

An integrated framework of security tool selection using fuzzy regression and physical programming

Hoai-Vu Nguyen*, Pauline Kongsuwan**, Sangmun Shin***,

Yongsun Choi***, Sangkyun Kim****

퍼지회귀분석과 physical programming을 활용한 정보보호 도구 선정 통합 프레임워크

Hoai-Vu Nguyen*, Pauline Kongsuwan**, 신상문***, 최용선***, 김상균****

Abstract

Faced with an increase of malicious threats from the Internet as well as local area networks, many companies are considering deploying a security system. To help a decision maker select a suitable security tool, this paper proposed a three-step integrated framework using linear fuzzy regression (LFR) and physical programming (PP). First, based on the experts' estimations on security criteria, analytic hierarchy process (AHP) and quality function deployment (QFD) are employed to specify an intermediate score for each criterion and the relationship among these criteria. Next, evaluation value of each criterion is computed by using LFR. Finally, a goal programming (GP) method is customized to obtain the most appropriate security tool for an organization, considering a tradeoff among the multi-objectives associated with quality, credibility and costs, utilizing the relative weights calculated by the physical programming weights (PPW) algorithm. A numerical example provided illustrates the advantages and contributions of this approach. Proposed approach is anticipated to help a decision maker select a suitable security tool by taking advantage of experts' experience, with noises eliminated, as well as the accuracy of mathematical optimization methods.

요 약

근거리통신망과 인터넷으로부터 유입되는 정보보호 위협이 증가하는 상황에 대처하기 위하여, 많은 기업들이 정보보호 시스템 구축을 고려하고 있다. 기업 내 의사결정자의 정보보호 도구 선택을 지원하기 위하여, 본 논문은 선형퍼지회귀분석 및 physical programming을 이용하는 세 가지 단계로 구성된 통합 프레임워크를 제안하였다. 첫

• 제1저자 : Hoai-Vu Nguyen 교신저자 : 최용선

• 투고일 : 2010. 07. 29, 심사일 : 2010. 08. 04, 게재확정일 : 2010. 08. 11.

* 베트남 FPT대, Computer기초학과 강사 ** 인제대학교 정보통신시스템학과 박사과정

*** 인제대학교 시스템경영공학과 교수 **** 강원대학교 산업공학과 교수

제, 정보보호도구 선정 기준 및 평가 기준에 대한 전문가들의 상대평가 의견을 바탕으로, 각 정보보호 기준들 간의 관계를 정량화시키기 위하여 analytic hierarchy process 및 quality function deployment 방법을 적용하였다. 그리고, 선형회귀분석법을 활용하여 각 기준별 평가값을 산출하였다. 마지막으로, 정보보호 시스템의 품질, 정보보호 수준, 비용 등의 다수 목적함수를 효과적으로 고려하기 위하여, physical programming weights 알고리즘을 통하여 도출된 가중치에 기반한 목표계획법을 활용하여 가장 적절한 정보보호 도구를 선정하였다. 이와 같은 과정은 구체적인 예제를 통해 단계별로 설명하고 그 장점을 가시적으로 제시하였다. 본 연구에서 제안한 방법은 전문가 제공 정보에서 발생 가능한 노이즈를 효과적으로 제거함으로써, 전문가의 경험을 통한 표준 정보보호 기준의 확보와 수학적 최적화 방법을 통한 정확성 확보의 장점을 의사결정자에게 제공할 것으로 기대된다.

▶ Keyword : security tool selection, analytical hierarchy process, quality function deployment, linear fuzzy regression, physical programming, goal programming.

1. Introduction

Today, information is one of the most important assets of any organization. The development of information technology has enabled the storage of vast amounts of information on computer systems and has ensured internal as well as external communication of organization networks. More specifically, information technology facilitates organizations in performing business transactions with customers, suppliers and other business partners. In addition, it supports organizations to provide their services to customer, and allows staff members to do their daily activities with accuracy, efficiency and effectiveness level using software, tools, and programs deployed in the organization's computer system. Some companies have become entirely dependent on computer and information systems for maintaining their day-to-day operations. Thus, information security is of vital importance for any organization and business. The Internet and local area networks, which are growing rapidly, have witnessed an increase in malicious attacks. Moreover, the importance of information systems and the increasing dependence of companies on such systems have made them vulnerable targets for attackers. All these factors have increased the necessity for deploying information security systems to protect organizations from external attacks, prevent information losses, and ensure secure

communication. Security managers must consider a wide range of security tools in order to select the most suitable one that can performs well at the right cost.

A large number of studies have discussed software quality and methods for the efficient development, evaluation, and selection of software as well as system projects ([1], [2], [3], [4]). Regarding security-related issues, there are also a number of methodologies available ([5], [6], [7], [8], [9], [10], [11]). Some provide general guidelines and evaluation of security products' functionality and effectiveness ([12], [13], [14]), but these comprehensive standards are time-consuming and expensive to evaluate. Moreover, the objective of these evaluation schemes is often to produce an official certification for each specific security tool, making it difficult to evaluate and select among those which have similar levels of certification [7]. Others based on two aspects which are annual loss expected (ALE) and return on security investment (ROSI) to evaluate information security system ([11], [15]). Recently, there is a new approach which uses security criteria and experts' estimations as the input data. Then estimation and optimization methods are employed to find out the relationship among these criteria and determine the most appropriate solution ([6], [7], [8], [10]). However this approach can still not eliminate the noise from experts' information nor address the issue that the optimization method uses a utility function which will not reflect exactly the physical meaning of the problems. To overcome these

drawbacks, this paper proposes a three-step integrated framework by using fuzzy regression (FR) and physical programming (PP) to help a decision maker (DM) on selecting a suitable security tool. First, based on the security criteria and expert's estimations analytic hierarchy process (AHP) and quality function deployment (QFD) are employed to specify an intermediate score for each criterion and the relationship among these criteria. Next, the dependent function of each evaluation criterion is computed using linear fuzzy regression (LFR). By using LFR to specify the estimation function, the vagueness and noise from experts' data can be reduced. Then, in order to integrate balance the multi-objectives of quality, credibility and costs, PP is utilized to find the optimal solution. Finally, setting the optimal solution as the target solution and using weights calculated by the physical programming weights (PPW) algorithm from the previous step, we apply a goal programming (GP) method to obtain the most appropriate security tool for an organization. The PP method which is used

here can involve not only the condition information and multiple design measures of engineering problems, but can also eliminate the weighting process when using the weighted-sum related optimization method. The case study example clearly illustrates the advantage and contribution of our approach.

An overview of the proposed procedure for selecting the most suitable security tool can be shown in Fig. 1. Section 2 provides the studies related to our applied domain - the selection of security tools for the organization. In Section 3, we explain the proposed integration approach including the security criteria and selection procedure, preprocess step, fuzzy regression for obtaining the dependent function of each criterion, and applied PP method and GP for finding the appropriate solution. Section 4 provides details on our approach and its application by means of a numerical example. Finally, Section 5 presents the conclusions and suggestions for future study.

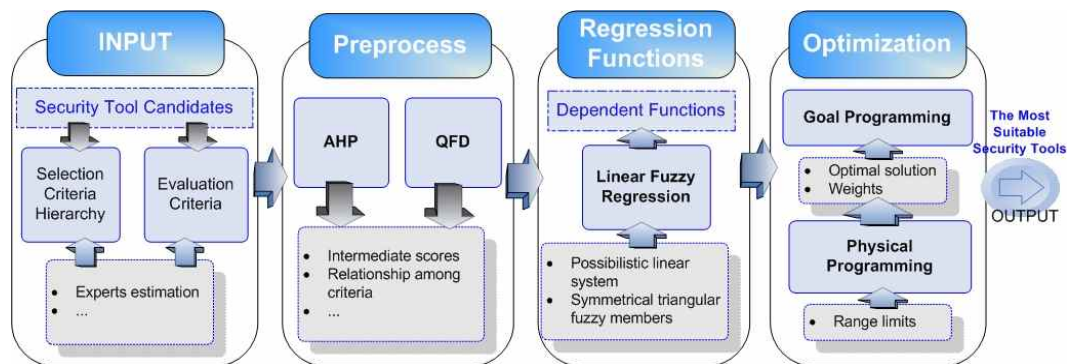


Fig. 1. Proposed approach for security tool selection

II. Literature review

Research on the selection/evaluation of security tools and related issues are considerably few ([5], [11], [15], [16]). Polk and Bassham [17] introduced a guide with criteria for judging the functionality,

practicality, and convenience of anti-virus tools. The strengths and limitations of various classes of anti-virus tools are discussed, as well as suggestions of appropriate applications for these tools. However, some classes of tools and most products are only available for personal computers. In addition, this study limits the functionality factors and does not concern about the providers, costs or other factors

which affect the decision in selecting antivirus tools. Firth et al. [18] proposed a lexicon of security functionalities to establish a common vocabulary between security objectives and the specification of tools selected to meet those objectives. These functionalities represent primitive actions that support information survivability and characterize an approach to analyze networked systems environments. Application of this analysis approach can help organizations in establishing criteria for selecting tools, and identifying requirements for new tool development to accommodate needs not currently met by available tools. There are some well-known security methodologies that have been introduced to evaluate and obtain high-quality information security systems such as ISO/IEC, ITSEC, TCSEC and etc. ([12], [13], [14]). These are the outcome of a series of efforts to develop criteria for the evaluation of information technology security and are broadly used within the international community. These standards focus on functionality or effectiveness of product itself. They cannot show the advantages or disadvantages between a large number of security tool candidates with various quality levels.

Recently, Kim and Lee [7] presented a methodology that consists of a *Process Model* (that consolidates strategic and operational viewpoints in a process model) and *Criteria* (that provides evaluation and selection criteria to support decisions on vendors and products) for supporting the selection of security control for information security management systems. The case study conducted by using AHP proves the potential value of this methodology in helping DM in supporting their selection of security controls. Choi and Shin [6] proposed a method for measuring the relative weights among the quality factors for a system on a development life cycle and simultaneously optimizing the balance between the level of quality and development costs. The paper suggests that the relative weights among the quality factors influence the operations of the system, and provides an optimal solution for the quality costs by

employing the desirability function (DF) approach. For optimization purposes, the study employs AHP as a multiple criteria decision making (MCDM) technique along with the DF approach. Nguyen et al. [10] proposed an integrated approach using AHP, mixed integer goal programming (MIGP) and the security criteria hierarchy to selection the most appropriate solution for an organization. The result of a case study showed the advantage of this approach. Kongsuwan et al. [8] proposed a 3-step approach to manage quality level for developing information security system adopting QFD. First, it showed how to find the importance of quality factors in the product by using QFD. Second, it presented an optimal cost or resource for quality factors under a limited budget. Lastly, it demonstrated how to find an overall quality level. Project leaders can consider this value as the quality of the final product itself. Applying this procedure the project team can gain the desired quality level by adjusting some requirements in the QFD step and recalculating a whole procedure. All the above-mentioned approaches based on the selection criteria to get the experts' estimation. Then, the problem is remodeled and solved by using some optimization methods. These approaches can employ the advantages from the criteria, the experience in the estimations of experts, and the correctness and flexibility of mathematics in the integrated optimization method to find out the most appropriate solution. From these studies, the security criteria hierarchy is well developed. However, there are still some limitations. When remodeling the problem and integrating experts' estimation, these methods still could not eliminate noise from the estimation data. In addition, the optimization methods use utility functions which can not exactly reflect the meaning of the problems. To overcome this, we propose an integrated approach to select the most appropriate solution based on LFR, PP and GP. Details of this approach are discussed in Section 3.

III. The proposed integration framework

In the following, the detailed integration framework for security tool selection is presented. First, we briefly introduce security tool selection criteria and procedures. Next, based on the AHP method, the intermediate score of these criteria is calculated. The QFD is then employed to describe the relationship for mapping between selection criteria and evaluation criteria. Using these intermediate scores, and the relationship mapping of two criteria types as the input of a LFR procedure we compute the dependent function of each evaluation criterion. Finally, PP is used to find the optimal solution; based on this solution we apply an adjusted GP to get the most appropriate security tool.

In order to more easily understand security tool criteria, we can think of the security tool as a product. Therefore, its capability criteria are the product's characteristics and the evaluation criteria can be defined as the customer requirements. These criteria are derived from ([7], [10], [19]) and slightly modified to suitable to our problem and method in this paper. The security tool selection criteria which are defined here include two kinds: capability criteria and evaluation criteria.

- Capability criteria: (1) product architecture, (2) product function, (3) provider's speciality, (4) product performance, (5) product service, and (6) provider's track record or ability;
- Evaluation criteria: (1) quality, (2) credibility of providers, and (3) costs.

More specifically, each capability criteria have their sub-criteria. Detail about them is shown in the Table 1 below [16].

1. Security tool selection criteria and procedure

Table 1. Capability criteria of security tool provider

Criteria	Sub-Criteria
Product architecture	hardware requirements, OS supported, source language, source code available, NOS supported, protocols supported, and component model supported
Product function	prevention, detection, recovery, and corrective
Provider's speciality	security expertise, solution lineup, best practice, and offers turnkey IT security
Produce performance	functionality, reliability, usability, efficiency, maintainability, and portability
Product service	warranty, maintenance, and support services
Provider's track record or ability	market share, certification, geographical coverage, and financial stability

Based on these criteria, the estimations of experts are obtained. Detailed scores of each security tool candidate for each criterion will be summarized by using AHP and the relation among these criteria is shown in the house of quality (HOQ) model. These will be discussed in Section 3.2.

In addition, one important item we need to

specify is a selection procedure. There are many procedures proposed for software, project, system, security control selection ([1], [2], [7], [19]). Each has advantages as well as disadvantages. Based on the advantages of previous models and the characteristics of the security domain, a procedure for security tool selection is proposed. Steps of the section procedure

are as follows:

1. Organize an introduction team
2. Identify evaluation and selection criteria
3. Extract detailed attributes of security tools
4. Collect all security tool alternatives
5. Reduce alternative list and send an invitation to vendors
6. evaluate the Request for Proposal (RFP) responses of vendors
7. Apply optimal selection framework
8. Obtain the most suitable security system.

Based on the security tool selection criteria and procedure which is introduced above, we applied three phases framework for Step 7. This framework helps the DM to select the most suitable security tool for an organization. Further details about these three phases are provided below.

2. Selection preprocess

The AHP, introduced by Saaty [20], addresses the methods for determining the relative importance of a set of factors. The AHP is widely used for tackling MCDM problems in real situations. In this paper, data collected from security experts using a questionnaire is utilized as the input of the AHP procedure to compute the intermediate scores of each selection criterion, as well as evaluation criterion. After applying the AHP we can eliminate the sub-criteria and consider only about the selection criteria. Then, QFD is employed to describe the relationship of the selection criteria and evaluation criteria. In fact, employing QFD here is only for the purpose of easily understanding the relationship among selection criteria, and between the selection criteria and evaluation criteria.

The general format of the HOQ matrix includes six major components: customer requirements, technical measures, relationship matrix, correlation matrix, planning matrix and weight, benchmarks and targets ([21], [22]). From the relationship matrix and correlation matrix we can derive the relationship information, as discussed above, for the next step - fuzzy regression.

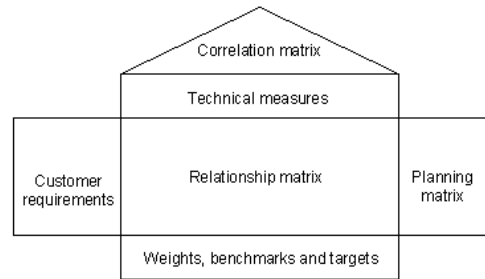


Fig. 2. The house of quality matrix

Fig. 2 helps us to more easily see the relationship among these selection criteria, as well as between the selection criteria and evaluation criteria. In addition, all summarized scores of each alternative are shown, such as the planning matrix and weight, and the benchmarks and targets matrix. These data are used as the input of the fuzzy regression method to compute the regression function of each evaluation criteria.

3. Fuzzy regression

In this section we briefly introduce a LFR and show how to apply this method to our problem. More specifically, we compute the dependent function of each evaluation criterion using the intermediate scores and the relationship mapping of two criteria types from the previous step as the input of a LFR procedure. Because information which is obtained from experts cannot be guaranteed to be exactly correct, we use a fuzzy regression. This method overcomes the problem of noise effect in the input data quite well and has been successfully applied in many engineering domains ([1], [2]).

The linear fuzzy regression model is defined by Tanaka [23] as follow:

$$y = \tilde{A}_0 + \tilde{A}_1 x_1 + \tilde{A}_2 x_2 + \dots + \tilde{A}_n x_n \dots\dots\dots (1)$$

where $\tilde{A}_j = (\alpha_j, c_j)$ is the fuzzy parameter, defined as the symmetrical triangular fuzzy numbers which center α_j and spreads c_j , respectively. The membership function is written as:

$$\mu_{\bar{A}_j}(x) = 1 - \frac{|\alpha_j - x|}{c_j}, \alpha_j - c_j \leq x \leq \alpha_j + c_j \dots\dots (2)$$

$$\mu_{\bar{A}_j}(x) = 0, otherwise$$

Tanaka [24] proposed an optimization model to obtain the fuzzy parameters. Solving this optimization problem, we obtained the regression function of each evaluation criterion, which is defined as a function of independent variables - selection criteria. These resultant dependent functions can be described as follows:

$$y_i = f_i(x_1, x_2, \dots, x_n); i = 1, 2, 3$$

and

$$x_j = g_j(x_1, \dots, x_{j-1}, x_{j+1}, x_n); j = 1, \dots, n \dots\dots\dots (3)$$

At the end of this step we have the above dependent functions. Based on these function, PP is employed to get the most suitable solution for an organization. Details are discussed in the next section.

4. Physical programming for optimization

PP is a new approach to computational design optimization which was recently developed by Messac [25]. PP provides greatly enhances an engineer's ability to obtain an optimal design by employing a flexible and more natural problem formulation framework. One of PP's advantages is the elimination of the need to specify optimization weights by DMs or experts. In this method, they only specify ranges of different degrees of desirability for each design measure. PP is also ideally suited to address the inherent multi-objective nature of decision problem, where multiple conflicting objectives govern the search of the best solution. For these reasons, it has been used primarily and widely in engineering design optimization ([26], [27], [28], [29]).

Within the PP procedure, the DM expresses his preferences with respect to each criterion using four different classes. Fig. 3 above depicts the qualitative meaning of each class. For each class, there are two cases: soft and hard, referring to the details of the

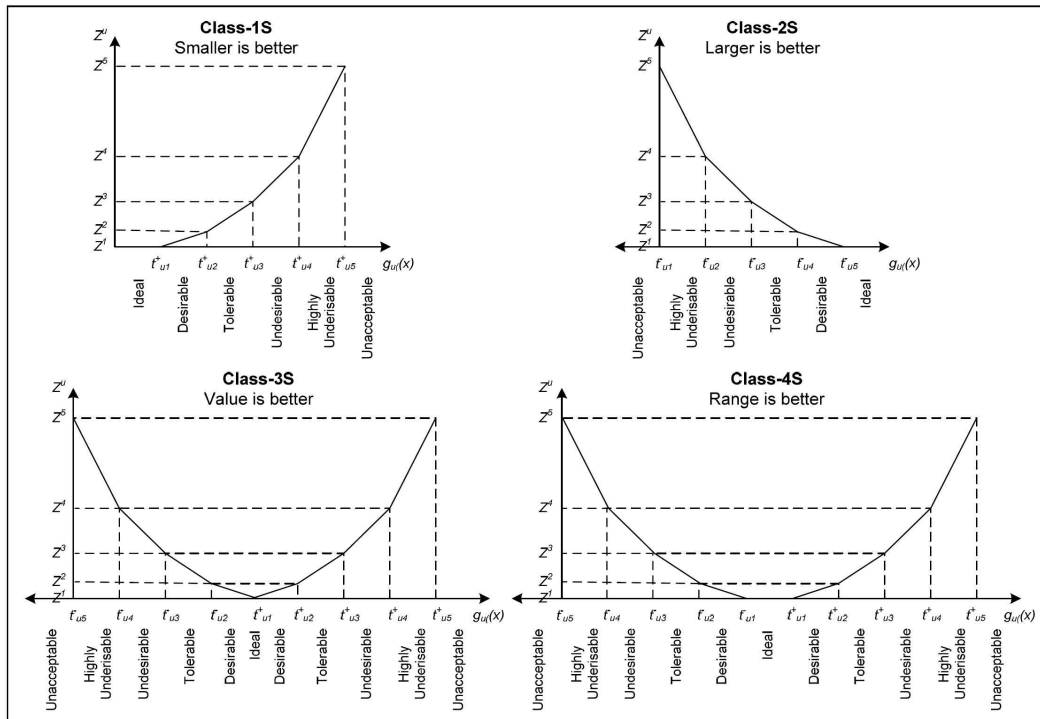


Fig. 3. PP class functions

DM's preference. Here, the decision variable vector is denoted as x , and the u th generic criterion as $g_u(x)$. The value of the criterion under consideration g_u is on the horizontal axis, and the function that will be minimized or maximized for that criterion, z_u hereby called the class function, is on the vertical axis. the desired behavior of generic criterion is described by one of four soft and four hard sub-classes. These classes illustrated in Fig. 3 are soft classes which can be characterized by:

- Class-1S: Smaller-is-better i.e. minimization
- Class-2S: Larger-is-better i.e. maximization
- Class-3S: Value-is-better
- Class -4S: Range-is-better

The PP lexicon comprises terms that characterize the degree of desirability of six ranges for each generic criterion for classes 1S and 2S, ten ranges for classes 3S, and eleven classes for class 4S. To illustrate the PP lexicon, consider the case of class 1S, shown in Fig. 3. In order of decreasing preference, the ranges are defined as follows:

Ideal range ($g_i \leq t_{i1}^+$; Range-1): A range over which every value of the criterion is ideal (the most desirable possible). Any two points of this range are of equal value to the DM:

- Desirable range ($t_{i1}^+ \leq g_i \leq t_{i2}^+$; Range-2): An acceptable range that is desirable;
- Tolerable range ($t_{i2}^+ \leq g_i \leq t_{i3}^+$; Range-3): An acceptable, tolerable range;
- Undesirable range ($t_{i3}^+ \leq g_i \leq t_{i4}^+$; Range-4): A range that, while acceptable, is undesirable;
- Highly undesirable range ($t_{i4}^+ \leq g_i \leq t_{i5}^+$; Range-5): A range that, while still acceptable, is highly undesirable; and
- Unacceptable range ($g_i \geq t_{i5}^+$; Range-6): The range of values that the generic metric may not take.

To evaluate the weights of each generic criterion, a PPW algorithm is applied [25]. After that, the PP problem model can be mathematically expressed as follows:

$$\min J = \sum_{i=1}^{n_c} \sum_{s=2}^5 (\widetilde{w}_{is}^- \widetilde{d}_{is}^- + \widetilde{w}_{is}^+ \widetilde{d}_{is}^+) \dots\dots\dots (4)$$

Subject to

$$\begin{aligned} g_i + d_{is}^- &\geq t_{i(s-1)}^-; & i \text{ in classes: } 2S, 3S, 4S \\ d_{is}^- &\geq 0; & (s = 2, 3, 4, 5; i = 1, 2, \dots, n_c) \\ g_i &\geq t_{i5}^-; \\ g_i - d_{is}^+ &\leq t_{i(s-1)}^+; & i \text{ in classes: } 1S, 3S, 4S \\ d_{is}^+ &\geq 0; & (s = 2, 3, 4, 5; i = 1, 2, \dots, n_c) \\ g_i &\leq t_{i5}^+; \\ x &\in S; \end{aligned}$$

where (d_{is}^-, d_{is}^+) are deviational variables. In our problem, we have three objectives which are quality, credibility and costs. By employing PP, the best solution is found. Then, based on the weights and the optimal solution which is obtained from PP step, weighted goal programming is utilized to specify the most suitable solution for an organization ([25], [30]).

IV. Case study

In this case study, the XYZ Company wants to implement an information security system. There are many candidate products in market for the company to choose from. We consider five candidates which are A1, A2, A3, A4 and A5. Among the many sub-criteria, three most important evaluation criteria are quality, credibility and cost, which must be strictly considered within the selection process. The objective of the project is to determine the most suitable security tool among these candidates which will satisfy the quality, credibility and cost requirements.

1. Preprocess and fuzzy regression phases

In this particular example, there are five security tools are considered to be selected for XYZ Company. As discussed in Section 3, our approach first applies AHP and QFD to obtain the intermediate scores of security tool criteria and the relationship between selection criteria and evaluation criteria, and among selection criteria. The result of these two phases is shown in Fig. 4. In this figure, we can see the

relationship between selection criteria and evaluation criteria in the center matrix. In addition, the relationship among the selection criteria is shown in the angle on the top of Fig. 4. All scores for each selection criteria were normalized to the range between 0 and 100, which means the percentage of perfect

characteristics. But, for fuzzy regression computing purpose, these values are normalized again to fit into the range between 0 and 1. On the right side of Fig. 4 above, the score of each evaluation criteria is set as an integer from 0 to 10, in which “0” is the worst case and “10” is the best of this criterion.

Selection Criteria	Relationship Matrix						Alternatives				
	Architecture	Function	Speciality	Performance	Track Record/Ability	Product Service	A1	A2	A3	A4	A5
Quality	V	V		V		V	7	6	8	7	8
Costs	V	V	V	V		V	8	7	8	7	9
Credibility of provider			V		V		6	8	7	5	8
A1	78	89	95	81	73	74					
A2	80	84	72	85	75	69					
A3	65	75	80	77	82	85					
A4	90	70	66	85	68	68					
A5	70	80	92	76	64	70					

Fig. 4. House of quality mapping selection criteria to evaluation criteria

In order to compute the dependent function of each evaluation criteria, as well as the dependent function among selection criteria, we employ the LFR, which is discussed in Section 3. After applying LFR we obtain the following dependent functions

$$y_i = f_i(x_1, x_2, \dots, x_6); 0 \leq y_i \leq 10; i = 1, 2, 3.$$

$$x_i = g_i(x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_6); 0 \leq x_i \leq 1; i = 1, \dots, 6.$$

..... (5)

where y1, y2, y3, x1, x2, x3, x4, x5, and x6 denote quality, credibility of supplier or vendor, costs, architecture, function, speciality, performance, track record or ability and product service, respectively.

In order to obtain the fuzzy parameters for dependent quality function (y1), the following optimization model [25] needs to be solved.

$$\min Z = 5c_0 + 3.854c_1 + 4.008c_2 + 3.833c_4 + 3.691c_6$$

..... (6)

Subject to

$$Ax^T \leq b^T$$

$$x = [\alpha_0, \alpha_1, \alpha_2, \alpha_4, c_6, c_1, c_2, c_4, c_6]$$

$$b = [-7, -6, -8, -7, -8, 7, 6, 8, 7]$$

$$A = \begin{bmatrix} -a & -0.5a \\ a & -0.5a \end{bmatrix}$$

$$a = \begin{bmatrix} 1 & 0.7805 & 0.8962 & 0.5829 & 0.7493 \\ 1 & 0.8034 & 0.8406 & 0.8572 & 0.6981 \\ 1 & 0.6593 & 0.7565 & 0.7725 & 0.8519 \\ 1 & 0.9021 & 0.7098 & 0.8568 & 0.6835 \\ 1 & 0.7088 & 0.8052 & 0.7633 & 0.7082 \end{bmatrix}$$

$$c_j \geq 0; j = 0, 1, 2, 4, 6;$$

Solving the above optimization problem by MATLAB, the fuzzy regression function of quality aspect is obtained as follows:

$$y_1 = 36.97 - 9.64x_1 - 14.04x_2 - 7.11x_4 - 7.63x_6$$

By applying the same procedure for the other criteria, all parameter estimations are obtained and we summarize all dependent functions of criteria below

$$y_1 = 36.97 - 9.64x_1 - 14.04x_2 - 7.11x_4 - 7.63x_6 \dots\dots\dots (7)$$

$$y_2 = -4.39 + 5.75x_3 + 9.57x_5$$

$$y_3 = -0.43 - 10.33x_1 + 5.19x_2 + 5.86x_3 + 9.71x_4 - 7.63x_6$$

$$x_1 = 1.26 - 0.65x_2$$

$$x_2 = 0.41 + 0.04x_1 + 0.4x_3 + 0.07x_4$$

$$x_3 = 1.12 + 0.43x_2 - 1.03x_4 + 0.28x_5$$

$$x_4 = 1.58 - 0.4x_2 - 0.61x_3$$

$$x_5 = 0.66 - 0.69x_3 + 0.77x_6$$

$$x_6 = 0.59 + 0.23x_5$$

In the next phase, using the information above we apply PP to find the most suitable security tool for XYZ Company.

2. Physical programming phase

Our objectives are to maximize the quality and the credibility of a security tool and minimize its cost. This problem can be defined as multi-objective problem below

- Maximize {Quality of product = y_1 }
- Maximize {Credibility of product = y_2 }
- Minimize {Cost = y_3 }
- Subject to: $f_i(x_j) = 0$; $y_j \in S_j$; $x_j \in S_x$

In this paper, PP is employed to solve the above problem. We first apply PP to find out the optimal solution (y_i^*, x_j^*). Then, we combine the advantage of PP and GP to find the most suitable security tool among these candidate products. More specifically, optimal solution (y_i^*, x_j^*) is set as the target solution for GP and the PPW procedure is used to obtain the weight of each goal.

First, the review team or DMs decide the range for each goal based on the views and requirements of the company for the selected security tool. The value of each goal is between 0 and 100, where "100" is the highest value and "0" is the lowest value. In sum, the range limits for each goal are shown in Tables 2, 3, and 4.

Table 2. Range limits for quality goal

Objective Function 1: Quality			
Class-2S: Larger is better			
Preference Level	Ranges	Lower Limits	Values
Ideal	$\geq t_{11}^-$	t_{11}^-	95
Desirable	(t_{12}^-, t_{11}^-)	t_{12}^-	75
Tolerable	(t_{13}^-, t_{12}^-)	t_{13}^-	65
Undesirable	(t_{14}^-, t_{13}^-)	t_{14}^-	60
Highly undesirable	(t_{15}^-, t_{14}^-)	t_{15}^-	50
Unacceptable	$\leq t_{15}^-$		

Table 3. Range limits for credibility goal

Objective Function 2: Credibility of Provider			
Class-2S: Larger is better			
Preference Level	Ranges	Lower Limits	Values
Ideal	$\geq t_{21}^-$	t_{21}^-	90
Desirable	(t_{22}^-, t_{21}^-)	t_{22}^-	80
Tolerable	(t_{23}^-, t_{22}^-)	t_{23}^-	70
(8) Undesirable	(t_{24}^-, t_{23}^-)	t_{24}^-	60
Highly undesirable	(t_{25}^-, t_{24}^-)	t_{25}^-	50
Unacceptable	$\leq t_{25}^-$		

Table 4. Range limits for costs goal

Objective Function 3: Costs			
Class-1S: Smaller is better			
Preference Level	Ranges	Lower Limits	Values
Ideal	$\leq t_{31}^+$	t_{31}^+	30
Desirable	(t_{31}^+, t_{32}^+)	t_{32}^+	50
Tolerable	(t_{32}^+, t_{33}^+)	t_{33}^+	60
Undesirable	(t_{33}^+, t_{34}^+)	t_{34}^+	70
Highly undesirable	(t_{34}^+, t_{35}^+)	t_{35}^+	80
Unacceptable	$\geq t_{35}^+$		

Then, applying the PPW algorithm, all weights will be obtained as shown in Table 5.

Table 5. Normalized weights calculated by using PPW procedure

Target	i	Normalized Weights			
		\widetilde{w}_{i2}	\widetilde{w}_{i3}	\widetilde{w}_{i4}	\widetilde{w}_{i5}
Quality	1	0.049	0.168	0.737	0.095
Credibility	2	0.104	0.124	0.255	0.602
Costs	3	0.052	0.176	0.255	0.602

Applying PP, our problem can be rewritten as follows:

$$\min_{\widetilde{d}_s, \widetilde{d}_{3s}^+, x} J = \sum_{s=2}^5 (\widetilde{w}_{1s} \widetilde{d}_{1s}^- + \widetilde{w}_{2s} \widetilde{d}_{2s}^- + \widetilde{w}_{3s} \widetilde{d}_{3s}^-)$$

Subject to

$$g_1 + \widetilde{d}_{1s}^- \geq \widetilde{t}_{1(s-1)}^-; \widetilde{d}_{1s}^- \geq 0; g_1 \geq \widetilde{t}_{15}^-; s = 2, 3, 4, 5 \dots (9)$$

$$g_2 + \widetilde{d}_{2s}^- \geq \widetilde{t}_{2(s-1)}^-; \widetilde{d}_{2s}^- \geq 0; g_2 \geq \widetilde{t}_{25}^-; s = 2, 3, 4, 5$$

$$g_3 + \widetilde{d}_{3s}^- \leq \widetilde{t}_{3(s-1)}^-; \widetilde{d}_{3s}^- \geq 0; g_3 \leq \widetilde{t}_{35}^-; s = 2, 3, 4, 5$$

$$y_1 = 36.97 - 9.64x_1 - 14.04x_2 - 7.11x_4 - 7.63x_6$$

$$y_2 = -4.39 + 5.75x_3 + 9.57x_5$$

$$y_3 = -0.43 - 10.33x_1 + 5.19x_2 + 5.86x_3 + 9.71x_4 - 7.63x_6$$

$$x_1 = 1.26 - 0.65x_2$$

$$x_2 = 0.41 + 0.04x_1 + 0.4x_3 + 0.07x_4$$

$$x_3 = 1.12 + 0.43x_2 - 1.03x_4 + 0.28x_5$$

$$x_4 = 1.58 - 0.4x_2 - 0.61x_3$$

$$x_5 = 0.66 - 0.69x_3 + 0.77x_6$$

$$x_6 = 0.59 + 0.23x_5$$

$$0 \leq y_i \leq 10; i = 1, 2, 3;$$

$$0 \leq x_j \leq 1; j = 1, 2, \dots, 6;$$

$$g_i = 10y_i; i = 1, 2, 3.$$

We used the MATLAB system to solve the above problem. The results obtained are as follows:

$$(y_1, y_2, y_3) = (8.241, 6.268, 3.582);$$

$$(x_1, x_2, x_3, x_4, x_5) = (0.677, 0.878, 1, 0.624, 0.514, 0.7$$

$$(\widetilde{d}_{12}^-, \widetilde{d}_{13}^-, \widetilde{d}_{14}^-, \widetilde{d}_{15}^-) = (12.6, 0, 0, 0);$$

$$(\widetilde{d}_{22}^-, \widetilde{d}_{23}^-, \widetilde{d}_{24}^-, \widetilde{d}_{25}^-) = (27.317, 17.32, 7.317, 0); \text{and}$$

$$(\widetilde{d}_{32}^+, \widetilde{d}_{33}^+, \widetilde{d}_{34}^+, \widetilde{d}_{35}^+) = (5.823, 0, 0, 0).$$

Next, to avoid the ambiguous and incorrect computation of each objective weight, in this step we use the weights which are obtained from PPW algorithm. The optimal solution (y_i^*, x_j^*) is set as the target solution. In this, we overcome two weak points of weighted GP, which are determination of weight and suitable target value for each goal. Now our problem is described as follows

$$\min w_q(\widetilde{d}_1^+, \widetilde{d}_1^-) + w_{cr}(\widetilde{d}_2^+, \widetilde{d}_2^-) + w_{co}(\widetilde{d}_3^+, \widetilde{d}_3^-) \dots (10)$$

Subject to

$$7\gamma_1 + 6\gamma_2 + 8\gamma_3 + 7\gamma_4 + 8\gamma_5 - \widetilde{d}_1^+ + \widetilde{d}_1^- = 8.241;$$

$$6\gamma_1 + 8\gamma_2 + 7\gamma_3 + 5\gamma_4 + 8\gamma_5 - \widetilde{d}_2^+ + \widetilde{d}_2^- = 6.268;$$

$$4\gamma_1 + 5\gamma_2 + 5\gamma_3 + 3\gamma_4 + 6\gamma_5 - \widetilde{d}_3^+ + \widetilde{d}_3^- = 3.582;$$

$$\gamma_i \in 0, 1;$$

$$i = 1, 2, \dots, 5;$$

$$\sum_{i=1}^5 \gamma_i = 1;$$

$$w_q = \widetilde{w}_{12}^-;$$

$$w_{cr} = \widetilde{w}_{24}^-; \text{ and}$$

$$w_{co} = \widetilde{w}_{32}^+.$$

Using the MATLAB software package, the result obtained is: $(\gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5) = (1, 0, 0, 0, 0)$. The result means that the security tool A1 is the most suitable for the XYZ Company. This result is reasonable and appropriate with the real result and is the evidence of the correctness of our approach. Detailed discussion of this result is presented in the following sub-section.

3. Result discussions

After collecting information from experts' estimations and applying AHP to gain the intermediate scores for six main selection criteria of each security tool, we can have an overview of these tools by looking at the Fig. 5 below. We can see that A1 security tool is slightly higher compared to the others. However, it is still very hard to determine exactly which tool is the most appropriate for an organization. If each expert focuses on different factors, the result will be different. From that observation, we recommend a three-step integrated framework for helping the DM select a security tool is proposed.

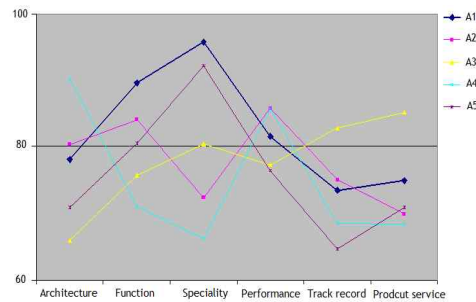


Fig. 5. Synthesis intermediate score at each main selection criterion of five security tools

To evaluate and ensure this methodology, we tried to compare the result of our approach with a real result obtained from the opinions of professional security consultants and security planners. Our results are similar to the real-world results in most instances, which show that our results reflect what happens in the real world. In addition, we believe that careful application of three-step can be widely applied, due to their usefulness and simple implementation.

V. Conclusion

The Internet and local area networks, which are growing rapidly, have witnessed an increase in malicious attacks. In addition, the importance of information systems and the increasing dependence of companies on such systems have made them vulnerable targets for attackers. For these reasons, many companies consider deploying a security system. To help a DM select a suitable security tool, this paper proposes a three-step integrated framework using fuzzy regression and PP.

First, based on the security criteria and expert's estimations, AHP and QFD are employed to specify the intermediate score of each criterion and the relationship among these criteria. Next, the dependent function of each evaluation criterion is computed by employing LFR. By using LFR to specify the estimation function, the vagueness and noise from experts' data are reduced. Then, in order to achieve a balance among multi-objectives, of quality, credibility and costs, PP is utilized to find the optimal solution. Finally, setting the optimal solution as a target solution and using weights calculated by PPW algorithm in the previous step, we apply the GP method to obtain the most appropriate security tool for an organization. To evaluate this approach, a case study example was presented and the result demonstrated its practical value.

The implications of this approach are:

- it takes the advantages of experts' experience;
- it considers diverse perspectives of previous

works to design standard security criteria; and

- it adopts mathematic optimization methods to improve the accuracy and reliability of decision process and results

Limitations and further research issues are summarized as follows:

- the security criteria of each specific type of security tools should be studied;
- the accuracy of the preprocess phase might be improved by considering the dependence among the security criteria;
- a multi-level framework based on the level of accuracy requirements of the selection process could be designed; and
- case studies which show the practical value of this framework and provide the reference models of application should be conducted.

Acknowledgement

This work was supported by the Korea Science and Engineering Foundation (KOSEF) grant funded by the Korea government (MOST) (No. R01-2007-000-21070-0). This work was also supported by the Korea Research Foundation Grant funded by the Korean Government(MEST) (KRF-2008-211-D00084).

References

- [1] E. Eetugrul Karsak, and C. Okan Ozogul, "An Integrated Decision Making Approach for ERP System Selection," *Expert Systems with Applications*, Vol. 36, No. 1, pp. 660-667, January 2009.
- [2] H.Y. Lin, P.Y. Hsu, and G.J. Sheen, "A Fuzzy-Based Decision-Making Procedure for Data Warehouse System Selection," *Expert Systems with Applications*, Vol. 32, No. 3, pp. 939-953, April 2007.
- [3] M.J. Schniederjans, and R.L. Wilson, "Using the Analytic Hierarchy Process and Goal Programming for Information System Project Selection,"

- Information and Management, Vol. 20, No. 5, pp. 333 - 342, May 1991.
- [4] M. Monheit, and A. Tsafirir, "Information Systems Architecture: a Consulting Methodology," *Proceeding of the 1990 IEEE International Conference on Computer Systems and Software Engineering*, Tel Aviv, Israel, 1990, pp. 568-572.
- [5] E.E. Anderson, and J. Choobineh, "Enterprise Information Security Strategies," *Computers & Security*, Vol. 27, No.1-2, pp. 22-29, March 2008.
- [6] M. Choi, and S. Shin, "Optimizing Quality Levels and Development Costs for Developing an Integrated Information Security System," *Information Security Applications*, edited by C. H. Lim and M. Yung, Vol. 4867, Lecture Notes in Computer Science, Springer, 2008, pp. 359-370.
- [7] S. Kim, and H.J. Lee, "A Study on Decision Consolidation Methods Using Analytic Models for Security Systems," *Computers & Security*, Vol. 26, No. 2, pp. 145 - 153, March 2007.
- [8] P. Kongsuwan, S. Shin, and M. Choi, "Managing Quality Level for Developing Information Security System Adopting QFD," *Proceeding of 2008 Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, Phuket, Thailand, 2008, pp. 19-24.
- [9] C.S. Leem, and S. Kim, "Introduction to an Integrated Methodology for Development and Implementation of Enterprise Information Systems," *Journal of Systems and Software*, Vol. 60, No. 3, pp. 249 - 261, February 2002.
- [10] H.V. Nguyen, S. Shin, and Y. Choi, "An integrated approach to the optimal selection of security tools using analytic hierarchy process and goal programming," *International Journal of Technology Management*, accepted for publication, 2009.
- [11] T. Tsiakis, and G. Stephanides, "The Economic Approach of Information Security," *Computers & Security*, Vol. 24, No. 2, pp. 105-108, March 2005.
- [12] ISO/IEC 15408-1:2005, http://www.iso.org/iso/catalogue_detail.htm?csnumber=40612.
- [13] EC advisory group SOG-IS, "Information Technology Security Evaluation Criteria (ITSEC)," Version 1.2, the Department of Trade and Industry, London, June 1991.
- [14] Department of Defense Standard, "Department of Defense Trusted Computer System Evaluation Criteria," DoD 5200.28-STD, December, 1985.
- [15] R. Hefner, and W. Monroe, "System Security Engineering Capability Maturity Model," *Proceeding of Conference on Software Process Improvement*, UC Irvine, USA, 1997.
- [16] M. Eloff, and S.H. Solms, "Information Security Management, Hierarchical Framework for Various Approaches," *Computers & Security*, Vol. 19, No. 3, pp. 243 - 256, March 2000.
- [17] W.T. Polk, "Guide to the Selection of Anti-Virus Tools & Techniques", Diane Books Publishing Company, 1992.
- [18] R. Firth, B. Fraser, S. Konda, and D. Simmel, "An Approach for Selecting and Specifying Tools for Information Survivability", Carnegie Mellon University, July 1998.
- [19] ISO/IEC 9126-1:2001, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=22749
- [20] T.L. Saaty, "A Scaling Method for Priorities in Hierarchical Structures," *Journal of Mathematical Psychology*, Vol. 15, No. 3, pp. 234 - 281, June 1977.
- [21] S. Chakraborty, and S. Dey, "QFD-Based Expert System for Non-Traditional Machining Processes Selection," *Expert Systems with Applications*, Vol. 32, No. 4, pp. 1208-1217, May 2007.
- [22] L. Chan, and M. Wu, "Quality Function Deployment: a Literature Review," *European Journal of Operational Research*, Vol. 143, No. 3, pp. 463-497, December 2002.
- [23] H. Tanaka, S. Uejima, and K. Asai, "Linear Regression Analysis with Fuzzy Model," *IEEE Transactions on Systems, Man, and Cybernetics*, Vol. 12, No. 6, pp. 903 - 907, November 1982.

[24] H. Tanaka, and J. Watada, "Possibilistic Linear Systems and Their Application to the Linear Regression Model," *Fuzzy Sets and Systems*, Vol. 27, No. 3, pp. 275 - 289, September 1988.

[25] A. Messac, S.M. Gupta, and B. Akbulut, "Linear Physical Programming: a New Approach to Multiple Objective Optimization," *Transactions on Operational Research*, Vol. 8, No. 1, pp. 39-59, October 1996.

[26] W. Chen, A. Sahai, A. Messac, and G.J. Sundararaj, "Exploration of the Effectiveness of Physical Programming in Robust Design," *ASME Journal of Mechanical Design*, Vol. 122, No. 2, pp.155-163, June 2000.

[27] E. Kongar, and S.M. Gupta, "Disassembly-to-Order System Using Linear Physical Programming," *Proceeding of IEEE International Symposium in Electronics and the Environment*, San Francisco CA, USA, 2002, pp. 312-317.

[28] E. Melachrinoudis, A. Messac, A. H. Min, "Consolidating a Warehouse Network: a Physical Programming Approach," *International Journal of Production Economics*, Vol. 97, No. 1, pp. 1-17, July 2005.

[29] M. Patel, K.E. Lewis, A. Maria, and A. Messac, "System Design through Subsystem Selection Using Physical Programming," *AIAA Journal*, Vol. 41, No. 6, pp. 1089-1096, June 2003.

[30] M.J. Schniederjans, "Linear Goal Programming", Petrocelli Books, 1984.

저 자 소 개



Hoai-Vu Nguyen
 2005 : Hanoi공대 공학사
 2009 : 인제대학교 공학석사
 2009 - 현재 :
 베트남 FPT대, Computer기초학과강사
 관심분야 : 정보보호, 정보시스템,
 소프트웨어공학



Pauline Kongsuwan
 2004 : 태국 Kasetsart University 공학사
 2009 : 인제대학교 공학석사
 2010 - 현재 : 인제대학교 정보통신 시스템학과 박사과정
 관심분야 : 정보보호, 정보시스템, 소프트웨어공학, 품질경영



신 상 문
 2002 : Clemson University 공학 석사
 2005 : Clemson University 공학 박사
 2005 - 현재 : 인제대학교 시스템경영 공학과 조교수
 관심분야 :
 Information management,
 robust design,
 multi-objective optimization



최 용 선
 1986 : 서울대학교 공학사
 1988 : KAIST 공학석사
 1993 : KAIST 공학박사
 1993 - 현재 : 인제대학교 시스템경영 공학과 교수
 관심분야 : 정보시스템, 통신망설계, 지리정보시스템



김 상 군
 1998 : 연세대학교 공학석사
 2005 : 연세대학교 공학박사
 2007-현재 : 강원대학교 산업공학과 교수
 관심분야 : 기술경영, 산업정보보호, 정보공학