Maritime Security—Assessment and Management

Z. L. Yang

PhD. Candidate
School of Engineering
Faculty of Technology and Environment, Liverpool John Moores University
Byrom Street, Liverpool L3 3AF
United Kingdom
Email: enrzyang@livjm.ac.uk
Tel: 0044 151 231 2028
Fax: 0044 151 231 2624

S. Bonsall

Dr.
Maritime Programme Co-ordinator
School of Engineering
Faculty of Technology and Environment, Liverpool John Moores University,
Byrom Street, Liverpool L3 3AF
United Kingdom
Email: s.bonsall@ljmu.ac.uk;
Tel: 0044 151 231 2235
Fax: 0044 151 231 2453

Q. G. Fang

Professor
Merchant Marine College, Shanghai Maritime University
1550, Pudong Dadao, Shanghai
People's Republic of China
Email: qgfang@mmc.shmtu.edu.cn
Tel: 0086 21 58855200
Fax: 0086 21 58850828

J. Wang

Professor of Marine Technology
School of Engineering, Faculty of Technology and Environment
Liverpool John Moores University
Byrom Street, Liverpool L3 3AF

United Kingdom
Email: j.wang@ljmu.ac.uk
Tel: 0033 151 231 2445
Fax: 0044 151 231 2453

Abstract After the tragedy of September 11, 2001, there is widespread concern in the international society that a terrorism organisation capable of the suicide hijackings of airliners could readily adapt these capabilities to major shipping targets. Techniques require to be developed to bridge maritime security gaps, which are defined as the potential areas associated with how to assess the security levels of a vulnerable maritime target and how to use the assessment to make appropriate decisions and controls. Some safety experts have focused their mind and attempted to use traditional risk assessment and decision making approaches to deal with possible terrorism threats in a maritime security area, investigate the key vulnerabilities and provide effective security control and management options. Two of the major challenges are to analyse security in situations of a high level uncertainty and to construct all information available with difference in nature in a utility form suitable as input to a risk inference mechanism. To solve such difficulties, this paper proposes a subjective security-based assessment and management framework using the combination of two fuzzy evidential reasoning (ER) approaches.

Keywords maritime security; security assessment; fuzzy logic; evidential reasoning

0 Introduction

The recently implemented International Shipboard and Port Facility Security (ISPS) Code [1] requires security assessment for various ship and port facility security plans. However, apart from its Section 8 in parts A and B, the Code does not prescribe a generally accepted methodology to carry out such assessment. Although Section 8 in Part B provides a number of issues to be considered when a security assessment is carried out, an obvious problem involved is that Part B is not mandatory and this may leave maritime stakeholders to choose and define their "suitable" methodologies and guidelines for individual maritime security assessments. For example, the American Bureau of Shipping (ABS) or Lloyd's Register favours the risk assessment guidelines provided by the United States Coast Guard (USCG), while Det Norske Veritas (DNV) and Germanischer Lloyd (GL) have developed guidelines based on checklists which have a close relationship to the ISPS Code. The USCG guidelines do not include any statements about likelihood of security threats, whereas the DNV-GL approach allows for a consideration of likely threats only[2]. The USCG approach requires the development of mitigation strategies and clear identification of the best option(s) from costly risk control measures and on the other hand, the users of the DNV-GL approach have to update their security assessments frequently depending on the latest security information available. As far as the threat of terrorism is concerned, the lack of critical mass in statistical data and the complexity of selecting the best SCO (optimisation) based on multiple security control attributes will prove the tasks of adapting traditional approaches to be challenging and generating novel and uniformed methodologies to be urgent.

One realistic way to analyse security with unavailable or incomplete objective data is to employ subjective assessment based on fuzzy *IF-THEN* rules in fuzzy set theory (FST). The approach based on the fuzzy rules, where conditional parts and/or conclusions contain linguistic variables [3] can model the qualitative aspects of human knowledge and reasoning process without employing precise quantitative analysis. It does not require an expert to provide a precise point at which a risk factor exists. This actually provides a tool for working directly with the linguistic information, which is commonly used in representing risk factors and carrying out safety assessment [4-7]. The purpose of analysing security is to identify the high-level risks in a prioritised list so as to ensure the correct decisions to be made and appropriate SCO(s) to be selected. However, realising such an objective requires other factors from economical, technical and environmental considerations to be satisfied. The factors can be defined as multiple decision attributes in analysing a complex maritime security management problem and normally investigated by the rules of a knowledge base in a hierarchical structure, in which the sub-criteria of the attributes can be further developed. In general, a bottom-up approach can be used to solve such a problem. Pieces of evidence from the lowest-level criteria are aggregated as evidence for the second lowest-level criteria/ attributes, which is in turn aggregated to produce evidence for higher-level attributes. The ER approach has presented the superiority in dealing with the synthesis of various pieces of evidence obtained/evaluated. Therefore, this study proposes a subjective security-based assessment and management framework using the combination of two fuzzy ER approaches. In the following, Section 2 outlines the security analysis and synthesis framework using a FRB-ER approach. The framework of synthesising security estimation and other multiple decision attributes is provided in Section 3 where the synthesis result can be used to produce the preference estimates associated with SCOs for ranking purposes. An illustrative example is used to demonstrate the application of the proposed framework in Section 4. Section 5 concludes this paper.

1 Fuzzy rule-based security analysis framework

The proposed framework for modelling security assessment consists of five major components, which outline all the necessary steps required for maritime security analysis.

1.1 Identify risk parameters and define fuzzy input and output variables

The threat-based risk parameters used to define subjective security estimates include those at both the senior and junior levels. The senior parameter is "***Security estimate* (*SE*)**", the single fuzzy output variable, which can be defuzzified to prioritise the risks. The variable is described linguistically and is determined by some junior parameters. In risk assessment, it is common to express a security level by degrees to which it belongs to such linguistic variables as "Poor", "Fair", "Average" and "Good" that are referred to as security expressions. To analyse the junior parameters, four fundamental risk parameters can be identified and defined as "*Will*" (***W***), "*Damage capability*" (***D***), "*Recall difficulty*" (***R***) and "*Damage probability*" (***P***). ***W*** decides the failure likelihood of a threat-based risk, which directly represents the lengths one goes to in taking a certain action. To estimate ***W***, one may choose to use such linguistic terms as "Very weak", "Weak", "Average", "Strong" and "Very strong". The combination of ***D*** and ***R*** responds to the consequence severity of the threat-based risk. Specifically speaking, ***D*** indicates the destructive force/execution of a certain action and ***R*** hints the resilience of the system after a failure or

disaster. The following linguistic terms can be considered as a reference to be used in subjectively describing the two sister parameters: “Negligible”, “Moderate”, “Critical” and “Catastrophic” for ***D*** and “Easy”, “Average”, “Difficult” and “Extremely Difficult” for ***R***. ***P*** means failure consequence probability and can be defined as the probability that damage consequences happen given the occurrence of the event. One may choose to use such linguistic terms as “Unlikely”, “Average”, “Likely” and “Definite” to describe it.

Fuzzy logic, based on FST, accommodates such linguistic terms through the concept of partial membership. In FST, everything is a matter of degree. Therefore, any existing element or situation in security assessment could be analysed and assigned a value (a degree) indicating how much it belongs to a member of the five sets of the risk parameters. Furthermore, five membership functions can be defined as five curves to describe how each point in the input and output space is mapped to a membership value (or degree of membership) between 0 and 1. Due to the advantage of simplicity, straight-line membership functions, especially triangular and trapezoidal membership functions have been commonly used to describe risks in safety assessment[8]. Consequently, the fuzzy membership functions in security assessment, consisting of five overlapping triangular or trapezoidal curves, are generated using the linguistic categories identified in knowledge acquisition and the fuzzy Delphi method[9]. They are provided in the work by Yang [10].

1.2 Construct a fuzzy rule base with a belief structure

Fuzzy logic systems are knowledge-based or rule-based systems constructed from human knowledge in the form of fuzzy *IF-THEN* rules [11]. An important contribution of the fuzzy system theory is that it provides a systematic procedure for transforming a knowledge base into a non-linear mapping [12]. A fuzzy *IF-THEN* rule is an *IF-THEN* statement in which some words are characterised by continuous membership functions. For example, the following is a fuzzy *IF-THEN* rule: *IF* ***W*** of a threat is “Very strong” AND ***D*** is “Catastrophic” AND ***R*** is “Extremely difficult” AND ***P*** is “Definite”, *THEN* ***SE*** is “Poor”. The descriptions of ***W***, ***D***, ***R***, ***P*** and ***SE*** are characterised by the membership functions. A fuzzy system is constructed from a collection of fuzzy *IF-THEN* rules from human experts or based on the domain knowledge and is then completed by combining these rules into a single system.

Obviously, the *IF-THEN* rules in this study can have two parts: an antecedent that responds to the fuzzy input and a consequence, which is the result/fuzzy output. In classical fuzzy rule-based systems, such input and output are usually expressed by single linguistic variables with 100% certainty and the rules constructed are also always considered as single output cases. However, when observing realistic maritime security situations, the knowledge representation power of the fuzzy rule systems will be severely limited if only single linguistic variables are used to represent uncertain knowledge. Four fuzzy input parameters include 17 (=5+4+4+4) linguistic variables, which can be assembled to produce 320 (=5×4×4×4) antecedents. Given a combination of input variables, *SE* may belong to more than one security expression with appropriate belief degrees. For example, a fuzzy rule with certain degrees of belief can be described as: *IF* ***W*** of a threat is “Very strong” AND ***D*** is “Catastrophic” AND ***R*** is “Extremely difficult” AND ***P*** is “Likely”, *THEN* ***SE*** is “Poor” **with a belief degree of 0.9**, “Fair” **with a belief degree of 0.1,** “Average” **with a belief degree of 0,** “Good” **with a belief degree of 0** and “Excellent” **with a belief degree**

of 0.

In order to model general and complex uncertain problems in security assessment, the classical fuzzy rule-based systems are extended to assign each rule a degree of belief. Assume that the four antecedent parameters, U_1=***W***, U_2=***D***, U_3=***R*** and U_4=***P*** can be described by linguistic variable A_{iJ_i}, where i=1, 2, 3, or 4 respectively and J_1 = 1, …, or 5, J_2, J_3 and J_4 = 1, …, or 4. One consequent variable ***SE*** can be described by 5 linguistic terms, D_1, D_2, D_3, D_4 and D_5. Let $A_{iJ_i}^k$ be a linguistic term corresponding to the i^{th} parameter in the k^{th} rule, with i=1, 2, 3 and 4. Thus, the generic k^{th} rule in the rule base can be defined as follows:

$\boldsymbol{R}_{\mathbf{k}}$: IF ***W*** is $A_{1J_1}^k$ and ***D*** is $A_{2J_2}^k$ and ***R*** is $A_{3J_3}^k$ and ***P*** is $A_{4J_4}^k$, then ***SE*** is D_1 with a belief degree of β_{1k}, D_2 with a belief degree of β_{2k}, D_3 with a belief degree of β_{3k}, D_4 with a belief degree of β_{4k} and D_5 with a belief degree of β_{5k} .

where $\sum_{i=1}^{5} \beta_{ik} = 1$, $k \in \{1, \ldots, 320\}$. It is noted that all the parameters and the belief degrees of the rules are usually assigned at the knowledge acquisition phrase by multiple experts on the basis of subjective judgements. An entire rule base including 320 rules with a belief degree structure is provided in [10].

1.3 Application of a frb-er approach

Once a rule-based system is established, it can be used to perform inference for given fuzzy or incomplete observations to obtain the corresponding fuzzy output, which can be used to assess the security level of a vulnerable maritime target. The inference procedure is basically composed of three steps, summarized as follows.

1.3.1 Observation transformation

Before starting the inference process, observations available should be analysed to determine their relationship with each junior risk parameter in the antecedent in a numerical form. Four kinds of possible observations may be represented using membership functions to suit conditions under this study. They are either a single deterministic value with 100% certainty, a closed interval, a triangular distribution or a trapezoidal distribution [11]. Having defined the four junior risk parameters above, a matching function method [7] can be employed to perform the observation transformation and determine the belief degrees to which actual observations, which have been numerically described, match to each linguistic variable in the antecedent.

The matching function method chooses the *Max-Min* operation to show the similarity between the real input fuzzy set A^r and the corresponding fuzzy linguistic variables A_{iJ_i}, because it is a classical tool to set the matching degree between fuzzy sets [3]. Therefore, the matching degree between A^r and A_{iJ_i} can be defined as follows:

$$a_{iJ_i} = M(A^r, A_{iJ_i}) = \max[\min(\mu_{A^r}(x), \mu_{A_{iJ_i}}(x))] \quad (1)$$

where x covers the domain of the input A^r. Each a_{iJ_i} represents the extent to which A^r belongs to the defined linguistic variables in the i^{th} risk parameter in the antecedents. It is noteworthy that the fuzzy input may also be directly judged and expressed by experts using linguistic variables without the requirements of observation transformation.

1.3.2 Activation of rule weights

The aim of the observation transformation to the risk parameters is to obtain the corresponding security levels for further evaluating the priority of risks. Thus, the introduction of the risk parameters with some similarity degrees transformed from the realistic observations into the rule-based inference system constructed above is necessary. An activating rule weight method is used to implement such an introduction. In other words, the distributions of different weights to all rules can be used to describe the relationship between the risk input transformed from observations and the rules in the system. In order to obtain an appropriate weight for the k^{th} rule, the similarity degrees related to the k^{th} rule are required to be synthesised in a logical way that can reflect the *AND* connective between their representing risk parameters. Liu *et al.* [7] have recommended using the *Product* operator as the logical tool to synthesise the degrees and deal with the dependencies of the parameters ***W***, ***D***, ***R*** and ***P***. Consequently, since the four junior risk parameters have the same importance, the weight of the k^{th} rule can be calculated as follows:

$$\theta_k = \frac{\prod_{i=1}^{4} \alpha_{iJ_i}^k}{\sum_{m=1}^{320} (\prod_{i=1}^{4} \alpha_{iJ_i}^m)} \quad (i = 1, 2, 3 \text{ or } 4;\ J_1 = 1, \ldots, \text{or } 5;\ J_2, J_3 \text{ and } J_4 = 1, \ldots, \text{or } 4) \quad (2)$$

Note that the situations where some of $\alpha_{iJ_i}^m$ are equal to zero will geminately simplify the calculation through the ignorance of the rules including those linguistic variables with a zero similarity degree.

1.3.3 Rule inference for the calculation of security levels using the er approach

Use of the rule weight method can successfully distribute different weights to all related rules and thus, enables the establishment of a new rule-based system, which can be summarized using the following rule expression matrix shown in Table 1.

Table 1 A new rule expression matrix for the introduction of observations

Antecedent \ Belief \ Consequence					Poor	Fair	Average	Good
A^1_{1J1}	A^1_{2J2}	A^1_{3J3}	A^1_{4J4}	θ_1	β_{11}	β_{21}	β_{31}	β_{41}
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
A^k_{1J1}	A^k_{2J2}	A^k_{3J3}	A^k_{4J4}	θ_k	β_{1k}	β_{2k}	β_{3k}	β_{4k}
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

A^{n}_{1J1}	A^{n}_{2J2}	A^{n}_{3J3}	A^{n}_{4J4}	θ_{n}	β_{1n}	β_{2n}	β_{3n}	β_{4n}

In the matrix, n represents the number of all rules whose weights are not zero.

Having represented each rule using the rule expression matrix, the ER approach [13-14] can be used to combine the rules and generate a final conclusion, which is a belief distribution on the security expressions as well as giving a panoramic view about the security level for a given observation.

1.4 Security synthesis in a hierarchy

The discussion above focuses on the security assessment of basic events at the bottom level of a hierarchical structure done by an expert. The security levels of a system on a higher level are often determined by all the associated vulnerable events of their individual components, which make up the structure. Therefore, this part is concerned with the security synthesis of a system at various levels such as:

- The synthesis of security estimates of a specific vulnerable event for a component done by a panel of experts; or
- The synthesis of security estimates of various vulnerable events to a component, furthermore, to the security associated with each sub-system, and finally the security associated with the system being investigated.

Consequently, the multi-expert and multi-level security synthesis can be carried out to obtain the security evaluation of the system using the ER approach introduced previously.

1.5 Ranking security estimates

In order to rank the security estimates expressed by fuzzy sets, the fuzzy linguistic variables require to be defuzzified by giving each of them an "appropriate" utility value (U_v). Many defuzzification algorithms have been developed, of which Chen and Klien [15] may be well suited to modelling the fuzzy security expressions.

Consequently, the four security linguistic expressions of the senior risk parameter can be deffuzzified as the set of [0, 0.3125, 0.5926, 1]. The index value (N_v) for ranking the security estimates can be calculated as follows:

$$N_v = \beta^1 \times 0 + \beta^2 \times 0.3125 + \beta^3 \times 0.5926 + \beta^4 \times 1 \qquad (3)$$

where β^i (i = 1, 2, 3, 4) is a belief degree measuring the subjective uncertainty that " *SE* belongs to each of the four security expressions".

2 Fuzzy link-based security management framework

The study of this section is to synthesise the security estimates acquired above with other associated decision attributes (i.e. cost and time) and obtain the overall performance scores for each SCO. The analysis of a complex security-based decision making problem can be carried out using a hierarchical structure, where the top decision making issue is often determined by multiple attributes. Each attribute usually has several parameters and the parameters may be further decomposed into more detailed sub-parameters. Such a top-down hierarchy can be kept under

analysis until the lowest level factors can be effectively assessed by domain experts using their subjective knowledge based on objective information. The generic model of the hierarchy is shown in Fig. 1.

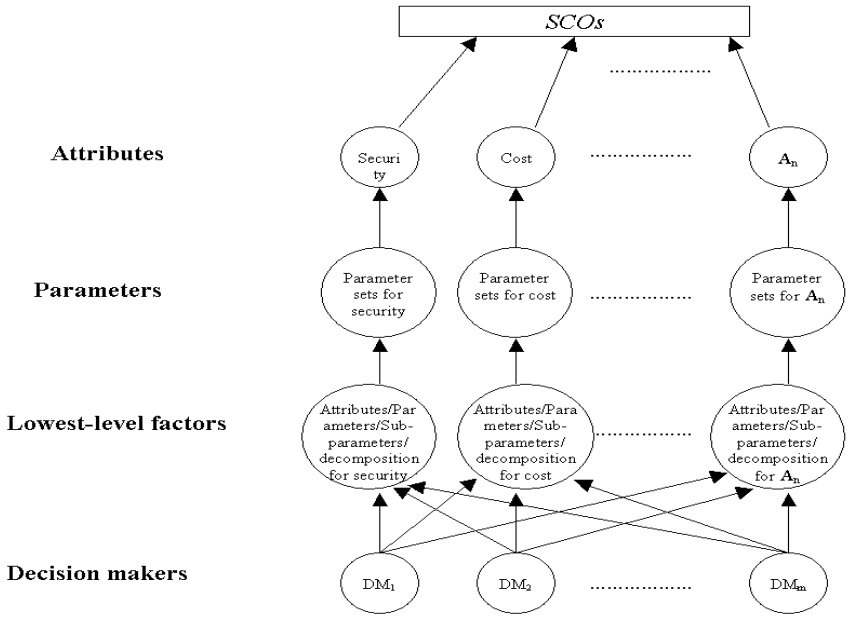

Fig. 1 A generic model of security-based decision making hierarchy

Once the hierarchy is constructed, the next step is to synthesise all evaluations from the experts to obtain the overall performance score of the top level event based on a bottom-up analysis. Let the estimation of the lowest-level factors based on all expert judgements to be fuzzy input and the overall performance scores to be fuzzy output. Then, the calculation of the fuzzy input can be obtained by combining the expert judgements using the ER approach. The transformation from fuzzy input to fuzzy output is usually complex and requires careful analysis of appropriate synthesising approaches.

In the work by Wang *et al.* [5], a traditional safety-cost based decision making method has been developed using the ER approach to provide a possible basis for the synthesis. However the applications of such a conventional method requires many assumptions such as the same amount of decision attribute linguistic variables and the unilateral-order relationship between the linguistic variables.

Having given the security analysis framework above, the FRB-ER method can be repeatedly used for the transformation from fuzzy input to fuzzy output in decision making. It requires establishing multiple fuzzy rule bases by following the top-down hierarchy, which can be produced by investigating individual family branches including a parent variable and its attached children. In the fuzzy rule bases, the linguistic variables used to express children constitute the antecedent part and the ones used to describe parent make up the consequence. An obvious weakness of this method is that both construction and calculation associated with multiple fuzzy rule bases are cost-ineffective and time consuming.

A fuzzy link-based method is developed for security-based multiple attribute decision-making analysis. The ER approach has proven to be an effective tool to deal with multidisciplinary

information and data. However, the application of the approach requires the assumption that all information and data is assessed or obtained on the basis of the same universe (one common utility space), which is often not the case in security management. Therefore, the information and data need to be transformed before being aggregated using either the rules based on fuzzy logic theory (which is related to the FRB-ER method) or the belief distributions based on the utility theory (which is associated with the FLB-ER) by decision makers. By taking the attribute "cost" in one multiple attribute decision making (MADM) analysis as an example, the FLB-ER approach can be introduced in the following context.

Assume the attribute "Cost" has its parent event "*SCO*" and children parameters "Investment" and "Maintenance" in a decision-making hierarchy. The top level event "*SCO*" can be expressed using such linguistic variables as "Slightly preferred", "Moderately preferred", "Average", "Preferred" and "Greatly preferred". The attribute "Cost" is described linguistically as "Very High", "High", "Average", "Low" and "Very Low". The linguistic variables used to assess the parameters "Investment" and "Maintenance" are individually the sets of ("Substantive", "Large", "Moderate", "Little") and ("Excessive", "Reasonable", "Marginal", "Negligible"). Then, a belief structure linked between the linguistic variables expressing different three-level attributes can be generated for the transformation from fuzzy input to output and shown in Fig. 2.

In Fig. 2, w represents the relative (normalised) weights of each attribute/parameters (same-level factors) under the same parent. The values attached to the arrows are the belief degrees β distributed by experts for indicating the relationships between linguistic variables of different-level decision factors. Note that the sum of the belief values from one linguistic variable is equal to one. For example, the parameter "Investment" with "Large" expression indicates that the level of the attribute "Cost" can be believed as 0.8 ($\beta_{i=2}^{c=2}$) "High" and 0.2 ($\beta_{i=2}^{c=3}$) "Average" without the presence of other evidence. As far as selecting the best "*SCO*" is concerned, the "High" cost evaluation can support "*SCO*" to 1 ($\beta_{c=2}^{r=2}$) "Moderately preferred" and the "Average" cost evaluation can be transformed into 1 ($\beta_{c=3}^{r=3}$) "Average" on the universe expressing "*SCO*". Such a linked belief structure can be used as a channel to transform the fuzzy input to fuzzy output by aggregating all values of fuzzy input, factor weights and belief degrees. The detailed transform process and aggregating calculations can be described in [10].

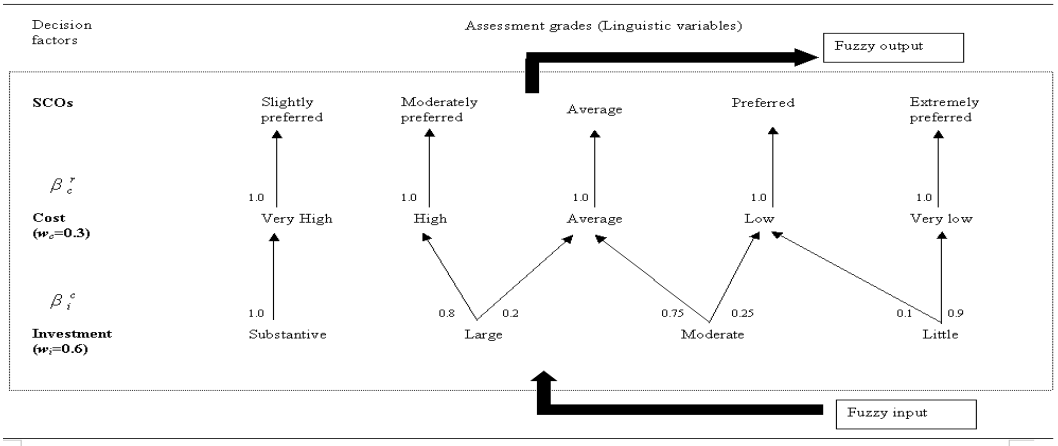

Fig. 2 An example of transforming fuzzy input to output

Suppose there are p SCOs, which are studied using s lowest-level factors and assessed by t experts. For the j^{th} SCO (j = 1, 2, …, p), the fuzzy input of the l^{th} factor (l = 1, 2,…, s) can be obtained by combining its t assessments from all experts on the basis of the ER approach. Using an Analytic Hierarchy Process (AHP) method [16], the weight of the l^{th} factor can also be calculated. Furthermore, using the fuzzy link-based approach, all fuzzy input can be transformed into their corresponding fuzzy output O^{Sj_l} with the individual weights w^{Sj_l} based on the same space, the utility expressions of SCOs. Then, all O^{Sj_l} can be further synthesised using the ER approach to obtain a preference estimate associated with the j^{th} SCO in terms of the utility expressions. The synthesised preference estimate U_j for the j^{th} SCO can be expressed as follows:

U_j = {u_j^1, *"Slightly preferred"*, u_j^2, *"Moderately preferred"*, u_j^3, *"Average"*, u_j^4, *"Preferred"*, u_j^5, *"Greatly preferred"*}

Preference degree P_j associated with the j^{th} SCO can be obtained by:

$$P_j = \sum_{t=1}^{5} u_j^t K_t \tag{4}$$

where the numerical values of K_t (t = 1, 2, …, 5) are assigned to describe the five utility expressions. The membership functions of the preference estimate can be decided by experts using the fuzzy Delphi method. Using the deffuzzification method in [15], the crispy values of the linguistic variables used to express the parameter preference can be obtained as follows:

$$K_1 = 0, K_2 = 0.3, K_3 = 0.5, K_4 = 0.7, K_5 = 1$$

SCO selection can therefore be carried out on the basis of the preference degrees associated with the p SCOs with regard to the particular considerations of security and other decision attributes. It is obvious that a larger P_j means that the j^{th} SCO is more desirable. The best SCO with the largest preference degree may be selected on the magnitudes of P_j.

3 An Illustrative example

The case introduced in the work by Yang *et al.* [17] is used and extended to illustrate the proposed framework in SCO selection and the inference reliability of the fuzzy rule-based approach in security assessment by comparing the results obtained from such two different studies.

A port is highly likely to be attacked by terrorists using two ways, attacking the channel/ waterway or bombing the quayside infrastructures/facilities of the terminals. Either of them can be associated with several attacking modes (See the analysis associated with Fig. 1 and Table 3 in [17]). Suppose there are four security analysts. There are four SCOs, which are described as follows:

SCO#1: *AIS* and Ship Identification Number.

SCO#2: Security awareness education as well as security and rescue training and drills.

SCO#3: Adequate perimeter fencing, lighting and locking, defending and cargo scanning devices and security equipments as well as supervision of transferring container cargo.

SCO#4: A security officer designated in the selection of staff (including the consideration of the background of employees or the reputation of the labour agency) as well as the positive identification of all visitors and vendors.

3.1 Ranking basic security events and calculating prior security estimate of top level events

Suppose four security analysts make the judgements on each attacking mode for the calculation of the prior security level of a target port. The judgements are assessed on the basis of the four defined junior risk parameters. For example, the mode of "using a missile or bomb to attack the channel" (EXT-CHA) can be analysed in Table 2. Using Equation (1), the input (observations) in Table 2 can be transformed and the judgements can be uniquely expressed by linguistic variables in Table 3. Then the fuzzy input based on all expert judgements can be obtained using the ER approach.

Table 2 An example of the subjective assessment of the junior risk parameters

Expert	***W***	***D***	***R***	***P***
E # 1	1, "Weak(W)"	(0.3, 0.5, 0.7)	{0.3, 0.4, 0.6, 0.7}	1, "Likely(L)"
E # 2	(0.1, 0.3, 0.5)	0.5, "Moderate(M)", 0.5, "Critical(Cr)"	(0.3, 0.5, 0.7)	{0.5, 0.6, 0.8, 0.9}
E # 3	[0.2, 0.4]	[0.4, 0.6]	[0.4, 0.6]	[0.6, 0.8]
E # 4	0.3	{0.3, 0.4, 0.6, 0.7}	1, "Average(A)"	(0.7, .08, 0.9)

Table 3 The unique linguistic variable expressions of the junior risk parameters

Expert	***W***	***D***	***R***	***P***
E # 1	1, "W"	0.5, "M", 0.5, "Cr"	0.17, "E", 0.5 "A", 0.33, "D"	1, "L"
E # 2	0.21, "VW", 0.53, "W", 0.26, "A"	0.5, "M", 0.5, "Cr"	0.14, "E", 0.57 "A", 0.29, "D"	0.43, "A", 0.57, "L"
E # 3	1, "W"	0.5, "M", 0.5, "Cr"	1, "A"	1, "L"
E # 4	1, "W"	0.5, "M", 0.5, "Cr"	1, "A"	1, "L"
Fuzzy input	0.04, "VW", 0.92, "W", 0.04, "A"	0.5, "M", 0.5, "Cr"	0.06, "E", 0.82 "A", 0.12, "D"	0.07, "A", 0.93, "L"

Having known the fuzzy input, the evaluation of the senior risk parameter, *SE* can be performed using the proposed FRB-ER method. In the rule base, 320 rules have been established, of which only 36 rules are fired in this particular case, i.e. Rules #18, #19, #22, #23, #26, #27, #34, #35, #38, #39, #42, #43, #82, #83, #86, #87, #90, #91, #98, #99, #102, #103, #106, #107, #146, #147, #150, #43, #82, #83, #86, #87, #90, #91, #98, #99, #102, #103, #106, #107, #146, #147, #150, #151, #154, #155, #162, #163, #166, #167, #170 and #171. Based on the individual matching belief degrees, the activation weight θ_k (k = 1,…, 36) of each rule in the fired sub-rule base is calculated using Equation (2). Consequently, the fuzzy rule expression matrix for the sub-rule base with the employed 36 rules is shown in Table 4.

Table 4 The fuzzy rule expression matrix of the EXT-CHA risk analysis

Rule	**Antecedent attribute (input)**					**Security estimate (output)**			
No	*W*	*D*	*R*	*D*	θ	Poor	Fair	Average	Good
18	Very weak	Moderate	Easy	Average	0.000084			0.5	0.5
19	Very weak	Moderate	Easy	Likely	0.001116			0.55	0.45
22	Very weak	Moderate	Average	Average	0.001148			0.7	0.3
23	Very weak	Moderate	Average	Likely	0.015252			0.75	0.25
26	Very weak	Moderate	Difficult	Average	0.000168			0.75	0.25
27	Very weak	Moderate	Difficult	Likely	0.002232			0.8	0.2
34	Very weak	Critical	Easy	Average	0.000084		0.2	0.7	0.1

35	Very weak	Critical	Easy	Likely	0.001116		0.35	0.65	
38	Very weak	Critical	Average	Average	0.001148		0.3	0.7	
39	Very weak	Critical	Average	Likely	0.015252		0.5	0.5	
42	Very weak	Critical	Difficult	Average	0.000168		0.5	0.5	
43	Very weak	Critical	Difficult	Likely	0.002232		0.6	0.4	
82	Weak	Moderate	Easy	Average	0.002016			0.6	0.4
83	Weak	Moderate	Easy	Likely	0.026784			0.75	0.25
86	Weak	Moderate	Average	Average	0.027552			0.8	0.2
87	Weak	Moderate	Average	Likely	0.366048			0.9	0.1
90	Weak	Moderate	Difficult	Average	0.004032			0.9	0.1
91	Weak	Moderate	Difficult	Likely	0.053568			1	
98	Weak	Critical	Easy	Average	0.002016		0.2	0.8	
99	Weak	Critical	Easy	Likely	0.026784		0.4	0.6	
102	Weak	Critical	Average	Average	0.027552		0.25	0.75	
103	Weak	Critical	Average	Likely	0.366048		0.45	0.55	
106	Weak	Critical	Difficult	Average	0.004032		0.5	0.5	
107	Weak	Critical	Difficult	Likely	0.053568		0.6	0.4	
146	Average	Moderate	Easy	Average	0.000084			0.9	0.1
147	Average	Moderate	Easy	Likely	0.001116		0.05	0.95	
150	Average	Moderate	Average	Average	0.001148			1	
151	Average	Moderate	Average	Likely	0.015252		0.1	0.9	
154	Average	Moderate	Difficult	Average	0.000168		0.1	0.9	
155	Average	Moderate	Difficult	Likely	0.002232		0.25	0.75	
162	Average	Critical	Easy	Average	0.000084		0.35	0.55	0.1
163	Average	Critical	Easy	Likely	0.001116		0.55	0.35	0.1
166	Average	Critical	Average	Average	0.001148		0.3	0.7	
167	Average	Critical	Average	Likely	0.015252		0.5	0.5	
170	Average	Critical	Difficult	Average	0.000168		0.5	0.5	
171	Average	Critical	Difficult	Likely	0.002232		0.7	0.3	

In Table 4, the ER approach is used to implement the combination of the 36 rules and generate the security estimate of the EXT-CHA threat. The final assessment result can be computed as follows and is shown in Fig. 3.

The prior SE of the EXT-CHA threat: {0, “Poor”, 0.188, “Fair”, 0.771, “Average”, 0.041, “Good”}

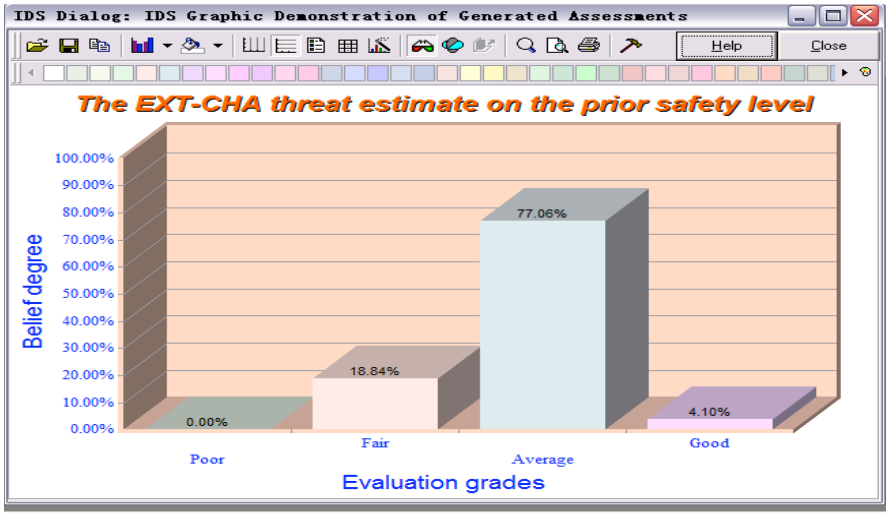

Fig. 3 The security estimate of the *EXT-CHA* threat

This result can be interpreted in such a way that the security estimate of the EXT-CHA threat is “Fair” with a belief degree of 0.188, “Average” with a belief degree of 0.771, and “Good” with a belief degree of 0.041.

Next, Equation (3) can be used to calculate the index value of the security estimate obtained for a ranking purpose as follows:

$$N_v = 0 \times 0 + 0.188 \times 0.3125 + 0.771 \times 0.5926 + 0.041 \times 1 = 0.557$$

Similar computations are performed for the other five basic events in the case. The security estimates generated for the VES-CHA, CARGO, EMPLOYEE, EXT-TER and VES-TER threats are summarised in Table 5. Since the FRB-ER and discrete fuzzy set approaches [17] have the same fuzzy input (subjective judgements), the fuzzy output should be kept in harmony to a significant extent in order to validate the reliability of the two different inference engines. The results have shown that the six basic events have been assessed with defuzzified values and ranked in an order to a quite similar extent with the results obtained from the work by Yang *et al.*[17]. The slight output difference in terms of deffuzzified values and ranking order is partly because of the application of different defuzzification methods and partly due to the accuracy of entirely subjective belief degree distributions in the rule base.

The ER approach can be used not only to aggregate fuzzy rules for the security analysis of the basic events in the FRB-ER framework but also to assess the security of the whole system (top level event) as well. According to the study in the work[17], the weights of the basic events can be appropriately distributed and obtained. Consequently the prior security estimate of the top event can be calculated by synthesising all fuzzy input of the basic events in Table 5 with their individual weights as follows:

The prior SE of the threat of terrorist attacking the port: {0.12, “Poor”, 0.371, “Fair”, 0.501, “Average”, 0.008, “Good”}.

Table 5 Security analysis and ranking of the basic events

Events	Junior security para-meters	E # 1	E # 2	E # 3	E # 4	Synthesised fuzzy input	Senior security estimates	Ranking (defuzz-ified values)
EXT-CHA	***W***	1, “W”	(0.1, 0.3, 0.5)	[0.2, 0.4]	0.3	0.04, “VW”, 0.92, “W”, 0.04, “A”	0, “P”, 0.188, “F”, 0.771, “A”, 0.041, “G”	0.5576
	D	(0.3, 0.5, 0.7)	0.5, “M”, 0.5, “Cr”	[0.4, 0.6]	{0.3, 0.4, 0.6, 0.7}	0.5, “M”, 0.5, “Cr”		
	R	{0.3, 0.4, 0.6, 0.7}	(0.3, 0.5, 0.7)	[0.4, 0.6]	1, “A”	0.06, “E”, 0.82, “A”, 0.12, “D”		
	P	1, “L”	{0.5, 0.6, 0.8, 0.9}	[0.6, 0.8]	(0.7, 0.8, 0.9)	0.07, “A”, 0.93, “L”		
VES-CHA	***W***	1, “S”	(0.5, 0.7, 0.9)	{0.5, 0.7, 0.8, 0.9}	0.7	0.1, “A”, 0.81, “S”, 0.09, “VS”	0.42, “P”, 0.48, “F”, 0.1, “A”,	0.211

	D	(0.7, 0.9, 1)	1, "Ca"	[0.8, 1]	{0.8, 0.9, 1, 1}	0.09, "Cr", 0.91, "Ca"	0, "G"	
	R	{0.7. 0.8, 0.9, 1}	(0.7, 0.8, 1)	[0.7, 0.9]	0.5, "D", 0.5, "ED"	0.48, "D", 0.52, "ED"		
	P	1, "L"	{0.6, 0.7, 0.8, 0.9}	[0.75, 0.85]	(0.7, 0.8, 0.9)	0.03, "A", 0.97, "L"		
CAR GO	***W***	1, "VS"	(0.8, 1, 1)	{0.8, 0.9, 1, 1}	1	0.08, "S", 0.92, "VS"	0.195, "P", 0.463, "F", 0.342, "A", 0, "G"	0.3473
	D	(0.3, 0.5, 0.7)	0.5, "M", 0.5, "Cr"	[0.4, 0.6]	{0.3, 0.4, 0.6, 0.7}	0.5, "M", 0.5, "Cr"		
	R	{0.4, 0.5, 0.6, 0.7}	(0.4, 0.5, 0.6)	[0.4, 0.6]	0.8, "A", 0.2 "D"	0.83, "A", 0.17 "D"		
	P	0.7, "A", 0.3 "L"	{0.3, 0.4, 0.5, 0.6}	0.55	(0.4, 0.5, 0.6)	0.78, "A", 0.22 "L"		
EMPLOYEE	***W***	1, "A"	[0.45, 0.55]	0.5	1, "A"	1, "A"	0.03, "P", 0.1, "F", 0.87, "A", 0, "G"	0.4924
	D	(0.3, 0.35, 0.4)	1, "M"	[0.3, 0.4]	{0.2, 0.3, 0.4, 0.5}	0.03, "N", 0.94, "M", 0.03, "Cr"		
	R	{0.3, 0.4, 0.5, 0.6}	(0.4, 0.5, 0.6)	[0.4, 0.6]	1, "A"	0.03, "E", 0.89, "A", 0.08, "D"		
	P	0.5, "L", 0.5 "D"	{0.7, 0.8, 0.9, 1}	[0.8, 1]	(0.8, 0.9, 1)	0.56, "L", 0.44 "D"		
EXT-TER	***W***	0.5, "A", 0.5, "S"	(0.5, 0.6, 0.7)	[0.5, 0.7]	0.6	0.5, "A", 0.5, "S"	0, "P" 0.241, "F", 0.755, "A", 0.004, "G",	0.5275
	D	(0.3, 0.35, 0.4)	1, "M"	[0.3, 0.4]	{0.2, 0.3, 0.4, 0.5}	0.03, "N", 0.94, "M", 0.03, "Cr"		
	R	{0.4, 0.5, 0.6, 0.7}	(0.4, 0.5, 0.6)	[0.4, 0.6]	0.8, "A", 0.2 "D"	0.83, "A", 0.17 "D"		
	P	1, "L"	{0.6, 0.7, 0.8, 0.9}	[0.75, 0.85]	(0.7, 0.8, 0.9)	0.03, "A", 0.97, "L"		
VES-TER	***W***	1, "S"	(0.5, 0.7, 0.9)	{0.5, 0.7, 0.8, 0.9}	0.7	0.1, "A", 0.81, "S", 0.09, "VS"	0.151, "P", 0.665, "F", 0.184, "A", 0, "G"	0.3172
	D	(0.6, 0.7, 0.8)	0.7, "Cr", 0.3 "Ca"	0.75	{0.6, 0.7, 0.8, 0.9}	0.74, "Cr", 0.26, "Ca"		
	R	{0.4, 0.5, 0.6, 0.7}	(0.4, 0.5, 0.6)	[0.4, 0.6]	0.8, "A", 0.2 "D"	0.83, "A", 0.17 "D"		
	P	0.5, "L", 0.5 "D"	{0.7, 0.8, 0.9, 1}	[0.8, 1]	(0.8, 0.9, 1)	0.56, "L", 0.44 "D"		

3.2 Making security-based decision making and selecting the best SCO

The FRB-ER approach contributes itself to the subjective security assessment and also exposes its weaknesses such as the complexity of inference. Therefore, when more elements require to be considered in a wider context, the FLB-ER approach proposed in Section 3 can be used. In this example, suppose there are four criteria chosen to decide the preference of the four SCOs. They are separately Security (S), Cost (C), Technique Requirement (TR) and Implement Time (IT). Some criteria have their sub-criteria. For example, the prior and posterior security estimations are

developed as the two sub-criteria of S, to demonstrate the security level changes after the implement of the SCOs. Such a hierarchy can be constructed in Fig. 4.

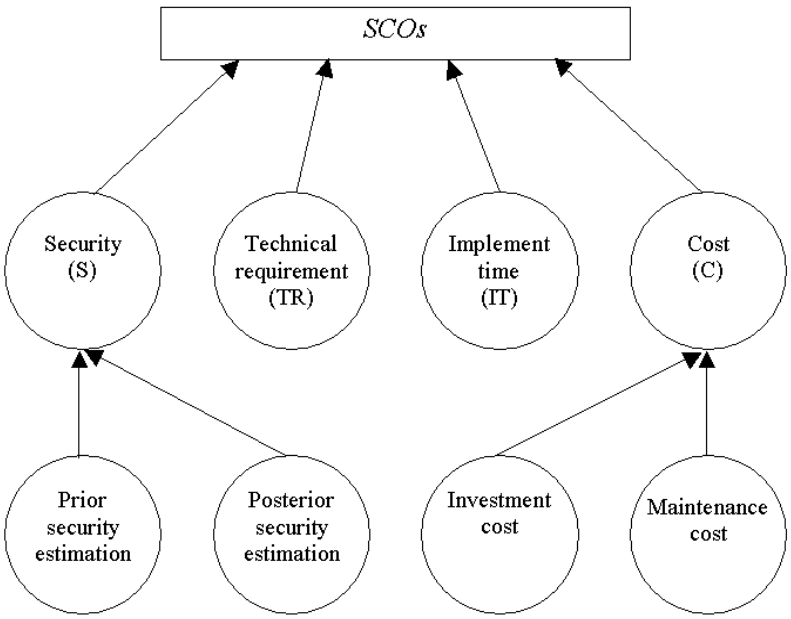

Fig. 4 The hierarchy of security based decision making

Suppose the four security analysts make their judgments on the lowest level criteria, which have been synthesised using the ER approach and shown in Table 6. Note that the judgements associated with the posterior security estimates are obtained using the FRB-ER approach in a similar way in which the prior security estimates are calculated. The linguistic terms used to express TR and IT are separately the sets of ("Very high(VH)", "High(H)", "Average(A)", "Low(L)", "Very low(VL)") and ("Very long(VL)", "Long(L)", "Average(A)", "Short(S)").

Table 6 The decision making attribute assessments

Lowest level criteria	*RCO*#1	*RCO*#2	*RCO*#3	*RCO*#4
Prior security estimate	0.12, "P", 0.371, "F", 0.501, "A", 0.008, "G"	0.12, "P", 0.371, "F", 0.501, "A", 0.008, "G"	0.12, "P", 0.371, "F", 0.501, "A", 0.008, "G"	0.12, "P", 0.371, "F", 0.501, "A", 0.008, "G"
Posterior security estimate	0, "P", 0.221, "F", 0.236, "A", 0.543, "G"	0, "P", 0.033, "F", 0.247, "A", 0.72, "G"	0.04, "P", 0.288, "F", 0.433, "A", 0.239, "G"	0.012, "P", 0.35, "F", 0.534, "A", 0.104, "G"
Technical requirement	0, "VH", 02, "H", 0.5, "A", 0.3, "L", 0, "VL"	0, "VH", 0.7, "H", 0.3, "A", 0, "L", 0, "VL"	0, "VH", 0, "H", 0, "A", 0, "L", 1, "VL"	0, "VH", 0, "H", 0, "A", 0.2, "L", 0.8, "VL"
Implement time	0.9 "VL", 0.1, "L", 0, "A", 0, "S"	0, "VL", 0.4, "L", 0.6, "A", 0, "S"	0, "VL", 0, "L", 0.2, "A", 0.8, "S"	0, "VL", 0, "L", 0, "A", 1, "S"
Investment cost	0, "S", 0.75, "La", 0.25, "M", 0, "Li"	0.4, "S", 0.6, "La", 0, "M", 0, "Li"	0, "S", 0.2, "La", 0.7, "M", 0.1, "Li"	0, "S", 0, "La", 0, "M", 1, "Li"
Maintenance cost	0, "E", 0, "R", 0.9, "M", 0.1, "N"	0.2, "E", 0.8, "R", 0, "M", 0, "N"	0, "E", 0.45, "R", 0.55, "M", 0, "N"	0, "E", 0, "R", 0.25, "M", 0.75, "N"

In order to obtain the best SCO, the judgements and estimates associated with each SCO require to be considered, combined and then defuzzified. However, as the fuzzy sets used to describe the judgements are defined on the basis of different universes, it may not be convenient to directly implement such a synthesis using the ER approach. It will be desirable that the FLB-ER approach can be used to carry out a unification of the different decision making attribute estimates in order

to avoid loss of useful information. Next, using the transforming graphic technique introduced in Fig. 2, the judgements listed in Table 6 can be transformed and expressed on a unified space, the preference of decision makers, as shown in Table 7.

Table 7 The unified decision making attribute assessments

Lowest level criteria	*RCO*#1	*RCO*#2	*RCO*#3	*RCO*#4
Prior security estimate	0.008, "SP", 0.375, "MP", 0.311, "A", 0.21, "P", 0.096, "GP"	0.008, "SP", 0.375, "MP", 0.311, "A", 0.21, "P", 0.096, "GP"	0.008, "SP", 0.375, "MP", 0.311, "A", 0.21, "P", 0.096, "GP"	0.008, "SP", 0.375, "MP", 0.311, "A", 0.21, "P", 0.096, "GP"
Posterior security estimate	0, "SP", 0.177, "MP", 0.257, "A", 0.159, "P", 0.407, "GP"	0, "SP", 0.026, "MP", 0.229, "A", 0.205, "P", 0.54, "GP"	0.04, "SP", 0.23, "MP", 0.447, "A", 0.103, "P", 0.18, "GP"	0.012, "SP", 0.28, "MP", 0.551, "A", 0.079, "P", 0.078, "GP"
Technical requirement	0, "SP", 02, "MP", 0.5, "A", 0.3, "P", 0, "GP"	0, "SP", 0.7, "MP", 0.3, "A", 0, "P", 0, "GP"	0, "SP", 0, "MP", 0, "A", 0, "P", 1, "GP"	0, "SP", 0, "MP", 0, "A", 0.2, "P", 0.8, "GP"
Implement time	0.9, "SP", 0.08, "MP", 0.02, "A", 0, "P", 0, "GP"	0, "SP", 0.32, "MP", 0.38, "A", 0.3, "P", 0, "GP"	0, "SP", 0, "MP", 0.1, "A", 0.18, "P", 0.72, "GP"	0, "SP", 0, "MP", 0, "A", 0.1, "P", 0.9, "GP"
Investment cost	0, "SP", 0.6, "MP", 0.338, "A", 0.062, "P", 0, "GP"	0.4, "SP", 0.48, "MP", 0.12, "A", 0, "P", 0, "GP"	0, "SP", 0.16, "MP", 0.565, "A", 0.185, "P", 0.09, "GP"	0, "SP", 0, "MP", 0, "A", 0.1, "P", 0.9, "GP"
Maintenance cost	0, "SP", 0, "MP", 0.09, "A", 0.81, "P", 0.1, "GP"	0.2, "SP", 0.16, "MP", 0.64, "A", 0, "P", 0, "GP"	0, "SP", 0.09, "MP", 0.415, "A", 0.495, "P", 0, "GP"	0, "SP", 0, "MP", 0.025, "A", 0.225, "P", 0.75, "GP"

Suppose the weights of decision making attributes and sub-criteria have been distributed in Table 8 by the four experts using an AHP method. Then, the judgements produced in Table 7 can be synthesised to obtain the utility description on the four SCOs using the ER approach, which can be further defuzzified as a crispy value for ranking the SCOs using Equation (4) as follows:

The preference assessment of the *RCO*#1: P_1 = {0.21, "SP", 0.222, "MP", 0.273, "A", 0.194, "P", 0.101, "GP"} = 0.44

The preference assessment of the *RCO*#2: P_2 = {0.076, "SP", 0.373, "MP", 0.313, "A", 0.119, "P", 0.119, "GP"} = 0.471

The preference assessment of the *RCO*#3: P_3 = {0.009, "SP", 0.081, "MP", 0.265, "A", 0.131, "P", 0.514, "GP"} = 0.836

The preference assessment of the *RCO*#4: P_4 = {0.002, "SP", 0.058, "MP", 0.113, "A", 0.106, "P", 0.721, "GP"} = 0.969

It can be noted that in this case, SCO#4 is ranked first, SCO#3 second, SCO#2 third and SCO#1 last. This implies that security and other decision making attributes are considered equally important while carrying out the security control evaluation, the best selection is SCO#4. When the relative importance of security against other attributeschanges, there may be different ranking orders of the SCOs. Suppose the relative weights of all the attributes and sub-attributes except security remain unchanged shown in Table 8. Fig. 5 shows the preference degrees associated with the four SCOs at different values of relative importance of security and the other attributes (TR, IT, C). For example, when the relative importance of security against the other attributes increases by 400%, the ranking of the four SCOs is SCO#2>SCO#4>SCO#3>SCO#1.

Table 8 The weights of decision making attributes

	Prior security estimate	Posterior security estimate	Technical requirement	Implement time	Investment cost	Maintenance cost
Weight ratio	0.1	0.9	1	1	0.6	0.4
Normalised weights	0.025	0.225	0.25	0.25	0.15	0.1

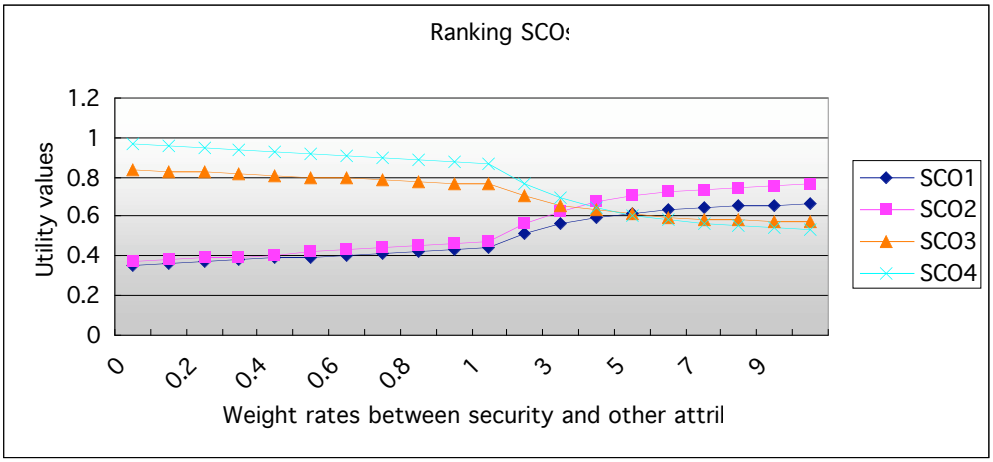

Fig. 5 Ranking of the SCOs

4 Conclusion

This paper outlines and explains a philosophy of subjective security based decision making modelling for maritime security assessment and management using fuzzy logic and ER approaches. For each SCO, the prior and posterior security estimates of each basic event are first carried out using the security analysis model based on the application of the FRB-ER approach. Then the ER approach is used to synthesise the prior/posterior security estimates to obtain the security estimates of the top event as the security attributes of the SCOs. Finally, the synthesis of security and other decision making attributes are performed using the MADM modelling based on a FLB-ER approach and mapped onto a common utility space before proceeding to the preference estimation and ranking SCOs.

Different from most conventional risk based decision making methodologies, the framework introduced is characterised with a unique feature associated with unification of input and output data. In the security analysis modelling, each input can be represented as a probability distribution on linguistic values for the antecedent using a belief structure. The main advantage of doing so is that precise data, random numbers and subjective judgements with uncertainty can be consistently modelled under a unified form. In the decision making modelling, the input data transformed by the linked belief structures can be unified and take into account subjective experts judgements with uncertainties having both probabilistic and possibilistic nature. Moreover, the ER approach provides a novel procedure for aggregating calculation, which can preserve the original features of multiple attributes with various types of information. This provides a solution for solving the difficulty of subjective risk assessment results involving academic bias resulting from various options from different individuals. Therefore, two kinds of combination of the fuzzy logic and ER

approaches can offer great potential in maritime security assessment and management.

Reference

[1] IMO. International Ship and Port Facility Security Code. SOLSA/CONF 5/34. London, UK: IMO Publication, 2002.

[2] Schroder J U, Mejia Jr M Q, Mukherjee P K, Manolis F M, Dreessen S. Potential Consequences of Imprecise Security Assessment. IAMU Journal 2006(4)2: 31-38.

[3] Zimmermann HJ. Fuzzy Set Theory and Its Application. Norwell, MA, Kluwer, 1991.

[4] Wang J, Yang J B, Sen P. Safety Analysis and Synthesis Using Fuzzy Set Modelling and Evidential Reasoning. Reliability Engineering & System Safety, 1995(47)3: 103-118.

[5] Wang J, Yang J B, Sen P. Multi-person and Multi-attribute Design Evaluations Using Evidential Reasoning Based on Subjective Safety and Cost Analyses. Reliability Engineering & System Safety, 1996(52): 113-128.

[6] Sii H S, Wang J, Ruxton T. A Fuzzy-logic-based Approach to Subjective Safety Modelling for Maritime Products. Journal of UK Safety and Reliability Society, 2001(21)2: 65-79.

[7] Liu J, Yang J B, Wang J, Sii H S, Wang Y M. Fuzzy Rule-based Evidential Reasoning Approach for Safety Analysis. International Journal of General Systems, 2004(23)2-3: 183-204.

[8] Wang J. A Subjective Methodology for Safety Analysis of Safety Requirements Specifications. IEEE Transactions on Fuzzy Systems, 1997(5)3: 418-430.

[9] Bojadziev G, Bojadziev M. Fuzzy Sets, Fuzzy Logic, Application. Singapore: World Scientific, 1995.

[10] Yang Z L. Risk Assessment and Decision Making of Container Supply Chains. PhD Thesis. Liverpool John Moores University, Liverpool, UK, 2006.

[11] Wang L X. A Course in Fuzzy Systems and Control, Prentice-Hall, NJ, USA, 1997.

[12] Sii H S, Wang J. Safety Assessment of FPSOs-The Process of Modelling System Safety and Case Studies. Report of the Project-"The Application of Approximate Reasoning Methodologies to Offshore Engineering Design" (EPSRC GR/R30624 and GR/R32413), 2002. Liverpool John Moores University, Liverpool, UK, 2002.

[13] Yang J B, Deng M, Xu D L. Nonlinear Regression to Estimate Both Weights and Utilities via Evidential Reasoning for MADM. Processing 5th International Conference, Optimization: Techniques and Applications. Hong Kong: Dec. 15-17, 2001.

[14] Yang J B, Xu D L. On the Evidential Reasoning Algorithm for Multiple Attribute Decision Analysis under Uncertainty. IEEE Transactions on Systems, Man and Cybernetics-Part A: Systems and Humans. 2002(32)3: 289-304.

[15] Chen C B, Klien C M. A Simple Approach to Ranking A Group of Aggregated Fuzzy Utilities. IEEE Transactions on System, Man, Cybernetics - Part B: Cybernetics, 1997(27)1: 26-35.

[16] Saaty T L. The Analytic Hierarchy Process. University of Pittsburgh, USA, 1980.

[17] Yang Z L, Bonsall S, Fang Q G, Wang J. Formal Safety Assessment of Container Liner Supply Chains. European Safety and Reliability Conference '05. Tri City, Poland, June 27-30, 2005.