Evaluation Indicators and Model of Network Technical Anonymity

Xi Chen and Gang Li

School of Economics and Management, Beijing University of Posts and Telecommunications
No.10. Xitucheng Road, Haidian District, 100876, Beijing, China
chenxibupt@263.net, lg280@sina.com

Abstract

The present study raises the concept of network technical anonymity, and designs its corresponding evaluation indicators and model, in order to provide the basis and methods for the evaluation of how anonymous a behavioral agent is on the net. Network technical anonymity is defined as the difficulty in tracking the real identity of a network agent. Five indicators have been designed as follows: name, valid address, alias and behaviors on the net and social attributions. Besides, based on AHP and the fuzzy theory, we have worked out the relative weights of the evaluation indicators and an evaluation model. With this model, we made evaluation of the network technical anonymity of several network applications that are commonly used now in China. The evaluation indicators and model can be applied to the evaluation of how anonymous a network user is in various kinds of network applications, and serve as references for management and design of web services.

Keywords: *Network technical anonymity, Network real name system, AHP, Fuzzy theory, Network user identification*

I. Introduction

The topic of network anonymity has long been the focus of scholars in network field. The activities on the net are more or less anonymous [1]. However, network anonymity exerts negative influence on people's social life on the Internet [2]. A debate has been reignited on the topic of whether a real-name system should be applied to the net [3]. Concerning the specific implementation of a real-name system, the basic requirement is to provide real information of their identity when users enjoy network services. It is commonly believed that there won't be anonymity after users providing real identity [4]. However, our perception of network behavioral agents' identity cannot be limited as either anonymous or real name because of the following two arguments: firstly, the special way of interaction on the net decides that even though one has provided real identity to ISP, he/she is still anonymous in the foreground of a network application [5]; secondly, even though one has not offered real identity to ISP, he/she may also be identified based on the various information on the foreground provided when participating network activities. That's why human flesh search is rampant.

Based on the understanding of the foresaid questions, we believe that network user identification does not only have two categories: anonymity and real name. Besides, the majority of users on the net may not be absolutely anonymous or not-anonymous. Whether being anonymous results from the cost of matching net users with real identities. The higher the cost is, the more anonymous a user is; the lower, the more not-anonymous.

Hayne and Rice claimed that there are two kinds of anonymity in social interaction, namely technical anonymity and social anonymity [6]. Users can not be identified through identifiable personal information (*i.e.*, information showing the real identity of an agent) that is eliminated technically, named technical anonymity. Social anonymity refers to perceived anonymous in interaction, in other words, even if the identify information is provided; one may have psychological perceptions of the anonymity of their real identity [7]. Based on this, we define network technical anonymity as the difficulties in technically utilizing available identify information to find out the real identity of behavioral agents on the net, and indicators for cost to be paid. Network technical anonymity aims to evaluate how anonymous users are on specific network application, and how anonymous a specific user is.

The present study is intended to explore the evaluation indicators and a model for studying network technical anonymity, providing practical basis and method of evaluation mechanism for network technical anonymity. This paper has two major parts: one is to design five basic evaluation indicators for network technical anonymity, and to work out the relative weights of the five indicators by using AHP. Besides, referring to the fuzzy theory and relative weights, an evaluation model is designed. The other is to apply the evaluation model to evaluation of the network technical anonymity of several commonly used network applications, which is an empirical study on the rationality of the indicators and the model.

2. Theoretical Basis

2.1. AHP and Its Processes

AHP (Analytic Hierarchy Process) is a structured technique for qualitative and quantitative analysis of ambiguous or complex decisions, developed by Thomas L. Saaty *et al.*, in University of Pittsburgh in the 1970s. Its stages of modeling are as follows:

Stage 1. Create a hierarchical model

After deeply analysis the object we study, we divide elements related to the object into various levels, and a hierarchical chart is made to show hierarchy of levels and affiliations between elements.

Stage 2. Create judgment matrix

Judgment matrix A is created by paired comparison. When comparing the influence of $X = (x_1, x_2, .., x_n)$ on the same object, two factors, x_i and x_j are chosen to compare with each other each time. a_{ij} Represents the ratio of the influence of x_i on the object to that of x_j. The value of a_{ij} is decided by Saaty's 1-9 Scale. A is a reciprocal matrix.

Stage3. Consistency check

Consistency check refers to the criterion for measuring the quality of judgment matrix A.

Definition: matrices that meet the formula $a_{ij}a_{jk} = a_{ik}, \forall i, j, k = 1, 2, ..., n$ are considered as consistent matrices. It is necessary to examine whether the judgment matrix A is rather inconsistent to make sure that A is acceptable.

Theorem 1: The largest eigenvalue of the reciprocal matrix A, λ_{max} is a positive real number, so are the components of its corresponding eigenvectors. The norms of other eigenvalues are strictly smaller than λ_{max}.

Theorem 2: If A is a consistent matrix, then A must be a reciprocal matrix. Then A^T, the transposed matrix of A, is also consistent. Any two rows of A are proportional, and the scaling factor is greater than zero, then let Rank（A）=1. The largest eigenvalue of the reciprocal matrix A, $\lambda_{\max} = n$, in which n refers to the order of A. The norms of other eigenvalues are all zero.

If $\lambda_{\max}$, the largest eigenvalue of A, corresponds to eigenvector $W = (w_1, ..., w_n)^T$,

Then $a_{ij} = w_i / w_j, \forall i, j = 1, 2, ..., n$.

Theorem 3: When the n-order reciprocal matrix A is a consistent matrix, if and only if its largest eigenvalue $\lambda_{\max} = n$, or if A is inconsistent, $\lambda_{\max} > n$ is definitely workable.

According to Theorem 3, it can be judged whether A is consistent or not by examining whether $\lambda_{\max}$ equals to n. Since characteristic roots are highly dependent on a_{ij}, $\lambda_{\max}$ is much greater than n, and that leads to higher degree of inconsistency of A. Therefore, consistency check for the judgment matrix provided by decision makers is a must to decide whether the matrix is acceptable.

Consistency check for a judgment matrix includes following steps:

Firstly, figure out consistency index (CI):

$$CI = \frac{\lambda_{\max} - n}{n - 1} \quad (1)$$

If CI is close to zero, then matrix A has satisfactory consistency.

Then, According to the corresponding value of average random consistency index RI of matrix A, to calculate the consistency ratio CR:

$$CR = \frac{CI}{RI} \quad (2)$$

When CR <0.1, the judgment matrix has satisfactory consistency.

2.2. Fuzzy Evaluation Theory

Fuzzy synthetic evaluation method is an effective method of making a comprehensive evaluation of a thing that is influenced by multiple factors. Based on the membership theory of fuzzy mathematics, this method transforms qualitative evaluation into quantitative evaluation, namely using fuzzy mathematics to make an overall evaluation of the thing or object that is influenced by multiple factors. It features clear results and high systematization. It can well solve fuzzy and hard-to-quantify problems and it is also suitable for solving all kinds of uncertain problems.

The basic principle is as follows. An evaluator's evaluation of the factor set which influences a thing's functions is often fuzzy. M kinds of evaluations compose the fuzzy evaluation set $V = \{v_1, v_2, ..., v_m\}$. Its comprehensive evaluation is a fuzzy subset of V, namely $B = (b_1, b_2, ..., b_n) \in \wp(\vee)$, in which there is $b_k = \mu_B(V_k), k = 1, 2, ..., m$, indicating v_k 's membership degree to B. It also shows the status of v_k in the comprehensive evaluation. To comprehensively evaluate B depends on the weight of the factor $u_i(1, 2, ..., n)$. Thus, once the weight, $W=(w_1,w_2,...,w_n)$, $\sum_{i=1}^{n} w_i = 1$, is given, a comprehensive evaluation B can be determined.

The modeling steps of fuzzy synthetic evaluation are as follows: 1) determine the factor set $U=\{u_1,u_2,...,u_n\}$; 2) determine the evaluation $V=\{v_1,v_2,...,v_m\}$; 3) determine the single-factor evaluation matrix $R=(r_{ij})_{m\times n}$; 4) determine the comprehensive evaluation vector $B=W \circ R$, in which, $b_j = \bigvee_{i=1}^{n}(w_i \wedge r_{ij}), i=1,2,...,n, j=1,2,...,m$. In it, $\wedge$ and $\vee$ are Zadeh operators, representing chose-large operation and chose-small operation respectively.

3. Designing Evaluation Indicators

Internet is a virtual digital information network constructed by information technology. People often use virtual identity to interact on the Internet. Various activities on the Internet will leave recorded and traceable information on it. This information provides directive clues with different degree of identification in order to identify a behavioral agent on the net. According to theory on identification of social identity developed by Gary T. R, there are seven elements about identifying one's real identity, namely, name, valid address, traceable alias, untraceable alias, behavior pattern, social attributions (*e.g.*, sex, age, belief, occupation), and object for identity recognition [7]. Concerning the features of social interaction on the net, alias may often suggest personal habits, and it is usually traceable. Therefore, traceable and untraceable alias are combined together as one indicator, that is, alias on the net. Object for identity recognition refers to material objects (*e.g.*, papers, keepsakes, and letters of introduction) intended to recognize one's identity. It is not applicable to network space with virtual digital information [8]. Therefore, based on the specific features of social interaction on the net, the present study selects five indicators to evaluation technical anonymity. On account of the evaluation of difficulties in tracking the five indicators on the net, we can work out technical anonymity of a behavioral agent on network applications. Indicators and their descriptions are as follows:

- **Name:** Legal name that a net user use in his/her household registration [9]. A behavioral agent on the net is a natural person in the real world, and name represents his/her real identity [10].
- **Valid address:** The valid address where a net user lives in the real world.
- **Alias on the net:** The alias a net user uses in the virtual society on the net, also known as the network ID; the same user may have more than one alias.
- **Behaviors on the net:** Information left when one is using the net such as, online speech, online comments, and access records.
- **Social attributions:** Information about one's real social attributions left when people are using network applications, such as, age, sex, occupation, and hobbies.

Concerning to identify the agents, each indicator carries different amount of information. Therefore, when using these indicators to evaluate network technical anonymity, their relative weights also differ with each other. Taking the above aspects into consideration, the present research figured out the relative weights of each indicator by AHP.

4. Questionnaires Survey

4.1. Design the Research

The present research mainly adopts experts' evaluation method, and evaluators are all experts in the fields of computers, Internet and information technology. Based on the previous interviews, we initiated many discussions with doctoral experts in the process of selecting evaluation indicators, setting up evaluation method, and designing questions. Only by doing this can we make our questions and way of asking them legitimate, objective and understandable. Finally, we finished the Evaluation Questionnaire concerning network technical Anonymity on Network Applications as the questionnaire for our survey. The results of this questionnaire are mainly used to collect data for the following two researches: one is to figure out the relative weights of each indicator. According to the relative values of evaluation indicators given by experts, Saaty value of each indicator is fixed [11]. AHP is used to work out relative weights. The other is to utilize the overall evaluation given by experts on the difficulties in identifying a user in a specific network application, to use relative weights vector of each indicator, and to adopt fuzzy comprehensive evaluation method [12], in order to evaluate the network technical anonymity of seven popular network applications. We also adopt experts' Mean Opinion Score as calibration to examine the validity of our evaluation scheme.

The evaluation on network technical anonymity includes seven popular types of applications [13], namely, instant message (IM), search engine, micro blog, blog, social network site (SNS), Campus Network BBS, and public BBS. Network technical anonymity is defined as the difficulty in tracking the real identity of a network agent. The more difficult, the more anonymous a user is. Therefore, we use Likert's five points scale to set up five grades. From low to high, they are very easy, quite easy, difficult, quite difficult, and very difficult.

4.2. Collecting Questionnaires

Research shows that if one wants to use experts' evaluation method, the number of experts should better be limited from 10 to 50 [12]. Our questionnaires are targeted to 40 experts in the Internet field. We receive 33 valid feedback, showing 82.5% of them are active in our research.

Inclusion criteria for experts: 1) a master or doctor degree on majors in computer, IT, or Internet. 2) Familiar with various Internet applications and basic technical structure of the net. 3) More than 5-year experience on using the Internet. 4) Be interested in the present research, providing advices and suggestions from various perspectives; be willing to fill in expert consultation questionnaires.

Table 1. Features of Experts

Item	Option	Number	Proportion	Item	Option	Number	Proportion
Sex	Male	17	51.52%	Time spent on the net	5 to 10 years	13	39.39%
	Female	16	48.48%		Over 10 years	20	60.61%
Age	21-25	2	6.06%	Major	Computer technology	22	66.67%
	26-30	10	30.3%		Internet	12	36.36%
	31-40	20	60.61%		Information technology	16	48.48%
	41-50	1	3.03%	Education	Master	21	63.64%
					Doctor	12	36.36%

Sex distribution of experts is quite even. They all have relatively high degree, aged from 26 to 40. They are familiar with the Internet. The majority is quite familiar to various network applications with over 10-year experience of using the Internet.

4. 3. Reliability and Validity of the Survey

We adopt the degree of agreements of experts' opinions, combined with specific design of questionnaire survey, the internal consistency of evaluation of indicators' weight and the evaluation of membership of indicators on corresponding network application is reflected by using Cronbach'a coefficient,and Kendall's Coefficient to evaluate the reliability of the calibration [14]. The Cronbach'a Coefficient of the five evaluation indicators is 0.778; the coordination degree of experts' opinions is satisfactory. Besides, the Cronbach'a Coefficients for each network application are shown in the following chart:

Table 2. Cronbach'a Coefficient for Technical Anonymity of Network Applications

K	Network application	Cronbach'a Coefficient
1	Instant message (IM)	0.718
2	Search engine	0.886
3	Micro blog	0.832
4	Blog	0.818
5	social network site(SNS)	0.870
6	Campus BBS	0.825
7	Public BBS	0.922

It shows that coordination degree of experts' opinions on the five indicators is good. The reliability of the survey is quite satisfactory.

As for validity, we adopt calibration-linking method. Calibration is experts' overall evaluation on seven network applications. The Kendall's coefficient of the internal coordination of the overall evaluation is 0.835, with 165.356 in Chi-square value and $p<0.01$.

It shows satisfactory coordination. We take the average value experts make on evaluating technical anonymity as calibration, whose Pearson's correlation index with scores of evaluation grade reaches 0.966, and $p<0.01$, showing that the evaluation results are in line with the intuitive sense experts have on the technical anonymity of these applications, and that the present study has high validity.

5. Evaluation Model and Case Evaluation

5.1. The Synthetic Evaluation Model of Network Technical Anonymity

STEP 1. To set up the Factor Set, Based on the Evaluation Index

Based on the index system in Table 1, set up the major factor set $U=\{u_1,u_2,u_3,u_4,u_5\}$, in which u_1 stands for the legal name, u_2 the effective address, u_3 the online nickname, u_4 the online behaviors and u_5 the social identity.

STEP 2. To determine the Weight of Index Factors

The weight set of all index factors is $W=(w_1,w_2,w_3,w_4,w_5)$, in which $\sum_{i=1}^{5} w_i = 1$. The weight of w_i can be determined by using analytic hierarchy process. First of all, grade, based on the relative importance of those evaluation indices. The grading will employ the Saaty Scale (1~9). Then, synthesize the grades of the experts. Calculate the value of W, namely the weight of the corresponding index in the whole index system. And at last solve the values of $\lambda_{\max}$, CI and CR and conduct the consistency check towards the evaluation matrix.

The Saaty Scale is determined with the use of the method of average assignment for relative importance. This study employs the questionnaire method and calculates the mean value of experts' evaluation of the difficulty of using specific indices to know the real identity of online users. The scale of Saaty is determined by taking advantage of those different grades. In addition, it calculates the weight and judgment matrix of those indices. The weight value of $\lambda_{\max}$ and the value of CR are shown in the following table.

Table 3. Factor Judgment Matrix

U	u_1	u_2	u_3	u_4	u_5
u_1	1	4	5	7	4
u_2	1/4	1	2	3	1/2
u_3	1/5	1/2	1	3	1/2
u_4	1/7	1/3	1/3	1	1/2
u_5	1/4	2	2	2	1

Use the root method to extract the largest eigenvalue and the corresponding eigenvector of the judgment matrix. Details are as follows:

$$T = \begin{bmatrix} 1 & 4 & 5 & 7 & 4 \\ 1/4 & 1 & 2 & 3 & 1/2 \\ 1/5 & 1/2 & 1 & 3 & 1/2 \\ 1/7 & 1/3 & 1/3 & 1 & 1/2 \\ 1/4 & 2 & 2 & 2 & 1 \end{bmatrix}, \text{ resulting in: } \quad \overline{W} = \begin{bmatrix} 3.55 \\ 0.94 \\ 0.68 \\ 0.37 \\ 1.15 \end{bmatrix}$$

After the unitary processing, resulting in

$$W^T = (0.529, 0.141, 0.102, 0.056, 0.172) \qquad \lambda_{\max} = \sum_{i=1}^{n} \frac{(TW)_i}{nw_i} = 5.211 \qquad CI = \frac{\lambda_{\max} - n}{n-1} = 0.0527$$

$$CR = \frac{CI}{RI} = 0.047 < 0.1$$

Judgment matrix has a satisfactory consistency. The weight of index factors is as follows:

Legal name u_1 : 0.529; effective address u_2 : 0.141; online nickname u_3 : 0.102; online behaviors u_4 : 0.056; social identity u_5 : 0.172.

STEP 3. Set up the Evaluation Set

Set up a unified evaluation set for each index, namely $V = \{v_1, v_2, ..., v_m\}$, in which v_1 stands for “very easy”, v_2 “easy”, v_3 “moderate”, v_4 “difficult” and v_5 “very difficult”.

STEP 4. Determine the Membership Matrix R_{ij} of Factor Set u_i

r_{ij} is the factor’s membership relationship of factor u_i according to the valuation v_j in the major factor set $U = \{u_1, u_2, u_3, u_4, u_5\}$. By establishing a fuzzy relation between u_i and v_j, the membership matrix $R = (r_{ij})_{m \times n}$ can be got. In it, n is the number of sub-factors in the major factor set u_i and m is the number of evaluation grades, which is 5. The membership r_{ij} can be got by using fuzzy statistical method. It is equal to the proportion of the number of people whose evaluation towards the index i is in the grade j to the total number of all the evaluators, namely:

$$r_{ij} = \frac{v_{ij}}{\sum_{j=1}^{m} v_{ij}} \qquad (3)$$

In it v_{ij} stands for the membership to the comment v_j of the factor u_i, indicating that there are v_{ij} experts approving the comment.

STEP.5. Calculate the Comprehensive Evaluation B_i

$$B_i = W_i \circ R_{ij}, i, j = 1, 2, 3, 4, 5 \qquad (4)$$

5.2. Application of the Model

We apply the evaluation model to evaluate network technical anonymity of seven popular network applications. According to the evaluation experts made on the evaluation indicators to examine the network technical anonymity of seven popular network applications, we calculate the membership matrix of each application, respectively $R_k, k = 1, 2, ..., 7$. Then, Use the formula $B_k = W \circ R_k$ to work out the fuzzy comprehensive evaluation value:

$$b_1 = W \circ R_1 = (0.529, 0.141, 0.102, 0.056, 0.172) \circ \begin{bmatrix} 0.242 & 0.303 & 0.152 & 0.212 & 0.091 \\ 0.303 & 0.303 & 0.242 & 0.030 & 0.121 \\ 0.546 & 0.242 & 0.152 & 0.061 & 0.000 \\ 0.636 & 0.121 & 0.182 & 0.000 & 0.061 \\ 0.455 & 0.212 & 0.121 & 0.212 & 0.000 \end{bmatrix} = \bigvee_{i=1}^{5}(0.242, 0.303, 0.152, 0.212, 0.121) = 0.303$$

Then, grade it ‘quite low’.

$$b_2 = W \circ R_2 = (0.529, 0.141, 0.102, 0.056, 0.172) \circ \begin{bmatrix} 0.152 & 0.242 & 0.182 & 0.152 & 0.273 \\ 0.212 & 0.242 & 0.242 & 0.121 & 0.182 \\ 0.333 & 0.182 & 0.152 & 0.212 & 0.121 \\ 0.364 & 0.303 & 0.152 & 0.091 & 0.091 \\ 0.424 & 0.212 & 0.152 & 0.152 & 0.061 \end{bmatrix} = \bigvee_{i=1}^{5}(0.152, 0.242, 0.182, 0.152, 0.273) = 0.273$$

Then, grade it ‘very high’.

$$b_3 = W \circ R_3 = (0.529, 0.141, 0.102, 0.056, 0.172) \circ \begin{bmatrix} 0.606 & 0.212 & 0.091 & 0.061 & 0.030 \\ 0.364 & 0.303 & 0.121 & 0.091 & 0.121 \\ 0.545 & 0.273 & 0.152 & 0.030 & 0.000 \\ 0.606 & 0.242 & 0.152 & 0.000 & 0.000 \\ 0.606 & 0.242 & 0.121 & 0.030 & 0.000 \end{bmatrix} = \bigvee_{i=1}^{5}(0.529, 0.212, 0.121, 0.091, 0.121) = 0.529$$

Then, grade it ‘very low’.

$$b_4 = W \circ R_4 = (0.529, 0.141, 0.102, 0.056, 0.172) \circ \begin{bmatrix} 0.303 & 0.333 & 0.182 & 0.091 & 0.091 \\ 0.212 & 0.242 & 0.212 & 0.182 & 0.152 \\ 0.394 & 0.303 & 0.212 & 0.091 & 0.000 \\ 0.485 & 0.333 & 0.121 & 0.061 & 0.000 \\ 0.515 & 0.394 & 0.061 & 0.030 & 0.000 \end{bmatrix} = \bigvee_{i=1}^{5}(0.303, 0.333, 0.182, 0.141, 0.141) = 0.333$$

Then, grade it ‘quite low’.

$$b_5 = W \circ R_5 = (0.529, 0.141, 0.102, 0.056, 0.172) \circ \begin{bmatrix} 0.606 & 0.212 & 0.121 & 0.030 & 0.030 \\ 0.273 & 0.394 & 0.212 & 0.061 & 0.061 \\ 0.515 & 0.212 & 0.212 & 0.061 & 0.000 \\ 0.606 & 0.303 & 0.061 & 0.030 & 0.000 \\ 0.636 & 0.242 & 0.091 & 0.030 & 0.000 \end{bmatrix} = \bigvee_{i=1}^{5}(0.529, 0.212, 0.141, 0.061, 0.061) = 0.529$$

Then, grade it ‘very low’.

$$b_6 = W \circ R_6 = (0.529, 0.141, 0.102, 0.056, 0.172) \circ \begin{bmatrix} 0.424 & 0.364 & 0.182 & 0.000 & 0.030 \\ 0.273 & 0.394 & 0.182 & 0.091 & 0.061 \\ 0.394 & 0.303 & 0.273 & 0.030 & 0.000 \\ 0.455 & 0.303 & 0.212 & 0.030 & 0.000 \\ 0.455 & 0.273 & 0.212 & 0.061 & 0.000 \end{bmatrix} = \bigvee_{i=1}^{5}(0.529, 0.212, 0.141, 0.061, 0.061) = 0.529$$

Then, grade it ‘very low’.

$$b_7 = W \circ R_7 = (0.529, 0.141, 0.102, 0.056, 0.172) \circ \begin{bmatrix} 0.030 & 0.152 & 0.394 & 0.212 & 0.212 \\ 0.061 & 0.152 & 0.394 & 0.152 & 0.242 \\ 0.273 & 0.303 & 0.242 & 0.121 & 0.061 \\ 0.303 & 0.364 & 0.182 & 0.061 & 0.091 \\ 0.242 & 0.303 & 0.242 & 0.091 & 0.121 \end{bmatrix} = \bigvee_{i=1}^{5}(0.242, 0.172, 0.394, 0.212, 0.212) = 0.394$$

Then, grade it ‘high’.

Let the value of network technical anonymity is within 0 to 1. Zero means that it is very easy to identify a person; while one means that it is totally impossible to find users' real identity. Each grade corresponds to a range of values: very low equals to 0~0.2, quite low 0.2~0.4, high 0.4~0.6, quite high 0.6~0.8, very high 0.8~1.

Table 4. Ratings of Technical Anonymity of Network Applications

K	Network applications	Level of technical anonymity	Value of technical anonymity
1	IM	Quite low	0.2~0.4
2	Search engine	Very high	0.8~1
3	Micro blog	Very low	0~0.2
4	Blog	Quite low	0.2~0.4
5	SNS	Very low	0~0.2
6	Campus BBS	Very low	0~0.2
7	Public BBS	High	0.4~0.6

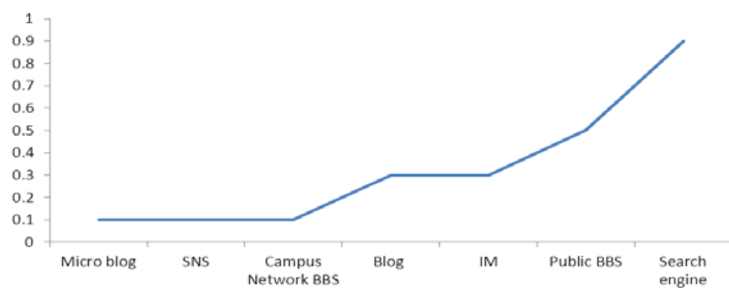


Figure 1. Middle Value of Technical Anonymity of Network Applications

6. Conclusions

The present study raises the concept of network technical anonymity, defining it as the difficulty in tracking the real identity of a network agent. It aims to provide a basic evaluation method to examine network technical anonymity. One task is to design five basic evaluation indicators for network technical anonymity, and to work out the relative weights of the five indicators by using AHP. Besides, referring to the fuzzy theory and relative weights, an evaluation model is designed. The other task is to apply the evaluation model and indicators to the evaluation of the grades of seven network applications. The reliability and validity is very high. Major results are: 1) among the five basic indicators to identify net users, real name is the most influential factor on disclosing a person's real identity. 2) Due to different functions and intentions of usage, difficulties in identifying users in different network applications vary. In other words, different applications have different degree of network technical anonymity. 3) According to the result of experiments shows that none of the network applications is absolutely anonymous, which leads us to realize that users can't hold absolute network technically anonymity. In fact, based on the registration information and IP address [16], one can find the real identity of a user technically; especially in the physical access layer, the Internet SPs adopt absolute real-name access authentication [17]. Therefore, there is hardly absolute anonymity on the net.

The present research is to evaluate network technical anonymity, and to provide a basic method for future evaluation. Network technical anonymity, in essence, is an important factor to show the relation between virtual society and the real world. It is closely related to people's activities on Internet. Based on the concept of network technical anonymity, further research can be expanded on three directions: the first is to detail the evaluation indicators system; the second is to examine the influence of network technical anonymity on peoples' usages and behaviors on the net by considering network technical anonymity as an observable variable; the third is to provide important references for ISPs to manage and design their services.

Acknowledgment

This work was supported in part by social management of network within the New Century Talents Support Program of Ministry of Education of China (CNET-07-0107).

References

[1] X. Chen and G. Li, "Game Analysis and Discussion on the Real Name System of Internet Public Sphere", Advances in Information Sciences and Service Sciences, vol. 4, no. 16, **(2012)**, pp. 272-279.
[2] M. K. Christopherson, "The positive and negative implications of anonymity in Internet social interactions: On the Internet, Nobody Knows You are a Dog", Computers in Human Behavior, vol. 5, no. 23, **(2007)**, pp. 3038-3056.
[3] W. M. Gao, "Analysis of Cyber Real-name System from the View of Law", Lan Zhou Academic, vol. 3, no. 14, **(2012)**, pp. 167-170.
[4] D. C. Cai and S. H. Liu, "Cyber Real-name System and the Governance of Online Offensive Information", Chinese Public Administration, vol. 11, no. 10, **(2012)**, pp. 68-71.
[5] W. Lu, "The Law Game between the Freedom of Expression and Cyber Real-name System", Lan Zhou Academic Journal, vol. 9, no. 13, **(2012)**, pp. 161-164.
[6] S. C. Hayne and R. E. Rice, "Attribution accuracy when using anonymity in group support systems", International Journal of Human–Computer Studies, vol. 47, no. 3, **(1997)**, pp. 429-250.
[7] G. T. Marx, "What's in a Name? Some Reflection on the Sociology of Anonymity", The Information Society: special issue on anonymous communication forthcoming, vol. 1, **(1999)**, pp. 1-12.
[8] D. Kesdogan and C. Palmer, "Technical challenges of network anonymity", Computer Communications, vol. 29, no. 3, **(2006)**, pp. 306-324.
[9] M. Xie, C. Wu and Y. L. Zhang, "A New Intelligent Topic Extraction Model on Web", Journal of Computers, vol. 6, no. 3, **(2011)**, pp. 466-473.
[10] C. Chen, D. J. He, S. Chan, J. J. Bu, Y. Gao and R. Fan, "Light weight and provably secure user authentication with anonymity for the global mobility network", International Journal of Communication Systems, vol. 24, no. 3, **(2011)**, pp. 347-362.
[11] Y. F. Zhao, D. W. Xu, T. S. Hou and C. Y. Liu, "Measure of the Initial Value of the Emission Right in Liao He River based on AHP", Statistics and Decision, vol. 2, no. 8, **(2013)**, pp. 50-53.
[12] C. Li and L. Xin, "Research on the Methods of Evaluating the Reliability and Validity of a Questionnaire", Chinese Journal of Statistics, vol. 5, no. 1, **(2008)**, pp. 541-545.
[13] I. Joshua, A. Mustafa and M. Goh, "Modeling funding allocation problems via AHP-fuzzy TOPSIS", International Journal of Innovative Computing, Information and Control, vol. 8, no. 5A, **(2012)**, pp. 3329-3340.
[14] H. I. Wang and C. C. Yu, "Measure the Performance of Reducing Digital Divide-the BSC and AHP Approach", Journal of Computers, vol. 6, no. 3, **(2011)**, pp. 389-396.
[15] R. King, "Assessing Anonymous Communication on Internet", Policy Deliberations, **(2001)**.
[16] M. Lu, "Study on Secret Key Management Project of WSN Based on ECC", Journal of Networks, vol. 7, no. 4, **(2012)**, pp. 652-659.
[17] S. Hayne and R. Rice, "Attribution Accuracy When Using Anonymity in Group Support Systems", International Journal of Human Computer Studies, vol. 47, no. 3, **(1997)**, pp. 429-450.

Appendix 1. Questionnaires to get relative importance of evaluation indicators

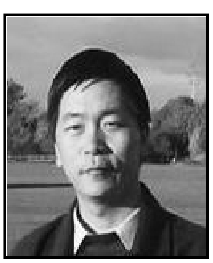
Indicators Number	Statements
1	The degree of difficulty in tracking the legal name and identity of the user.
2	The degree of difficulty in tracking the user's valid residence
3	The degree of difficulty in tracking the common network ID
4	The degree of difficulty to extract user-specific network language and behavioral characteristics
5	The degree of difficulty in determining user's social attributes (such as: age, gender, occupation, hobbies, etc.)
The degree of difficulty in tracking the indicator in this network application A:Very easy … E:Very difficult	

Appendix 2. Questionnaires to get the difficulty in tracking corresponding indicators

Indicators Number	Statements
1	With the legal name and identity number of the user, we can determine his/her true identity.
2	With the user's address we can determine his/her true identity.
3	With the user's network ID which is able to track the ID in the network, we can determine his/her true identity.
4	According to the characteristics of the words and behaviors of a user in the network will be able to determine his/her true identity.
5	Through the social attribute characteristics, such as the age, gender, occupation, and so on, we could determine true identity of the Internet users.
To what extent do you agree or disagree with the statements: A:completely disagree … E:totally agree	

Authors

Xi Chen is a PHD candidate at the School of Economics and Management, Beijing university of posts and telecommunications, China. She also got her bachelor's degree major in computer science and technology, and master's degree in management science from the same university BUPT. Her research interests include network information management, and network behaviors.
Connect her at: chenxibupt@263.net



Gang Li is a professor at the School of Economics and Management, Beijing University of posts and telecommunications, Beijing, China, as well as a doctoral tutor. He got his PHD degree from Nankai University, Tianjin, China. His research interests include Network public information management and network regulation.
Connect him at: lg280@sina.com