(\tilde{B}))}. \end{aligned} \quad (5)$$

Where $x_{\tilde{A}}^*$ and $x_{\tilde{B}}^*$ are the horizontal centers of gravity. $P(\tilde{A})$ and $P(\tilde{B})$ are the perimeters. $P(\tilde{A})$ is calculated as follows:

$$P(\tilde{A}) = \sqrt{(a_1 - a_2)^2 + w_{\tilde{A}}^2} + \sqrt{(a_3 - a_4)^2 + w_{\tilde{A}}^2} + (a_3 - a_2) + (a_4 - a_1) \quad (6)$$

$A(\tilde{A})$ and $A(\tilde{B})$ are the areas of $\tilde{A}$ and $\tilde{B}$. $A(\tilde{A})$ is calculated as follows:

$$A(\tilde{A}) = w_{\tilde{A}}(a_3 - a_2 + a_4 - a_1) / 2 \quad (7)$$

The larger the value of $S(\tilde{A}, \tilde{B})$ is, the more similar the two generalized trapezoidal fuzzy numbers $\tilde{A}$ and $\tilde{B}$ is.

B. Dempster-Shafer evidence theory [8,9]

Evidence theory first supposes the definition of a set of hypotheses $\Theta = \{H_1, H_2, \dots, H_N\}$ called the frame of discernment [8,9]. It is composed of N exhaustive and exclusive hypotheses. Form the frame of discernment Θ , let us denote $P(\Theta)$, the power set is composed with the 2^N propositions A of Θ . A BPA is a function from $P(\Theta)$ to $[0,1]$ defined by:

$$m: P(\Theta) \rightarrow [0,1] \quad A \mapsto m(A), \quad (8)$$

$$\sum_{A \in P(\Theta)} m(A) = 1, \quad m(\emptyset) = 0. \quad (9)$$

Dempster's combination rule, noted by $m = m_1 \oplus m_2$, is the first one within the framework of evidence theory which can combine two BPAs m_1 and m_2 to yield a new BPA:

$$m(A) = \frac{1}{1-k} \sum_{B \cap C = A} m_1(B) m_2(C) \quad (10)$$

$$k = \sum_{B \cap C = \emptyset} m_1(B) m_2(C) \quad (11)$$

where k is a normalization constant, called conflict because it measures the degree of conflict between m_1 and m_2 . The larger k is, the greater the conflict between m_1 and m_2 is.

When conflicting evidence is present, Dempster's rule for combining beliefs often produces counter-intuitive results [12]. To solve these problems, several alternatives to the normalization process have been proposed [12-14]. One of the efficient methods is the use of discounting coefficient [14]. Discounting coefficients can be seen as reliability coefficients. It means the reliability of the information source. Given reliability coefficient α , the next step is to incorporate it into the fusion process. To handle conflict between information sources, a discounting rule is given as follows:

$$\begin{cases} m^\alpha(\Theta) = (1-\alpha)m(\Theta) + \alpha \\ m^\alpha(\Theta) = (1-\alpha)m(\Theta) + \alpha, \forall A \subset \Theta \text{ and } A \neq \emptyset \end{cases} \quad (12)$$

These discounted BPAs can be combined to obtain the fused result, using the Dempster's rule of combination.

III. THE MODEL OF E-COMMERCE SYSTEM SECURITY ASSESSMENT

In security assessment of E-Commerce system, the experts not only must refer basic performance of E-Commerce system, but also need to consider subjective criteria, expectations, and some other important information. However, these information usually cannot concretely quantify with fuzziness. Therefore, using fuzzy multi-criteria decision-making to evaluate E-Commerce system security is more practical. Below we introduce our method step by step.

Step 1. Establishing a decision hierarchical structure

The first step is to establish a hierarchical structure of evaluating E-Commerce system security. For security assessment of E-Commerce systems, many criteria need be considered. It is difficult to reasonably distribute the weights of the criteria, which is the true reflection of importance of each criterion in the whole security assessment system.

Therefore, the multilevel evaluation need be considered. The evaluation criteria of the model are classified into three levels, as depicted in Table **Error! Reference source not found.** The first level criteria are network security, transaction security, information security as well as physical security. In the second level, all the first level criteria are divided into 2~3 second level criteria. Further, in the third level, all the second level criteria are divided into 2~3 third level criteria. The experts will give their opinions on the third level criteria.

To hedge risks, more experts are usually required to be involved in the decision-making process in order to make reasonable decisions. A group of five experts is identified in our example to aid in the E-Commerce system security assessment. In our method, their opinions of the ratings are represented by the form of the linguistic variables in Table I. The experts give their ratings of the third level criteria, shown in Table III.

Step 2. Integrating the ratings of the third level criteria.

The integration value of the ratings of the third level criteria could be calculated by the fuzzy arithmetic operator. Because of the difference of the knowledge and the background of every expert, the credibility of the rating, which is given by different experts, is different. So when the ratings of the third level criteria are integrated, the weight criterion of every expert could be different. Obviously, $\sum_{t=1}^T m_t = 1$ satisfies the normalization, and the larger m_t is, the more influential the expert t 's opinion is on the evaluation result. Without loss of generality, in this example, we set every expert with the same weight criterion $m_t = 1/T$, $t=1,2,\dots,T$, T is the number of experts.

Let $r_{ijk} = (a_{ijk}, b_{ijk}, c_{ijk}, d_{ijk})$, $i=1,2,\dots,M$, $j=1,2,\dots,N$; $k=1,2,\dots,K$, $t=1,2,\dots,T$, be the linguistic variable of the rating, which is given to the third level criterion U_{ijk} by expert t . Then, the integrated rating $\bar{r}_{ijk} = (a_{ijk}, b_{ijk}, c_{ijk}, d_{ijk})$ of the third level criterion U_{ijk} can be calculated as

$$\bar{r}_{ijk} = (m_1 \times r_{ijk1}) \oplus (m_2 \times r_{ijk2}) \oplus \dots \oplus (m_T \times r_{ijkT}). \quad (13)$$

For example, in Table III, the ratings, which are given to the third level criterion "Operating system security U_{111} " by the five experts, are "Very good (VG)", "Good (G)", "Medium good (MG)", "Good (G)", and "Medium poor (MP)", respectively. Then, the integrated rating of the criterion "Operating system security" could be calculated as follows:

$$\begin{aligned} \bar{r}_{111} &= [0.2 \times (8, 9, 10, 10)] \oplus [0.2 \times (7, 8, 8, 9)] \oplus [0.2 \times (5, 6, 7, 8)] \\ &\quad \oplus [0.2 \times (7, 8, 8, 9)] \oplus [0.2 \times (2, 3, 4, 5)] \\ &= (5.8, 6.8, 7.4, 8.2) \end{aligned}$$

In the same way, all the integrated ratings of the third level criteria could be calculated. The results are listed in Table III.

Step 3. Determining BPA based on the similarity of fuzzy numbers.

At first, we use (5) to calculate the similarities between all the integrated ratings and all the linguistic variables of the ratings, respectively. Then, normalizing the obtained similarities, the BPA can be obtained and listed in Table IV.

Step 4. Combining the BPA from the third level to the first level using Dempster's combination rule.

Once the BPAs of the third level criteria are obtained, we can use Dempster's combination rule (10) to combine all the third level evidence to obtain the second level evidence. For example, the BPA of the second level criterion "System security U_{11} " can be calculated as follows:

$$m_{U_{11}} = m_{U_{111}} \oplus m_{U_{112}}$$

All the other BPAs of the second level criteria can be obtained in a same way. Once the BPAs of the second level criteria are obtained, we can calculate the BPAs of the first

level criteria in the same way. For example, the BPA of the first level criterion "Network security U_1 " can be calculated as follows:

$$m_{U_1} = m_{U_{11}} \oplus m_{U_{12}} \oplus m_{U_{13}}$$

The fusion results are listed in Table V.

TABLE III. DATA FOR E-COMMERCE SYSTEM SECURITY ASSESSMENT

The first level criteria	The second level criteria	The third level criteria	The ratings					The integrated ratings
			Expert1	Expert2	Expert3	Expert4	Expert5	
Network security U_1	System security U_{11}	Operating system security U_{111}	VG	G	MG	G	MP	(5.8,6.8,7.4,8.2)
		Electronic commerce software security U_{112}	G	G	MG	VG	F	(6.2,7.2,7.6,8.4)
	Network operation security U_{12}	Data backup and recovery U_{121}	VG	VG	MG	MG	F	(6.0,7.0,7.8,8.4)
		Firewall security U_{122}	G	MG	MP	P	VP	(3.0,3.8,4.4,5.4)
		Local area network(LAN) Security U_{123}	F	F	MP	MG	G	(4.4,5.4,5.8,6.8)
	Web security U_{13}	Web application server security U_{131}	MP	F	MG	G	G	(5.0,6.0,6.4,7.4)
		Web database security U_{132}	MG	MP	F	P	G	(3.8,4.8,5.2,6.2)
Transaction security U_2	Logistics security U_{21}	Logistics base security U_{211}	VP	P	MG	G	VG	(4.2,5.0,5.6,6.4)
		Logistics distribution Safety U_{212}	VG	G	F	MG	MP	(5.2,6.2,6.8,7.6)
	Electronic transaction security U_{22}	Identity authentication security U_{221}	G	MG	MP	VG	MP	(4.8,5.8,6.6,7.4)
		Transaction confirmation security U_{222}	F	F	MG	MP	G	(4.4,5.4,5.8,6.8)
		Payment service security U_{223}	MG	F	F	MG	G	(5.0,6.0,6.4,7.4)
		Electronic payment system security U_{224}	G	F	F	MG	G	(5.4,6.4,6.6,7.6)
		Data Transmission encryption mechanism U_{225}	G	G	MG	F	MP	(5.0,6.0,6.4,7.4)
		Digital signature mechanism U_{226}	VG	G	MG	F	MP	(5.2,6.2,6.8,7.6)
Information security U_3	Information storage security U_{31}	Database security U_{311}	F	F	MG	MP	P	(3.2,4.2,4.6,5.6)
		Terminal security U_{312}	VP	P	F	MP	MG	(2.4,3.2,3.8,4.8)
	Information audit security U_{32}	Information content audit security U_{321}	G	MG	MP	F	MP	(4.0,5.0,5.6,6.6)
		Information subject verification security U_{322}	MG	F	MP	P	MP	(2.8,3.8,4.4,5.4)
Physical security U_4	Room environment security U_{41}	Management institution security U_{411}	P	F	MP	G	MG	(3.8,4.8,5.2,6.2)
		Site security U_{412}	G	VG	MG	MP	F	(5.2,6.2,6.8,7.6)
	Hardware protection security U_{42}	Equipment information protection c U_{421}	MG	MP	F	VP	P	(2.4,3.2,3.8,4.8)
		Input/output control measures U_{422}	MP	P	MG	G	VP	(3.0,3.8,4.4,5.4)

TABLE IV. GENERATING BPA ACCORDING TO THE SIMILARITIES

The third level criteria	$m(VP)$	$m(P)$	$m(MP)$	$m(F)$	$m(MG)$	$m(G)$	$m(VG)$
Operating system security U_{111}	0.0794	0.0988	0.1290	0.1585	0.1888	0.1799	0.1656
Electronic commerce software security U_{112}	0.0729	0.0971	0.1224	0.1596	0.1820	0.1944	0.1716
Data backup and recovery U_{121}	0.0749	0.0947	0.1280	0.1548	0.1897	0.1860	0.1719
Firewall security U_{122}	0.1342	0.1492	0.1782	0.1745	0.1462	0.1174	0.1003
Local area network(LAN) Security U_{123}	0.1037	0.1228	0.1485	0.1804	0.1710	0.1459	0.1277
Web application server security U_{131}	0.0928	0.1126	0.1388	0.1709	0.1844	0.1592	0.1413
Web database security U_{132}	0.1144	0.1328	0.1580	0.1897	0.1579	0.1328	0.1144
Logistics base security U_{211}	0.1090	0.1280	0.1530	0.1854	0.1642	0.1395	0.1209
Logistics distribution Safety U_{212}	0.0892	0.1071	0.1364	0.1649	0.1919	0.1625	0.1480
Identity authentication security U_{221}	0.0932	0.1105	0.1460	0.1670	0.1911	0.1534	0.1388
Transaction confirmation security U_{222}	0.1037	0.1228	0.1485	0.1804	0.1710	0.1459	0.1277

Payment service security U_{223}	0.0928	0.1126	0.1388	0.1709	0.1844	0.1592	0.1413
Electronic payment system security U_{224}	0.0853	0.1104	0.1309	0.1707	0.1870	0.1707	0.1450
Data Transmission encryption mechanism U_{225}	0.0928	0.1126	0.1388	0.1709	0.1844	0.1592	0.1413
Digital signature mechanism U_{226}	0.0892	0.1071	0.1364	0.1649	0.1919	0.1625	0.1480
Database security U_{311}	0.1277	0.1459	0.1710	0.1804	0.1485	0.1228	0.1037
Terminal security U_{312}	0.1480	0.1625	0.1919	0.1649	0.1364	0.1072	0.0891
Information content audit security U_{321}	0.1091	0.1253	0.1576	0.1813	0.1692	0.1365	0.1210
Information subject verification security U_{322}	0.1345	0.1493	0.1828	0.1720	0.1478	0.1153	0.0983
Management institution security U_{411}	0.1144	0.1328	0.1580	0.1897	0.1579	0.1328	0.1144
Site security U_{412}	0.0891	0.1072	0.1364	0.1649	0.1919	0.1625	0.1480
Equipment information protection U_{421}	0.1480	0.1625	0.1919	0.1649	0.1364	0.1072	0.0891
Input/output control measures U_{422}	0.1342	0.1492	0.1782	0.1745	0.1462	0.1174	0.1003

TABLE V. THE BPA OF THE FIRST LEVEL CRITERIA

The first level criteria	$m(VP)$	$m(P)$	$m(MP)$	$m(F)$	$m(MG)$	$m(G)$	$m(VG)$
Network security U_1	0.0047	0.0183	0.0862	0.2939	0.3492	0.1733	0.0744
Transaction security U_2	0.0023	0.0103	0.0577	0.2809	0.4661	0.1323	0.0504
Information security U_3	0.0811	0.1298	0.2767	0.2714	0.1482	0.0607	0.0321
Physical security U_4	0.0630	0.1075	0.2294	0.2803	0.1882	0.0845	0.0471

Step 5. Integrating the importance weights of the first level criteria and obtaining the discounting coefficient

It is very important to select the importance weights of the first level criteria, because they reflect the positions and the functions of the criteria in evaluation and directly affect the comprehensive evaluation results. However, because the focuses of the different experts are different, the weights which the different experts gave are not the same. In this paper, the experts give their opinions of the importance of the first level criteria using the linguistic variables in Table II, shown in Table VI. Similar to the integration of ratings, the integrated weights of the first level criteria can also be obtained using fuzzy arithmetic operator. Let $w_{it} = (a_{it}, b_{it}, c_{it}, d_{it})$; $i=1,2,\dots,M$; $t=1,2,\dots,T$, be the linguistic variable of the weight, which is assigned to the first level criterion U_i by expert t . Without loss of generality, in this example, we set every expert with the same weight criterion $m_t = 1/T$, $t=1,2,\dots,T$, T is the number of experts. Then, the integrated weight $\bar{w}_i = (a_i, b_i, c_i, d_i)$ of the first level criterion U_i can be obtained as

$$\bar{w}_i = (m_1 \times w_{i1}) \oplus (m_2 \times w_{i2}) \oplus \dots \oplus (m_T \times w_{iT}). \quad (14)$$

The integrated weights of the first level criteria are listed in Table VI. Then, defuzzify the integrated weight into a crisp number using (4).

$$\bar{w}_1^{crisp} = 0.25 \times (0.68 + 0.78 + 0.82 + 0.90) = 0.795$$

All the crisp numbers of the integrated weights could be calculated in the same way. The results are listed in Table

VI. Obviously, the greater the crisp number of the criterion is, the more important the criterion is. As can be seen from the Table VI, "Network security" is the most important criterion based on the integrated experts' opinions, while "Physical security" is the least important criterion.

In order to realize the different effects of the first level criteria with the different importance weights, the discounting coefficient could be calculated based on the crisp numbers of the criteria as follows:

$$\alpha_i = \frac{\bar{w}_i^{crisp}}{\max_{i=1,\dots,M} \{\bar{w}_i^{crisp}\}}, \quad i=1,2,\dots,M. \quad (15)$$

For example, the discounting coefficient of the criterion "Transaction security" is $0.735/0.795=0.9245$. In the same way, all the other discounting coefficient of each criterion can be obtained and shown in Table VI. Apparently, the greater the crisp number of the criterion is, the greater the discounting coefficient is. Then, the discounting coefficient will be used in the following fusion of multi-criteria data based on Dempster's combination rule. According to (12) and the above analysis, it shows that important criterion makes greater effect on the final assessment than the less important one.

Step 6. Discounting the BPA of the first level criteria.

Equation (12) and the discounting coefficient in Table VI are used to discount the BPA of the first level criteria in Table V. The results are listed in Table VII.

TABLE VI. THE IMPORTANCE WEIGHTS OF THE FIRST LEVEL CRITERIA

The first level criteria	The evaluation weight					The integrated weights	Crisp number	Discounting coefficient
	Expert1	Expert2	Expert3	Expert4	Expert5			
Network security U_1	VH	H	H	MH	H	(0.68,0.78,0.82,0.90)	0.7950	1
Transaction security U_2	H	M	VH	H	MH	(0.62,0.72,0.76,0.84)	0.7350	0.9245
Information security U_3	M	VH	L	ML	H	(0.44,0.54,0.58,0.66)	0.5550	0.6981
Physical security U_4	M	H	L	L	ML	(0.30,0.40,0.42,0.52)	0.4100	0.5157

TABLE VII. THE DISCOUNTED BPA OF THE FIRST LEVEL CRITERIA

The first level criteria	$m(VP)$	$m(P)$	$m(MP)$	$m(F)$	$m(MG)$	$m(G)$	$m(VG)$	$m(\Theta)$
Network security U_1	0.0047	0.0183	0.0862	0.2939	0.3492	0.1733	0.0744	0
Transaction security U_2	0.0021	0.0095	0.0534	0.2597	0.4309	0.1223	0.0466	0.0755
Information security U_3	0.0566	0.0906	0.1931	0.1895	0.1035	0.0424	0.0224	0.3019
Physical security U_4	0.0325	0.0554	0.1183	0.1445	0.0971	0.0436	0.0243	0.4843

Step 7. Combining the discounted BPA.

All the first level criteria's BPAs can be combined using Dempster's combination rule. The fusion results are shown in Table VIII. Based on the results in Table VIII, decisions can now be easily made, resulting in "Medium good" as the final security rating of the E-commerce system.

TABLE VIII. FUSION RESULTS

$m(VP)$	$m(P)$	$m(MP)$	$m(F)$	$m(MG)$	$m(G)$	$m(VG)$
0.0008	0.0039	0.0397	0.3643	0.4988	0.0746	0.0179

IV. CONCLUSION

In this paper, to solve the problem of E-Commerce security assessment, a new fuzzy MCDM method is proposed based on FST and DST. The proposed method has some merits as follows: First, the new method describes the experts' opinion by linguistic variables which can be expressed in trapezoidal (or triangular) fuzzy numbers. As we know, the decisions are subjective because they are made by the experts relying on their individual competence. Therefore, it is more appropriate to present the data using fuzzy numbers instead of crisp numbers. Second, Dempster's combination rule is used to combine the BPA which is transformed from the experts' opinions. Compared to the probability theory, DST can efficiently represent random and fuzzy information and can combine evidence without prior information. Therefore, the proposed method enables the ultimate decision makers to take advantage of both methods' merits to get the final reasonable security assessment result. In addition, the proposed method can be easily used to solve other MCDM problems.

ACKNOWLEDGMENT

This work was supported in part by a grant from National Natural Science Foundation of China, Grant No.61104214, Aviation Science Foundation, Grant No.2011ZC53041, and Foundation for Fundament Research of Northwestern Polytechnical University, Grant No.JC20120235.

REFERENCES

- [1] M. Gerber and R. Von Solms, "From risk analysis to security requirements," *Computers and Security*, vol.20(7), 2001, pp.577–584.
- [2] K. Ogata and K. Futatsugi, "Proof score approach to analysis of electronic commerce protocols," *International Journal of Software Engineering and Knowledge Engineering*, vol.20, 2010, pp.253–287.
- [3] I. C. Lin and C. C. Chang, "A countable and time-bound password-based user authentication scheme for the applications of electronic commerce," *Information Science*, vol.179(9), 2009, pp. 1269–1277.
- [4] T. Wasin, "E-commerce transaction security model based on cloud computing," *Proceedings of IEEE CCIS2012*, 2012, pp. 462–465.
- [5] Y. Kim, G. Park and T. Kim, "Security evaluation for information assurance," *Proceedings of the 5th IEEE International Conference on Computational Science and Applications*, 2007, pp. 227–230.
- [6] Y. J. Zhang, X. Y. Deng, D. J. Wei and Y. Deng, "Assesment of E-commerce security using AHP and evidential reasoning," *Expert Systems with Applications*, vol.39, 2012, 3611–3623.
- [7] H. J. Zimmermann, *Fuzzy set theory and its applications*. Boston: Kluwer Academic Publishers, 1991.
- [8] A. P. Dempster, "Upper and lower probabilities induced by a multi-valued mapping," *Annals of Mathematics and Statistics*, vol.38, 1967, pp.325–339.
- [9] G. Shafer, *A Mathematical Theory of Evidence*, Princeton University Press, Princeton University Press, Princeton, 1976.
- [10] S. J. Chen and S. M. Chen, "Fuzzy risk analysis based on similarity measures of generalized fuzzy numbers," *IEEE Trans. Fuzzy Syst.*, vol. 11(1), 2003, pp. 45–56.
- [11] S.M. Chen, "Evaluating weapon systems using fuzzy arithmetic operations," *Fuzzy Sets and Systems*, vol.77 (3), 1996, pp.265–276.
- [12] C. K. Murphy, "Combining belief functions when evidence conflicts," *Decision Support Systems*, vol.29, 2000, pp.1–9.
- [13] E. Lefevre, "Belief function combination and conflict management," *Information Fusion*, vol.3, 2002, pp.149–162.
- [14] P. Smets, "Belief functions: the disjunctive rule of combination and the generalized Bayesian theorem," *International Journal of Approximate Reasoning*, vol.9, 1993, pp. 11–35.
- [15] W. Jiang, F. Xin, D.M. Dejie and Y. Deng, "A Modified Similarity Measure of Generalized Fuzzy Numbe," 2011 International Conference on Advanced in Control Engineering and Information Science, *Procedia Engineering*, Aug. 2011, pp. 2773–2777.