International Journal of Innovative Computing, Information and Control
Volume **11**, Number **6**, December **2015**

ICIC International ©2015 ISSN 1349-4198
pp. 2177–2191

A SIMILARITY-BASED M(1, 2, 3) APPROACH AND ITS APPLICATION IN RATING THE SECURITY OF NETWORK SYSTEMS

Junhu Ruan[1,4], Takashi Samatsu[2] and Yan Shi[3,4]

[1]College of Economics and Management
Northwest A&F University
No. 3, Taicheng Road, Yangling 712100, P. R. China
rjh@nwsuaf.edu.cn

[2]School of Industrial and Welfare Engineering
[3]General Education Center
Tokai University
9-9-1, Toroku, Higashi-ku, Kumamoto 862-8652, Japan
samatsu@tokai.ac.jp; yshi@ktmail.tokai-u.jp

[4]Institute of Systems Engineering
Dalian University of Technology
No. 2, Linggong Road, Dalian 116023, P. R. China

Received June 2015; revised October 2015

Abstract. *The security of network systems is one of the most important issues in the era of information, and it is a multiple criteria problem to evaluate the security of information networks. Many evaluation approaches have been reported in the literature. However, one key issue not fully considered in extant studies is how to obtain the values of these multiple evaluation criteria, and in most evaluation models some redundant criteria values are calculated. Motivated by these observations, in the work we first use the pairwise comparison method to attain the values of each evaluation aspect of the security of information networks, and then develop a novel similarity-based M(1, 2, 3) approach to rate the security of alternative networks. Application study shows that the proposed approach could rate the overall security of alternative information networks and recognize the most vulnerable aspects of each information network, which provides good supports for making policies to enhance the security of alternative information networks.*

Keywords: Network systems, Security evaluation, Similarity-based M(1, 2, 3)

1. Introduction.

In the era of information and network, almost all commercial organizations are communicating and operating their businesses through internal and external information networks. One common issue these organizations attach great importance to is the security of their information networks through which they make online confidential operations every day. Any breach of network security may result in substantial losses for the businesses [1]. Thus, many security techniques such as firewalls, virus protection, intrusion detection and security authentication have been developed by practitioners for helping their customers build secure and reliable information networks.

Meanwhile, researchers and scholars are also making their efforts to study on how to build secure networks, and how to evaluate and enhance the security of information networks. Consequently, a plenty of protocols, algorithms and other security techniques have been reported, as the following review work summarized. Skoularidou and Spinellis [2] presented a reference monitor security model to analyze security architectures for network clients, and observed meaningful insights from the aspects of firewall vendors, code signing, and smart cards. Sharma et al. [3] gave a review on the security frameworks for wireless sensor networks from the aspects of symmetric cryptographic techniques, asymmetric cryptographic techniques and hybrid cryptographic techniques. Geravand and Ahmadi [4] made an up-to-date survey of the application of Bloom filters and their variants which are used to address security problems with different types of networks. Steenbruggen et al. [5] reviewed the possibilities opened up by the use of location based services within the domain of transport safety and security. Specifically, recent studies dealt with the network security based on the reliability engineering [6,7]. Islam et al. [6] analyzed the challenges of wireless sensor networks from the aspect of reliability and security, and examined the effectiveness of extant solution measures, which gave out some interesting research directions. Kondakci [7] mentioned that the reliability engineering is a general concept in the analysis of network security, and many extant studies on network security could be included in the framework. The applicability of reliability engineering is due to the complexity involved in dealing with the network security. Besides the general studies on network security based on reliability engineering, extensive specific contributions have also been made. Readers could refer to [7] for details.

In this work, we focus on how to evaluate the security of information networks, so here some related studies on the evaluation of network security are reviewed in detail. Chang and Hung [8] stated that the evaluation of alternative network security systems is with multiple and imprecise criteria, and they developed an algorithm which uses the fuzzy weighted average approach to deal with the fuzzy numbers and obtain the fuzzy weighted averages for evaluating the security of network systems. Li et al. [9] first used the pure linguistic weighted arithmetic averaging operator to aggregate the linguistic information corresponding to each alternative and get the overall value of the alternatives, and then ranked the security of the alternative network systems. Meanwhile, Zhang [10] also thought comprehensive evaluation model for computer network security is a group decision-making problem, and established an optimization model based on the basic ideal of traditional TOPSIS (The Technique for Order of Preference by Similarity to Ideal Solution) to determine the attribute weights. Liu and Zhang [11] stated that IT management must identify and assess vulnerabilities across many disparate hardware and software platforms to prioritize these vulnerabilities, and proposed a method for qualitative rating and quantitative scoring vulnerabilities. Malavenda et al. [12] presented an approach to analyze the security of wireless sensor networks, based on the regulations intended for wireless communication devices.

As we can see, almost all extant studies on the evaluation of network security stated that it is a multi-attribute decision making (MADM) problem to evaluate the security of information networks. However, one key issue which is not fully considered in above studies is how to obtain the values of these multiple evaluation criteria. When facing a group of alternative information networks, it is necessary to properly quantify the judgment of experts, and it is often easier for decision-makers to judge which one of two alternatives is better than to judge which one of many alternatives is the best. Meanwhile, most of extant evaluation methods did not give enough consideration on the redundancy among evaluation index values. Actually, not all evaluation index values play identical roles for evaluating the objects, according to information entropy theory. In Jiang and Ruan's work [13], they presented an $\mathrm{M}(1,2,3)$ algorithm which could effectively reduce the redundant index values in the evaluation process. However, the classic $\mathrm{M}(1,2,3)$ algorithm does not consider how to attain the evaluation index values, and needs the criterion values of each index, which result in weak feasibility and operability in real world applications.

Motivated by these observations, we first use the pairwise comparison method to attain the values of each evaluation aspect of the security of information networks, and then develop a similarity-based $\mathrm{M}(1,2,3)$ approach to rate the security of alternative networks. Application study shows that the proposed approach could rate the overall security of alternative information networks and recognize the most vulnerable aspects of each information network. The integrated approach could be used to not only attain the evaluation index values but also reduce the redundant data in the evaluation of network security, which also provides a general evaluation technique for other kinds of multi-attribute decision making problems.

The rest of this paper is organized as follows. Section 2 briefly reviews the preliminaries of the work. In Section 3, we develop an integrated similarity-based $\mathrm{M}(1,2,3)$ approach for rating the security of information networks, including problem definition, the proposed approach, and the framework of the proposed approach. In Section 4, we apply the proposed approach to evaluate and rate the security of 10 information networks in one real-world organization, which shows the effectiveness of the proposed approach. Section 5 concludes the work and gives some future directions.

2. The Preliminaries.

2.1. Fuzzy logic and membership functions.

Fuzzy set theory was first proposed by Zadeh in 1965 [14], which is the theoretical basis of fuzzy logic. In the real world, people often face problems with imprecise and uncertain information, which are impossible or difficult for classical set theory to solve [15]. Specifically, in the evaluation of network security, it is easier for evaluators to use fuzzy values to judge the possible range of each index, due to the uncertainty in the actual process.

In traditional set theory, an element in one universal set either belongs to a set or does not. Fuzzy set theory allows an element in universal set to partially belong to a fuzzy set. The membership function is one key concept in fuzzy set theory, which is used to represent the degrees of one element belonging to one fuzzy set. For any set, a normal membership function on the set is any function from the set to the real unit interval $[0,1]$, so the membership of one element is between 0 and 1. For example, evaluators use the hundred-mark system to score the security of one alternative network as $[80,85,90]$. By the normal membership function, both the memberships of 80 and 90 are 0, and the membership of 85 is 1.

2.2. Existing $\mathbf{M(1,2,3)}$.

As mentioned in the Introduction, most extant evaluation methods do not give enough consideration to the redundancy among evaluation index values. Jiang and Ruan [13] presented an $\mathrm{M}(1,2,3)$ algorithm which could effectively reduce the redundant index values in the evaluation process. Here we give a brief review on the existing $\mathrm{M}(1,2,3)$.

Suppose that there are m indexes which affect evaluation object Q, where the importance weight $\lambda_j(Q)$ of index j $(j = 1 \sim m)$ about object Q is given and satisfies:

$$0 \le \lambda_j(Q) \le 1, \quad \sum_{j=1}^{m} \lambda_j(Q) = 1 \tag{1}$$

Every index is classified into p classes. C_k represents the kth class and C_k is prior to C_{k+1}. The membership $\mu_{jk}(Q)$ of the jth index belonging to C_k is given, where $k = 1 \sim p$ and $j = 1 \sim m$, and $\mu_{jk}(Q)$ satisfies:

$$0 \le \mu_{jk}(Q) \le 1, \quad \sum_{k=1}^{P} \mu_{jk}(Q) = 1 \tag{2}$$

To determine the membership $\mu_k(Q)$ of object Q belonging to C_k, Jiang and Ruan [13] presented an $\mathrm{M}(1,2,3)$ algorithm as follows.

Definition 2.1. *If $\mu_{jk}(Q)$ $(k = 1 \sim p,\ j = 1 \sim m)$ is the membership of the jth index belonging to C_k and satisfies Equation (2), then we define $\alpha_j(Q)$ as the distinguishable weight of the jth index corresponding to Q by the following equations:*

$$H_j(Q) = -\sum_{k=1}^{p} \mu_{jk}(Q) \cdot \log\mu_{jk}(Q) \tag{3}$$

$$v_j(Q) = 1 - \frac{1}{\log p} H_j(Q) \tag{4}$$

$$\alpha_j(Q) = \nu_j(Q) \Big/ \sum_{t=1}^{m} \nu_t(Q) \quad (j = 1 \sim m) \tag{5}$$

Definition 2.2. *If $\mu_{jk}(Q)$ $(k = 1 \sim p,\ j = 1 \sim m)$ is the membership of the jth index belonging to C_k and satisfies Equation (1), and $\alpha_j(Q)$ is the distinguishable weight of the jth index corresponding to Q, then*

$$\alpha_j(Q) \cdot \mu_{jk}(Q) \quad (k = 1 \sim p) \tag{6}$$

is called effective distinguishable value of the kth class membership of the jth index, or the kth class effective value for short.

Definition 2.3. *If $\alpha_j(Q) \cdot \mu_{jk}(Q)$ is the kth class effective value of the jth index, and $\lambda_j(Q)$ is importance weight of the jth index related to object Q, then*

$$\lambda_j(Q) \cdot \alpha_j(Q) \cdot \mu_{jk}(Q) \quad (k = 1 \sim p) \tag{7}$$

is called comparable effective value of the kth class membership of the jth index, or the kth class comparable value for short.

Definition 2.4. *If $\lambda_j(Q) \cdot \alpha_j(Q) \cdot \mu_{jk}(Q)$ is the kth class comparable value of the jth index of Q, where $(j = 1 \sim m)$, then*

$$M_k(Q) = \sum_{j=1}^{m} \lambda_j(Q) \cdot \alpha_j(Q) \cdot \mu_{jk}(Q) \quad (k = 1 \sim p) \tag{8}$$

is named the kth class comparable sum of object Q.

Definition 2.5. *If $M_k(Q)$ is the kth class comparable sum of object Q, and $\mu_k(Q)$ is the membership of object Q belonging to C_k, then*

$$\mu_k(Q) \overset{\Delta}{=} M_k(Q) \Big/ \sum_{t=1}^{p} M_t(Q) \quad (k = 1 \sim p) \tag{9}$$

The above membership transformation method can be summarized as "effective, comparison and composition", which is denoted as $\mathrm{M}(1,2,3)$. Using $\mathrm{M}(1,2,3)$, we could reduce the redundancy among the evaluation index values when determining the membership $\mu_k(Q)$ of object Q belonging to C_k. $\mathrm{M}(1,2,3)$ has been used in various fields such as network security evaluation [13], emergency path selection [16], and supplier performance evaluation [17]. As one continuation to [13], in this work we integrate the $\mathrm{M}(1,2,3)$ algorithm with the pairwise comparison method and similarity measurement method, to develop a similarity-based $\mathrm{M}(1,2,3)$ approach.

3. The Proposed Approach.

3.1. Problem definition.

Assume that there are n information networks $\{N_1, N_2, \ldots, N_n\}$, and decision-makers are considering the following three aspects to rate the security of these n information networks (Note that our approach is not subject to the number of evaluation indexes, that is, it is also effective for more evaluation indexes).

F_1: The security of the persons involved in the network. The persons involved in the network include the development and construction personnel of the network, the management and operation personal of the network, and the confidentiality management regulations for the related personal.

F_2: The security of the network itself. The aspect involves the security of the software and hardware used in the network, such as the firewall technology applied in the network, and the data encryption mechanism.

F_3: The security of the environment where the network locates in. It is important to locate the information networks in a safe environment, in order to avoid the physical accession of potential invaders.

The objective of the decision-making is to rank these n information networks from the most secure to the most insecure, and identify the most vulnerable aspects for each network.

3.2. A novel similarity-based M(1, 2, 3) approach for rating network security.

As we can see, all the three aspects are qualitative factors, which need to be qualified properly. It is easier for decision-makers to judge which one of two alternatives is better than the other, so we use the pairwise comparison to obtain the values of the three aspects for each information network.

In terms of any of the three aspects F_j, the preference of information network N_i over N_l (denoted by x_{il}^j) is measured by one integer number from 1 to 9. The detailed meanings of the nine numbers are as Table 1 shows.

Table 1. The 1-9 comparative scales

Scales	Meanings
$x_{il}^j = 1$	N_i is as safe as N_l in terms of aspect F_j
$x_{il}^j = 3$	N_i is a little safer than N_l in terms of aspect F_j
$x_{il}^j = 5$	N_i is obviously safer than N_l in terms of aspect F_j
$x_{il}^j = 7$	N_i is strongly safer than N_l in terms of aspect F_j
$x_{il}^j = 9$	N_i is extremely safer than N_l in terms of aspect F_j
Note that 2, 4, 6, 8 are the medians of the above judgments, and $x_{li}^j = 1/x_{il}^j$	

Using the above 1-9 comparative scales in Table 1, we can obtain all the comparative values x_{il}^j $(i, l = 1, 2, \ldots, n;\ j = 1, 2, 3)$. However, the comparative value x_{il}^j denotes the preference of information network N_i over only N_l in terms of index F_j. In order to determine the preference of information network N_i over all other information networks, we give the following definition.

Definition 3.1. *The preference of information network N_i over all other information networks in terms of index F_j (denoted by x_i^j) is the summation of the comparative value*

x_{il}^j *for* $l = 1, 2, \dots, n$ *except* $l = i$*:*

$$x_i^j = \sum_{\substack{l=1 \\ l \neq i}}^{n} x_{il}^j, \quad \forall j \in \{1, 2, 3\} \tag{10}$$

In order to evaluate information networks in terms of all the three aspects $\{F_1, F_2, F_3\}$, we should know what are the most secure and insecure information networks. However, there are no standards of the most secure and insecure information networks because any most secure and insecure things are often measured by comparison. Motivated by our previous work [16], we define the most secure and insecure information networks according to all the alternative information networks.

Definition 3.2. *The most secure information network is the information network made up of the most secure aspects among all the alternative information networks, that is,*

$$N^* = \left\{(x^1)^*, (x^2)^*, (x^3)^*\right\} \tag{11}$$

where $(x^j)^* = f_{best}\left(x_1^j, x_2^j, \dots, x_n^j\right)$, $j = 1, 2, 3$.

Definition 3.3. *The most insecure information network is the information network made up of the most insecure aspects among all the alternative information networks, that is,*

$$N_* = \left\{(x^1)_*, (x^2)_*, (x^3)_*\right\} \tag{12}$$

where $(x^j)_* = f_{worst}\left(x_1^j, x_2^j, \dots, x_n^j\right)$, $j = 1, 2, 3$.

As we can see, the most secure and insecure information networks are made up of the most secure and insecure aspects respectively, so they may be virtual information networks because different information networks often have their own advantages. After we determine the most secure and insecure information networks, we can measure the relative similarity of any aspect of the information networks to the most secure and insecure aspects.

Definition 3.4. *The relative similarity of any aspect of some information network to the most secure and insecure aspects is equivalent to*

$$q_i^j = \frac{x_i^j - (x^j)_*}{(x^j)^* - (x^j)_*} \tag{13}$$

Assume that the importance weight $\lambda_j(N)$ of F_j $(j = 1, 2, 3)$ about the overall security of the information network is given and satisfies:

$$0 \leq \lambda_j(N) \leq 1, \quad \sum_{j=1}^{3} \lambda_j(N) = 1 \tag{14}$$

Every evaluation aspect is classified into 5 ordered levels: very secure (C_1), secure (C_2), general (C_3), insecure (C_4) and very insecure (C_5). The membership μ_{jk} of the jth evaluation aspect belonging to C_k is given, where $k = 1, 2, \dots, 5$ and $j = 1, 2, 3$, and μ_{jk} satisfies:

$$0 \leq \mu_{jk} \leq 1, \quad \sum_{k=1}^{5} \mu_{jk} = 1 \tag{15}$$

Seen from Equation (13), we can find the relative similarity of any aspect of some information network is more than or equal to 0 and is less than or equal to 1, that is, $0 \leq q_i^j \leq 1$, so in the work we assign the five ordered levels as five ordered values between

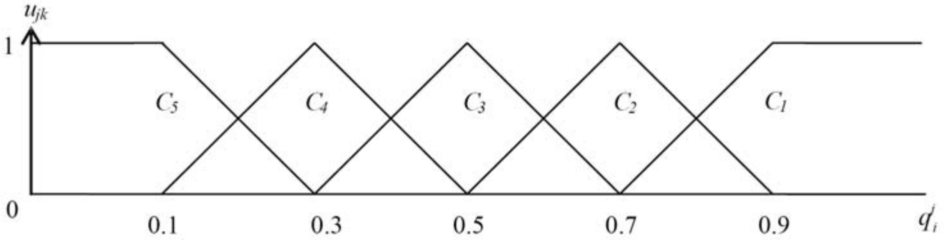

FIGURE 1. The membership functions of the five ordered levels

0 and 1: 0.9 (C_1, very secure), 0.7 (C_2, secure), 0.5 (C_3, general), 0.3 (C_4, insecure), 0.1 (C_5, very insecure). Their membership functions are as Figure 1 shows.

The calculation equation of the memberships is as follows:

$$u_{jk} = \begin{cases} 1 \text{ or } 0, & 0 \le q_i^j \le 0.1 \\ \frac{q_i^j - a_1}{a_2 - a_1}, & 0.1 \le a_1 \le q_i^j \le a_2 \le 0.9 \\ \frac{a_3 - q_i^j}{a_3 - a_2}, & 0.1 \le a_2 \le q_i^j \le a_3 \le 0.9 \\ 1 \text{ or } 0, & 0.9 \le q_i^j \le 1 \end{cases} \tag{16}$$

where a_1, a_2, a_3 are the three parameters of the membership functions. Using the classified membership functions, we can get the membership degrees of each aspect of some information network to five different levels.

Let α_j denote the distinguishable weight of the jth aspect corresponding to the security of information network. According to Definition 2.1,

$$\alpha_j = 1 - \frac{1}{\log p}\left(-\sum_{k=1}^{5}\mu_{jk}\cdot\log\mu_{jk}\right)\Bigg/\sum_{j=1}^{3}\left(1 - \frac{1}{\log p}\left(-\sum_{k=1}^{5}\mu_{jk}\cdot\log\mu_{jk}\right)\right) \tag{17}$$

According to Definition 2.2, the effective distinguishable value of the kth class membership of the jth aspect could be calculated:

$$\left(1 - \frac{1}{\log p}\left(-\sum_{k=1}^{5}\mu_{jk}\cdot\log\mu_{jk}\right)\Bigg/\sum_{i=1}^{3}\left(1 - \frac{1}{\log p}\left(-\sum_{k=1}^{5}\mu_{jk}\cdot\log\mu_{jk}\right)\right)\right)\cdot\mu_{jk} \tag{18}$$

According to Definition 2.3, the comparable effective value of the kth class membership of the jth aspect could be calculated:

$$v_k^j = \lambda_j(N)\cdot\left(1 - \frac{1}{\log p}\left(-\sum_{k=1}^{5}\mu_{jk}\cdot\log\mu_{jk}\right)\Bigg/\sum_{j=1}^{3}\left(1 - \frac{1}{\log p}\left(-\sum_{k=1}^{5}\mu_{jk}\cdot\log\mu_{jk}\right)\right)\right)\cdot\mu_{jk} \tag{19}$$

According to Definition 2.4, we could calculate the kth class comparable sum of the security of information network:

$$M_k = \sum_{j=1}^{3} v_k^j \tag{20}$$

Then we can calculate the membership of the security of information network belonging to C_k:

$$\mu_k \triangleq M_k\Bigg/\sum_{k=1}^{5} M_k, \quad \forall k = 1, 2, \ldots, 5 \tag{21}$$

Finally, we could use the criterion of maximal membership degree to judge the level of the information network.

3.3. **The framework of the proposed approach for rating network security.** According to the proposed approach in the last subsection, we summarize the framework of the proposed approach for rating network security as follows:

Step 1: Determine the evaluation aspects of rating network security (As analyzed above, we consider three aspects to rate the security of information networks: the security of the persons involved in the network, the security of the network itself and the security of the environment where the network locates in);

Step 2: Obtain the comparative values x_{il}^{j} $(i, l = 1, 2, \ldots, n;\ j = 1, 2, 3)$ by the pairwise comparison;

Step 3: Calculate the preference of information network N_i over all other information networks in terms of index F_j using Equation (6);

Step 4: Determine the most secure and insecure information networks according to Definition 3.2 and Definition 3.3 respectively;

Step 5: Calculate the relative similarity of each aspect of information networks to the most secure and insecure ones using Equation (9);

Step 6: Calculate the distinguishable weight of the jth aspect corresponding to the security of information network using Equation (13);

Step 7: Calculate the effective distinguishable value of the kth class membership of the jth aspect using Equation (18);

Step 8: Calculate the comparable effective value of the kth class membership of the jth aspect using Equation (19);

Step 9: Calculate the kth class comparable sum of the security of information network using Equation (20);

Step 10: Calculate the membership of the security of information network belonging to C_k using Equation (21) and using the criterion of maximal membership degree to judge the level of the information network.

4. **Application Study.** In order to show the effectiveness of the proposed approach, we applied the approach to evaluating 10 information networks in Dalian city of China. These 10 networks belong to one big company, and the managers want to know the security of these networks, in order to plan new network improvement schemes. Here we do not give the specific names of the company in order to avoid non-academic issues.

4.1. **Obtaining the comparative values.** As mentioned above, it is often not easy for decision-makers to judge which one of many alternatives is the best, but it is easy for them to judge which one of two alternatives is better than the other. Thus, according to the three evaluation aspects mentioned in Section 3.1, we first let experts group pairwise compare the 10 information networks using the 1-9 comparative scales in Table 1, getting the comparative values in terms of each evolution aspect, as Tables 2-4 show.

Seen from the results in Tables 2-4, the comparative values meet the consistency. For example, in terms of the evaluation factor F_1, the security of information network N_1 is more secure than that of information network N_4 (The comparative value is 2) and the security of information network N_4 is more secure than that of information network N_5 (The comparative value is 2), so the security of information network N_1 should be more secure than that of information network N_5 (The comparative value is indeed 3).

After applying the pairwise comparison to obtaining all the comparative values x_{il}^{j} $(i, l = 1, 2, \ldots, 10; j = 1, 2, 3)$, we can use Equation (6) to calculate the preference of

TABLE 2. The comparative values in terms of F_1

	N_1	N_2	N_3	N_4	N_5	N_6	N_7	N_8	N_9	N_{10}
N_1	1	1/2	6	2	3	4	1/4	1/3	4	5
N_2	2	1	7	3	4	5	1/3	1/2	5	6
N_3	1/6	1/7	1	1/5	1/4	1/3	1/9	1/8	1/3	1/2
N_4	1/2	1/3	5	1	2	3	1/5	1/4	3	4
N_5	1/3	1/4	4	1/2	1	2	1/6	1/5	2	3
N_6	1/4	1/5	3	1/3	1/2	1	1/7	1/6	1	2
N_7	4	3	9	5	6	7	1	2	7	8
N_8	3	2	8	4	5	6	1/2	1	6	7
N_9	1/4	1/5	3	1/3	1/2	1	1/7	1/6	1	2
N_{10}	1/5	1/6	2	1/4	1/3	1/2	1/8	1/7	1/2	1

TABLE 3. The comparative values in terms of F_2

	N_1	N_2	N_3	N_4	N_5	N_6	N_7	N_8	N_9	N_{10}
N_1	1	5	6	4	3	8	3	2	8	7
N_2	1/5	1	2	1/2	1/3	4	1/3	1/4	4	3
N_3	1/6	1/2	1	1/3	1/4	3	1/4	1/5	3	2
N_4	1/4	2	3	1	1/2	5	1/2	1/3	5	4
N_5	1/3	3	4	2	1	6	1	1/2	6	5
N_6	1/8	1/4	1/3	1/5	1/6	1	1/6	1/7	1	1/2
N_7	1/3	3	4	2	1	6	1	1/2	6	5
N_8	1/2	4	5	3	2	7	2	1	7	6
N_9	1/8	1/4	1/3	1/5	1/6	1	1/6	1/7	1	1/2
N_{10}	1/7	1/3	1/2	1/4	1/5	2	1/5	1/6	2	1

TABLE 4. The comparative values in terms of F_3

	N_1	N_2	N_3	N_4	N_5	N_6	N_7	N_8	N_9	N_{10}
N_1	1	1/2	6	5	6	5	2	2	3	4
N_2	2	1	7	6	7	6	3	3	4	5
N_3	1/6	1/7	1	1/2	1	1/2	1/5	1/5	1/4	1/3
N_4	1/5	1/6	2	1	2	1	1/4	1/4	1/3	1/2
N_5	1/6	1/7	1	1/2	1	1/2	1/5	1/5	1/4	1/3
N_6	1/5	1/6	2	1	2	1	1/4	1/4	1/3	1/2
N_7	1/2	1/3	5	4	5	4	1	1	2	3
N_8	1/2	1/3	5	4	5	4	1	1	2	3
N_9	1/3	1/4	4	3	4	3	1/2	1/2	1	2
N_{10}	1/4	1/5	3	2	3	2	1/3	1/3	1/2	1

information network N_i over all other information networks in terms of index F_j, that is, the x_i^j. Let us take the calculation of x_1^1 as the example,

$$x_1^1 = \sum_{\substack{l=1\\ l\neq 1}}^{10} x_{1l}^1 = 1/2 + 6 + 2 + 3 + 4 + 1/4 + 1/3 + 4 + 5 = 25.08$$

Table 5. The results of x_i^j

	N_1	N_2	N_3	N_4	N_5	N_6	N_7	N_8	N_9	N_{10}
x_i^1	25.08	32.83	$\mathbf{2.16}_*$	18.28	12.45	7.59	$\mathbf{51.00}^*$	41.50	7.59	4.22
x_i^2	$\mathbf{46.00}^*$	14.62	9.70	20.58	27.83	$\mathbf{2.88}_*$	27.83	36.50	$\mathbf{2.88}_*$	5.79
x_i^3	33.50	$\mathbf{43.00}^*$	$\mathbf{3.29}_*$	6.70	$\mathbf{3.29}_*$	6.70	24.83	24.83	17.58	11.62

In the same way, we can attain the results of all other x_i^j, as Table 5 shows.

4.2. **Calculating the relative similarities and membership degrees.** Then, we can determine the best and worst values of the preferences in terms of each evaluation factor, as the bold values in Table 5 show. Thus, according to Definition 3.2 and Definition 3.3, the most secure and insecure information networks are respectively:

$$N^* = \left\{(x^1)^*, (x^2)^*, (x^3)^*\right\} = \{51.00, 46.00, 43.00\}$$

and

$$N_* = \left\{(x^1)_*, (x^2)_*, (x^3)_*\right\} = \{2.16, 2.88, 3.29\}$$

As we can see, the most secure and insecure information networks are two virtual information networks. The closer some information network is to the most secure one, the more secure the information network is, and the closer some information network is to the most insecure one, the more insecure the information network is. In order to measure the closeness of each information network to the most secure and insecure ones, we use Definition 3.4 to calculate the relative similarities, as Table 6 shows.

Table 6. The relative similarities of each aspect of these information networks

	N_1	N_2	N_3	N_4	N_5	N_6	N_7	N_8	N_9	N_{10}
x_i^1	0.47	0.63	$\mathbf{0.00}_*$	0.33	0.21	0.11	$\mathbf{1.00}^*$	0.81	0.11	0.04
x_i^2	$\mathbf{1.00}^*$	0.27	0.16	0.41	0.58	$\mathbf{0.00}_*$	0.58	0.78	$\mathbf{0.00}_*$	0.07
x_i^3	0.76	$\mathbf{1.00}^*$	$\mathbf{0.00}_*$	0.09	$\mathbf{0.00}_*$	0.09	0.54	0.54	0.36	0.21

After getting the relative similarities of each aspect of these information networks, we can use the membership functions defined in Figure 1 and Equation (12) to calculate the membership degrees of each aspect of these information networks to the five ordered levels: 0.9 (C_1, very secure), 0.7 (C_2, secure), 0.5 (C_3, general), 0.3 (C_4, insecure), 0.1 (C_5, very insecure), as Tables 7-9 show.

Seen from the membership degrees in Tables 7-9, we can find the security orders and levels of these ten information networks in terms of each evaluation aspect.

(1) In terms of F_1 (The security of the persons involved in the network), the security orders and levels are (The values in the brackets are the maximal membership degrees):

C_1: $N_7(1.00), N_8(0.527)$

C_2: $N_2(0.640)$

C_3: $N_1(0.847)$

C_4: $N_4(0.850), N_5(0.553)$

C_5: $N_3(1.000), N_6(0.944), N_9(0.944), N_{10}(1.000)$

TABLE 7. The membership degrees of F_1 of these information networks

	C_1	C_2	C_3	C_4	C_5
N_1	0.000	0.000	**0.847**	0.153	0.000
N_2	0.000	**0.640**	0.360	0.000	0.000
N_3	0.000	0.000	0.000	0.000	**1.000**
N_4	0.000	0.000	0.150	**0.850**	0.000
N_5	0.000	0.000	0.000	**0.553**	0.447
N_6	0.000	0.000	0.000	0.056	**0.944**
N_7	**1.000**	0.000	0.000	0.000	0.000
N_8	**0.527**	0.473	0.000	0.000	0.000
N_9	0.000	0.000	0.000	0.056	**0.944**
N_{10}	0.000	0.000	0.000	0.000	**1.000**

TABLE 8. The membership degrees of F_2 of these information networks

	C_1	C_2	C_3	C_4	C_5
N_1	**1.000**	0.000	0.000	0.000	0.000
N_2	0.000	0.000	0.000	**0.861**	0.139
N_3	0.000	0.000	0.000	0.290	**0.710**
N_4	0.000	0.000	**0.552**	0.448	0.000
N_5	0.000	0.393	**0.607**	0.000	0.000
N_6	0.000	0.000	0.000	0.000	**1.000**
N_7	0.000	0.393	**0.607**	0.000	0.000
N_8	0.398	**0.602**	0.000	0.000	0.000
N_9	0.000	0.000	0.000	0.000	**1.000**
N_{10}	0.000	0.000	0.000	0.000	**1.000**

TABLE 9. The membership degrees of F_3 of these information networks

	C_1	C_2	C_3	C_4	C_5
N_1	0.304	**0.696**	0.000	0.000	0.000
N_2	**1.000**	0.000	0.000	0.000	0.000
N_3	0.000	0.000	0.000	0.000	**1.000**
N_4	0.000	0.000	0.000	0.000	**1.000**
N_5	0.000	0.000	0.000	0.000	**1.000**
N_6	0.000	0.000	0.000	0.000	**1.000**
N_7	0.000	0.212	**0.788**	0.000	0.000
N_8	0.000	0.212	**0.788**	0.000	0.000
N_9	0.000	0.000	0.299	**0.701**	0.000
N_{10}	0.000	0.000	0.000	**0.548**	0.452

(2) In terms of F_2 (The security of the network itself), the security orders and levels are (The values in the brackets are the maximal membership degrees):

C_1: $N_1(1.000)$

C_2: $N_8(0.602)$

C_3: $N_4(0.552), N_5(0.607), N_7(0.607)$

C_4: $N_2(0.861)$

C_5: $N_3(0.710), N_6(1.000), N_9(1.000), N_{10}(1.000)$

(3) In terms of F_3 (The security of the environment where the network locates in), the security orders and levels are (The values in the brackets are the maximal membership degrees):

C_1: $N_2(1.000)$

C_2: $N_1(0.696)$

C_3: $N_7(0.788), N_8(0.788)$

C_4: $N_9(0.701), N_{10}(0.548)$

C_5: $N_3(1.000), N_4(1.000), N_5(1.000), N_6(1.000)$

Seen from the above orders, policy makers could find which networks are vulnerable in terms of each aspect. Thus, they could make targeted policies to enhance the security of each information network. However, due to the inconsistency in terms of different aspects, these relative similarities are needed to be fused together to judge the overall security of these information networks. In the following sections, we show the overall rating results of these information networks respectively by the similarity-based $\mathrm{M}(1, 2, 3)$.

4.3. **Rating results by the similarity-based M(1, 2, 3).** The weights of the three aspects of the security of information networks have important impacts on the rating results. In the work, we do not focus on the determination of the weights, and just assume that the weights of the three aspects are the same, that is, $\lambda_1(N) = \lambda_2(N) = \lambda_3(N) = 1/3$. Based on the attained relative similarities in Table 6 and the membership degrees in Tables 7-9, we could use the similarity-based $\mathrm{M}(1, 2, 3)$ to calculate the membership degrees of information networks, as Table 10 shows.

TABLE 10. The membership degrees of information networks

	C_1	C_2	C_3	C_4	C_5
N_1	**0.5050**	0.1829	0.2643	0.0477	0
N_2	**0.4267**	0.1622	0.0912	0.2754	0.0445
N_3	0	0	0	0.0691	**0.9309**
N_4	0	0	0.1847	0.3824	**0.4329**
N_5	0	0.1064	0.1643	0.1469	**0.5825**
N_6	0	0	0	0.0169	**0.9831**
N_7	**0.4420**	0.1650	0.3931	0	0
N_8	0.2906	**0.4173**	0.2921	0	0
N_9	0	0	0.0747	0.1945	**0.7308**
N_{10}	0	0	0	0.1219	**0.8781**

Seen from the results in Table 10, we can use the criterion of maximal membership degree to evaluate the overall security of these ten information networks:

C_1: $N_1(0.5050), N_2(0.4267), N_7(0.4420)$

C_2: $N_8(0.4173)$

C_5: $N_3(0.9309), N_4(0.4329), N_5(0.5825), N_6(0.9831), N_9(0.7308), N_{10}(0.8781)$

To make the comparison, we summarize the results in Section 4.2 and Section 4.3 into Table 11.

Seen from the summarized results in Table 11, the proposed approach could not only evaluate the security of the 10 information networks in terms of the three aspects but also evaluate the overall security of these information networks. Meanwhile, the proposed

Table 11. The final rating results

	Rating results in terms of F_1	Rating results in terms of F_2	Rating results in terms of F_3	The overall security	The most vulnerable aspects
N_1	C_3	C_1	C_2	C_1	F_1
N_2	C_2	C_4	C_1	C_1	F_2
N_3	C_5	C_5	C_5	C_5	F_1, F_2, F_3
N_4	C_4	C_3	C_5	C_5	F_3
N_5	C_4	C_3	C_5	C_5	F_3
N_6	C_5	C_5	C_5	C_5	F_1, F_2, F_3
N_7	C_1	C_3	C_3	C_1	F_2, F_3
N_8	C_1	C_2	C_3	C_2	F_3
N_9	C_5	C_5	C_4	C_5	F_1, F_2
N_{10}	C_5	C_5	C_4	C_5	F_1, F_2

approach could recognize the most vulnerable aspects of each information network. These results could provide good supports for the following making policies to enhance the security of these information networks.

(1) Since the security of networks N_3, N_4, N_5, N_6, N_9 and N_{10} is rated as the "very insecure", decision-makers should take timely actions to improve the security of these networks, especially to networks N_3 and N_6 whose membership degrees are very high. Specifically, decision-makers could refer to the recognized most vulnerable aspects of these networks as the last column in Table 11 shows.

(2) For networks N_1, N_2, N_7 and N_8 which are rated as "very secure" or "secure", decision-makers should also take some specific measurements according to the most vulnerable aspects of these networks. For example, some stricter personnel management and training policies involved in network N_1 could be made, since the most vulnerable aspect of network N_1 is F_1 (that is, the security of the persons involved in the network).

Meanwhile, in order to show the advantage of our approach, we conducted the comparison of the results by our approach with those by the TOPSIS (Technique for Order Preference by Similarity to Ideal Solution) method which is widely used for MADM problems [18]. Using the data in Table 5 and the weight of each aspect, the ranking result by the classic TOPSIS is $N_1 \succ N_8 \succ N_7 \succ N_2 \succ N_4 \succ N_5 \succ N_9 \succ N_{10} \succ N_6 \succ N_3$. According to the rating results and membership degrees in Table 10, the overall ranking result to all the information networks by our approach is $N_1(C_1, 0.5050) \succ N_7(C_1, 0.4420) \succ N_2(C_1, 0.4267) \succ N_8(C_2, 0.4173) \succ N_4(C_5, 0.4329) \succ N_5(C_5, 0.5825) \succ N_9(C_5, 0.7308) \succ N_{10}(C_5, 0.8781) \succ N_3(C_5, 0.9309) \succ N_6(C_5, 0.9831)$ (Note that for C_1 and C_2, bigger membership degrees mean better, and for C_4 and C_5, bigger membership degrees mean worse).

As we can see, the overall ranking result by our approach is consistent with that by the TOPSIS except N_8 and N_6. The inconsistency probably result from the redundant data is included in Table 5. However, the classic TOPSIS method does not deal with the redundancy, which may result in the unrealistic ranking. In addition, the TOPSIS method cannot produce the reliability information, but our approach could use the membership degree to show the reliability of rating some information network as a specific level. In a word, our integrated approach is superior to the classic TOPSIS since our approach could delete the redundancy in original data and provide the reliability information in the rating results.

5. **Conclusions.** The main contributions of the work could be summarized as follows: (i) Three evaluation aspects on the security of information networks are first analyzed, and the pairwise comparison method is used to obtain the values corresponding to these aspects of one information network over other networks; (ii) The most secure and insecure information networks are defined according to all alternative information networks and the relative similarity is defined to measure the closeness of any information network to the most secure and insecure information networks; (iii) Based on the attained relative similarities, a novel similarity-based $\mathrm{M}(1, 2, 3)$ approach is developed to evaluate the security of information networks. Application study shows that the proposed approach could evaluate the overall security of alternative information networks and recognize the most vulnerable aspects of each information network.

Although the work develops a similarity-based $\mathrm{M}(1, 2, 3)$ approach for rating and evaluating the security of alternative information networks, there are also some issues needed to be studied further, such as the determination of the weights of evaluation criteria.

Acknowledgment. This research is supported by National Natural Science Foundation of China by Grant (No. 71471025), 2015 Hong Kong Scholars Program (No. XJ2015007), Fundamental Research Funds Program from Northwest A&F University (No. 2452015230). An earlier version of this work was posted at the 2014 Joint 7th International Conference on Soft Computing and Intelligent Systems and 15th International Symposium on Advanced Intelligent Systems (SCIS & ISIS 2014), and recommended for publishing on this journal with the permission of IEEE Publisher.

REFERENCES

[1] C. H. Liao and C. W. Chen, Network externality and incentive to invest in network security, *Economic Modelling*, vol.36, pp.398-404, 2014.

[2] V. Skoularidou and D. Spinellis, Security architectures for network clients, *Information Management & Computer Security*, vol.11, no.2, pp.84-91, 2003.

[3] G. Sharma, S. Bala and A. K. Verma, Security frameworks for wireless sensor networks-review, *Procedia Technology*, vol.6, pp.978-987, 2012.

[4] S. Geravand and M. Ahmadi, Bloom filter applications in network security: A state-of-the-art survey, *Computer Networks*, vol.57, no.18, pp.4047-4064, 2013.

[5] J. Steenbruggen, M. T. Borzacchiello, P. Nijkamp et al., Data from telecommunication networks for incident management: An exploratory review on transport safety and security, *Transport Policy*, vol.28, pp.86-102, 2013.

[6] K. Islam, W. Shen and X. Wang, Wireless sensor network reliability and security in factory automation: A survey, *IEEE Trans. Systems, Man, and Cybernetics, Part C: Applications and Reviews*, vol.42, no.6, 2012.

[7] S. Kondakci, Analysis of information security reliability: A tutorial, *Reliability Engineering & System Safety*, vol.133, pp.275-299, 2015.

[8] P. T. Chang and K. C. Hung, Applying the fuzzy-weighted-average approach to evaluate network security systems, *Computers & Mathematics with Applications*, vol.49, no.11-12, pp.1797-1814, 2005.

[9] Y. Li, X. Shan and G. Wu, Comprehensive evaluation model for computer network security with linguistic information, *Advances in Information Sciences and Service Sciences*, vol.3, no.9, pp.126-131, 2011.

[10] S. Zhang, A model for evaluating computer network security systems with 2-tuple linguistic information, *Computers and Mathematics with Applications*, vol.62, no.4, pp.1916-1922, 2011.

[11] Q. Liu and Y. Zhang, VRSS: A new system for rating and scoring vulnerabilities, *Computer Communications*, vol.34, no.3, pp.264-273, 2011.

[12] C. S. Malavenda, F. Menichelli and M. Olivieri, A regulation-based security evaluation method for data link in wireless sensor network, *Journal of Computer Networks and Communications*, vol.2014, pp.1-15, 2014.

[13] H. Jiang and J. Ruan, Fuzzy evaluation on network security based on the new algorithm of membership degree transformation – $\mathrm{M}(1, 2, 3)$, *Journal of Networks*, vol.4, no.5, pp.324-331, 2009.

[14] L. A. Zadeh, Fuzzy sets, *Information and Control*, vol.8, pp.338-353, 1965.

[15] J. Chen, Derivation of membership functions for fuzzy variables using genetic algorithms, *Project Report*, Mississippi State University, 1998.

[16] J. Ruan, X. Wang, Y. Shi and Z. Sun, Scenario-based path selection in uncertain emergency transportation networks, *International Journal of Innovative Computing, Information and Control*, vol.9, no.8, pp.3293-3305, 2013.

[17] S. Hemalatha, K. R. Babu, K. N. Rao et al., Analysis of supplier's performance through FPIR/FNIR and membership degree transformation, *Proc. of 2015 International Conference on Computer Science and Information Technology*, Bangalore, India, 2015.

[18] Z. Yue, TOPSIS-based group decision-making methodology in intuitionistic fuzzy setting, *Information Sciences*, vol.277, pp.141-153, 2014.