A Quantitative and Qualitative Analysis-based Security Risk Assessment for Multimedia Social Networks

Zhiyong Zhang[1], Lijun Yang[1], Hanman Li[1], and Fei Xiang[2]

(Corresponding author: Zhiyong Zhang)

Department of Computer Science, Information Engineering College, Henan University of Science and Technology[1]
Luoyang 471023, P. R. of China
(Email: z.zhang@ieee.org)
Department of Electronic Technology, Electrical Engineering College, Henan University of Science and Technology[2]

(Received Apr. 29, 2013; revised Dec. 13, 2013; accepted Jan 29, 2014)

Abstract

The emerging Multimedia Social Network (MSN) provides much more conveniences for the transmission and sharing of multimedia digital contents. However, the scenario on the distribution and spreading of copyrighted digital contents between users at will brings about a burning problem of Digital Rights Management (DRM). In addition, the open Internet and MSN platform are facing the security risks of digital contents copyrights infringements. The paper proposed a quantitative and qualitative-based risk analysis and assessment method, considering potential paths existence in MSN. Several risk impact factors was introduced, such as trust risk and user demands. Specifically, Value at Risk, a risk calculation method widely used in the financial field, as a quantitative analysis, was employed here. While an expert scoring sheet, as a qualitative approach, is used to evaluate non-quantifiable factors. Finally, the effectiveness of the security risk assessment method and related algorithm was verified by a well-designed experiment. We defined the size of the community followed by the "Rule of 150," and construct a random non-overlapped multimedia social network by using YouTube dataset. The experiment indicates that the relationships of risk loss with average rate of risk occurrence and risk preference of content providers are revealed.

Keywords: Digital rights management, multimedia social network, qualitative and quantitative analysis, risk assessment

1 Introduction

With the rapid development of network socialization, a large quantity of multimedia social network services and tools emerge, aiming at providing network tools, services and applications for transmission and sharing of the digital multimedia contents (such as digital images, audio and video, Java mobile applications, etc.) for MSN users. At present, the popular multimedia social networks throughout the world include Youtube, SongTaste, Youku, etc. These networks that are organized by users' social relationships are mainly used for using, sharing, and disseminating digital media content. They show obvious advantages in directly, quickly and flexibly transmitting digital contents. But, it also brings some risks for insecure transmission and uncontrollable sharing of the copyrighted digital contents. The unauthorized distribution, transmission and misuse of the digital contents make the problems of digital rights management increasingly prominent [14, 16, 17]. In the conditions of ubiquitous security flaws and malicious attacks, security risk management belongs to an effective way to ensure contents security and mitigate valuable digital asset risk. Therefore, the problem as to how to evaluate the transmission risk of digital rights under the multimedia social networks becomes our focus of concern. Further, DRM of multimedia social network will be better solved.

In recent years, the secure information spread and sharing in social networks, including multimedia social network and the special-purpose social network [7], has attracted much attention gradually. The research of DRM has two major technical paths: the preventive DRM technology and the reactive DRM technology. The preventive DRM technology is mainly based on the theory of cryptography and the usage control technology. The reactive one employs digital watermarking to protect digital contents and the corresponding copyrights. Whatever, for MSN scenario, the sharing strengthening of digital contents increases their exposure and leads to greater threat. Recently, some researchers focus on the information spread risk of social network, and the main research objective is to evaluate the risks of the unauthorized information access among users based on traditional access control policies. Different from the existing methods, this paper's main contribution is to integrate quantitative with qualitative approaches to evaluating the risks of potential digital rights distribution in multimedia social network scenario.

The remaining parts are arranged as below: firstly, Section 2 introduces the relevant researches on social network DRM and risk assessment. Section 3 describes background and theoretical knowledge involved in this article. Section 4 analyses the transmission risk of digital rights, and puts forward the risk assessment method by combining the qualitative and quantitative approaches. Section 5 provides Risk assessment algorithm. Section 6 makes an experiment by YouTube dataset and analyses the experimental results. Finally, Section 7 summarizes this research and shows the subsequent work.

2 Related Works

In recent years, some researchers have made extensive researches on social network platform and DRM. With regard to access control of digital contents for multimedia social networks, Barbara et al. [1] pointed out that the enhanced social network access control system is the first step to solve the existing security and privacy issues in online social networks. In order to resolve the current limitations, they proposed an expandable, fine-grain access control model based on semantic, web-online social networking. Sachan et al. [9] come up with an effective fine-grained access control model based on bit-vector transform. This model is able to convert certificates related to the digital contents into an effective structure. Security, storage and execution efficiency of this scheme are verified through mathematical and simulation experiment. Villegas [10] represented a personal data access control (PDAC) scheme. PDAC computes a ”trusted distance” measure between users that is composed of the hop distance on the social network and an affine distance derived from experiential data. For online social network, Park et al. [8] proposed a user-activity-centric framework for access control, which determines four key control behaviors: attribute, policy, relation and session controls. This frame not only supports access control based on user relations, but also applies to common attribute-based access control.

In order to improve media content copyright protection and to diminish the illegal spread of media content in social networks, Lian et al. [6] proposed a content distribution and copyright authentication system based on the media index and watermarking technology. The results of the experiments confirmed that the system had strong robustness and stability. In addition, Chung et al. [3] proposed a novel video matching algorithm, as well as developed an intelligent copyright protection system based on this algorithm. Confirmed by experiments, the proposed algorithm can effectively conduct video matching; and the proposed system was suitable for copyright protection for video sharing networks. With the intention of solving the problem of content security in online social networks, Yeh et al. [13] proposed a security model based on multi-party authentication and key agreement. This proposed model can achieve user authentication between communities with a strong non-repudiation and flexibility. We proposed a MSN trust model based on small-world theory [18]. This model can effectively evaluate and dynamically update the value of trust between users, as well as identify malicious share users.

Unfortunately, with the development of MSN, DRM-enabling digital contents are suffering from huge risks owing to increasingly serious copyright infringement and misuse. More attention should be paid to security risk assessment for the social networks. A probability-based method to evaluate unauthorized access risk (UAR) was proposed in [2]. This scheme is capable of accurately computing the probability of information transmission in all connected paths between two users, and the method practicability has been proved by tests. In addition, Wang et al. [11] presented a statistical risk assessment method to quantify the threats in the networks. The information flow between two users in the social information network scenarios is thus evaluated. For a generic security risk assessment, Huang et al. [5] proposed a novel approach to addressing some implementation issues involved in employing such an information security risk assessment standard of ISO/IEC 27005:2011(E), and use the chlorine processing system in a water treatment plant as an example to well indicate the effectiveness of the proposed method. We have ever tried to highlight a multi-disciplinary method for all-around examinations on risks to digital assets in the contents sharing scenario [15]. The method is a qualitative and quantitative fuzzy risk assessment, which is used for estimating a novel concept called Risk-Controlled Utility (RCU) in DRM. Then, we emphasize on an application case of the emerging trusted computing policy, and analyze the influences of different content sharing modes.

Summarily, there is a lack of risk assessment method for potential digital rights distribution in multimedia social network scenario, further better solved DRM issue.

3 Background Knowledge

Based on relations between users, the existing researches have mined potential transmission paths and credible potential paths for the multimedia social networks. Since the judgment of the credible potential paths is closely related to user-defined trust threshold, and the setting of the trust threshold has certain risk, the copyrighted digital contents transmitted and shared through the credible potential paths are still risky. For this reason, this article mainly carries out researches on risk assessment of digital right transmission via the credible potential paths. Thus, the relevant concepts of MSN potential paths are

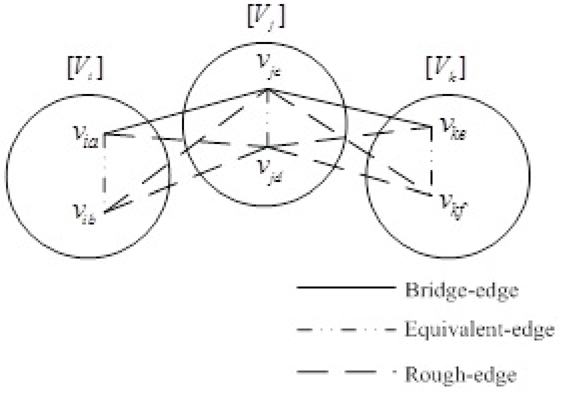

Figure 1: The potential paths in MSN

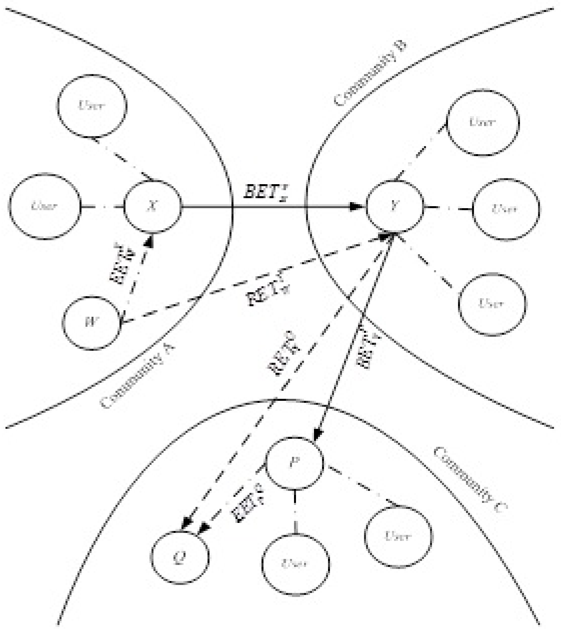

Figure 2: Potential path trust calculation

introduced in the following.

3.1 The Potential Paths in MSN

A social network consists of several locally dense "communities." In social networks, each community represents an actual social organization formed on the basis of social relationship or interest. That is, the node-node connection within community is relatively dense, but between which connections are very loose. A weak relation tends to transfer non-recurring information between different communities. Therefore, more alternation and information spread are performed between communities through weak relations, hence making it become an "information bridge" [12].

As shown in Figure 1, the MSN are divided into three communities, and the relation between users in the same community is very strong, whereas in different communities are relatively weak. Nodes in the same community have an equivalence relation. The connected edge of any nodes in the same community is called equivalent edge. The weak connection edge for connecting different communities is called the bridge edge. Through the weak relation between the communities, the rough relation will be produced, such as $< v_{ia}, v_{jd} >$, $< v_{jd}, v_{kf} >$ (as shown in the dotted line), what is called the rough edge. A path composed by continuous rough edges refers to a potential path (PP). So, in Figure 1, $< v_{ia}, v_{jd} >, < v_{jd}, v_{kf} >$ is a potential path from v_{ia} to v_{kf}. $< v_{ib}, v_{jd} >$, $< v_{jd}, v_{ke} >$ is the potential path in S from v_{ib} to v_{ke}; and $< v_{ib}, v_{jd} >$, $< v_{jd}, v_{kf} >$ is the potential path in S from v_{ib} to v_{kf}.

3.2 Trust Measurements of (Credible) Potential Paths

There is the direct trust between two users connected equivalent-edge and bridge-edge. So, the equivalent-edge trust calculation between communities is same to bridge-edge trust calculation, which can adopt a trust model for MSN in the reference [18]. Further, rough-edge trust (RT) can be obtained by integrating equivalent-edge trust (EDT) and bridge-edge trust (BDT). The EDT in a community is the direct trust between two nodes of connected equivalent edges in that community. Bridge-edge direct trust (BDT) is the direct trust between two users with a weak connected edge. In Figure 2, the trust value of the potential paths from W to U is shown as Equation (1).

$$RT_w^u = EDT_w^v \cdot BDT_v^u. \tag{1}$$

The definition of potential paths indicates that all edges on the potential paths are rough-edges. The trust value of the potential paths (expressed as T_{pp}) is a product of all rough-edge trust values in the path, as shown in Equation (2):

$$T_{pp}(v_1, v_2, \cdots, v_n) = \Pi_{i=1}^n RT_{v_i}^{v_{i+1}} (i = 1, 2, \cdots, n), \tag{2}$$

where the relation between v_i and v_{i+1} $(i = 1, 2, \cdots, n)$ is the rough relation.

Figure 2 also shows the definition of potential path, in which a potential path exists from W to $T < W, U >< U, T >$. Moreover, Equation (2) indicates that the trust value of this potential path $T_{pp}(W, U, T) = RT_w^u \cdot RT_U^t$, where RT_w^u and RT_u^t are rough-edge trust values. The trust value of potential paths is described in Equation (1).

Based on the trust value of potential paths, we try to find the credible potential paths. The method is described as follows: First, trust value T_{pp} of the potential path is calculated. Second, the user defines a trust threshold, which is denoted by $T_{threshold}$. Finally, there is a comparison between T_{pp} and $T_{threshold}$.

Definition 1 (Credible Potential Path, CPP). *If $T_{pp_{v_1 \to v_n}} \geq T_{threshold}$, the potential path v_1 to v_n is called as a credible potential path $CPP_{v_1 \to v_n}$.*

4 Security Risk Assessment on Potential Digital Rights Distribution

In order to effectively control the risk of digital rights transmission on the credible potential paths, the main problems focus on identification, quantification and evaluation of transmission risk. Through effectively analyzing and calculating risk of digital content transmission on the potential paths of multimedia social networks, and evaluating possible loss brought by the risks, the rights are flexibly and safely shared and transmitted between users. Security of digital content transmission is enhanced for the multimedia social networks.

4.1 Quantitative and Qualitative Analytic Approach

In order to evaluate transmission risks of copyrighted digital contents in multimedia social network, this article adopts both quantitative and qualitative risk assessment approaches. In risk management, Annualized Loss Expectancy (ALE) is a common quantitative analysis tool used for computing an expected loss for an annual unit, and in general it includes the following elements:

- Asset Value (AV) denotes a tangible or intangible worth of digital assets by using monetary or other styles, and it is determined by the potential impact caused by the loss of assets.
- Annual Rate of Risk Occurrence (ARRO) is a prediction of how often a specific risk event is likely to happen each year.
- Exposure Factor (EF) indicates the impact of risks on a target system.

According to the transmission feature of digital rights among MSN users, we introduce Risk of Trust (RT), which refers to the transaction process by the trust relationship reflects the risk of the interactive event. With regard to such a risk severity factor as user demands for contents in DRM ecosystem, we introduce User Demand (UD). So, ALE is defined as Equation (3).

$$ALE = AV \cdot ARRO \cdot EF \cdot UD \cdot RT, \tag{3}$$

where, for main parameters of ALE, Asset Value is easily acquired and depicted by the monetary value of digital contents, ARRO is calculated by Poisson Distribution of the annual risk occurrence, EF and UD are yielded through the fuzzy assessments, and RT is quantified through the relation between trust and risk.

4.1.1 VaR-based Calculation on Maximum ARRO

Value at Risk (VaR) [4] denotes the maximum possible loss of certain assets value in normal fluctuations of market. The basic idea is to take advantage of the historical volatility information to infer future situation, and this inference refers to a probability distribution. VaR is an essential calculation method for estimating the maximum risk values based on a confidence degree $(1-\alpha)$ in a given time period, and it was defined as

$$Prob(L \leq VaR) = 1 - \alpha,$$

where L is an expected risk loss, VaR is the maximum loss, and α is determined by Content Providers' opinions on risks to a specific DRM ecosystem, that is,

$$\begin{cases} 0 \leq \alpha < 0.5 & \text{Risk-averse} \\ \alpha = 0.5 & \text{Risk-neutral} \\ 0.5 < \alpha \leq 1 & \text{Risk-seeking} \end{cases} \tag{4}$$

Taking it into consideration that the Poisson Distribution is a common probability function depicting the likelihood of random events occurrence, we attempted to employ the Poisson Distribution and VaR to calculate the $ARRO$, that is an estimation on the maximum occurrence rate of a random copyrights infringement/illicit usage event of digital contents. Thus, the maximum occurrence rate is in line with Poisson Distribution with the parameter λ. And then, by using Equation (5), the maximum value of $ARRO$ can be calculated.

$$Prob(x \leq MAX_{ARRO}) = 1 - \alpha. \tag{5}$$

In this case, a Multimedia Social Network has the specific annual occurrence rate of copyrights infringements threat, as is compliant to Poison Distribution with λ that denotes the average $ARRO$ of random risky events. According to Equations (4) and (5), when λ respectively is equal to 1.8, 5, 9, MAX_{ARRO} can be gained for three different Providers' opinions, that is,
When $\lambda = 1.8$,

$$MAX_{ARRO} = \begin{cases} 5 & \alpha = 0.03 & \text{Risk-averse} \\ 2 & \alpha = 0.5 & \text{Risk-neutral} \\ 1 & \alpha = 0.54 & \text{Risk-seeking} \end{cases} \tag{6}$$

When $\lambda = 5$,

$$MAX_{ARRO} = \begin{cases} 9 & \alpha = 0.03 & \text{Risk-averse} \\ 4 & \alpha = 0.5 & \text{Risk-neutral} \\ 2 & \alpha = 0.88 & \text{Risk-seeking} \end{cases} \tag{7}$$

When $\lambda = 9$,

$$MAX_{ARRO} = \begin{cases} 16 & \alpha = 0.01 & \text{Risk-averse} \\ 8 & \alpha = 0.5 & \text{Risk-neutral} \\ 3 & \alpha = 0.98 & \text{Risk-seeking} \end{cases} \tag{8}$$

Obviously, the maximum of $ARRO$ decreases with the increase of α.

4.1.2 Fuzzy Assessments on EF and UD by Using Triangular Fuzzy Number

With respect to two fundamental parameters EF and UD, we adopt the triangular fuzzy number-based subjection function to estimate risk factors influencing digital rights transmission. Besides, about fuzzy assessments of UD and EF, there were six judges participating in the risk assessments. In this case, we firstly presented the assessment scale and corresponding semantics of UD and EF, which is shown by Table 1. And, a group of assessment values for parameters UD and EF were given in Table 2.

Table 1: Five-level scale descriptions of UD and EF factors

Level	Scale	UD Description	EF Description
1	90	Strong	High
2	70	Medium to Strong	Medium to High
3	50	Medium	Medium
4	30	Weak to Medium	Low to Medium
5	10	Weak	Low

According to the fuzzy assessment method, UD and EF were calculated as follows:

- As UD is a single-factor assessment participated by six reviewers, $zeta_{s_i}(x) = (\sum_{t=1}^{6} \zeta_{s_i}(x^t))/6$, $s_i \in \{90, 70, 50, 30, 10\}$. According Table 2, the subjection degree vector of UD is $SD_{UD} = (0.333, 0.425, 0.167, 0.1, 0)$. In terms of the principle for the maximum subjection degree, the optimal SD is 0.425, and UD is 70.
- EF is a multi-factor fuzzy assessment procedure, and the final value of SD should consider two factors (Credible potential path length and the trust value of credible potential paths) and its weights, which are shown in Table 2. So we gained $SD_{EF} = (0.382, 0.286, 0.21, 0.123, 0)$. The optimal EF is 0.382, and EF is 90.

In the calculations of ALE, UD and EF was normalized. That is, UD is 0.7, and EF is 90.

4.2 Trust Risks of Credible Potential Paths

Digital content sharing between users under multimedia social networks is based on certain trust relation, which will directly affect sharing and transmission of digital contents. For multimedia social networks, trust is closely associated with the risk, i.e. the higher the trust value between two users, the smaller the risk in sharing content information. So trust values of two interacting parties can reflects the risks in interaction events. Other conditions being equal, the higher the trust, the lower the risk would be; otherwise, the higher the risk. So we can suppose that trust value plus value-at-risk is approximately equivalent to 1. Based on the relation between trust and risk, trust risk value RT of the credible potential paths is given by Equation (9):

$$RT = 1 - T_{pp} (0 \leq T_{pp} \leq 1). \tag{9}$$

5 Algorithm Design

Risk assessment process of digital right transmission for multimedia social network divides into the following steps: first, all potential paths between two user-nodes in different communities are identified, and then the trust values of the potential paths are calculated. The credible potential paths in the range of user-defined trust threshold are found. Finally, the quantitative and qualitative approaches are proposed in this article to evaluate the risks in the credible potential paths. The process of the algorithm is described as the follows Algorithm 1.

Algorithm 1 Mining and Risk Assessment of Credible Potential Paths between any Two Nodes in MSN

```
1: Input: All the potential paths $PP_{i \to j}$ from $i$ to $j$; the number of share cycle $ShareNum$; the trust calculation window size $WindowSize$; feedback weight factor $Rate$; the trust threshold $T_{threshold}$; Asset Value $AV$; the value of Annual Rate of Risk Occurrence $ARRO$; the value of Exposure Factor $EF$; the value of User Demand $UD$.
2: Output: The trust values $T_{PP_{i \to j}}$ of $PP_{i \to j}$, all the credible paths $CPP_{i \to j}$, and Annualized Loss Expectancy ($ALE$).
3: Begin
4: To calculate direct trust value between the nodes from the same equivalence community class based on $ShareNum$, $WindowSize$ and $Rate$;
5: Based on the potential paths trust calculation method, trust value $T_{PP_{i \to j}}$ of all potential paths between $i$ and $j$ is computed;
6: The obtained trust value $T_{PP_{i \to j}}$ from Step 4 is compared with the trust threshold $T_{threshold}$. Then, according Definition 1, $CPP_{i \to j}$ will be obtained;
7: Return trust value $T_{PP_{i \to j}}$ and the credible potential paths $CPP_{i \to j}$.
8: To calculate $ALE$ of the credible potential paths $CPP_{i \to j}$ according to Equation (3), here, $RT_{PP_{i \to j}}$ is equal to $(1 - T_{PP_{i \to j}})$;
9: Return $ALE$ value of the credible potential paths $CPP_{i \to j}$;
10: End
```

6 Experiment and Analysis

In order to verify the effectiveness of the quantitative-and-qualitative-combined method for risk assessment, simulation experiment is made. The hardware of the simulation experiment is listed below: AMD Athlon(tm) X2 240 Processor 2.8G, 2G, and Microsoft Windows 7 ultimate. We made an experiment based on a representative real-world MSN YouTube dataset (http://socialnetworks.mpi-sws.org/data-imc2007.html), and further found a random multimedia social network with non-overlapped communities, as shown in Figure 3. Three sharing commu-

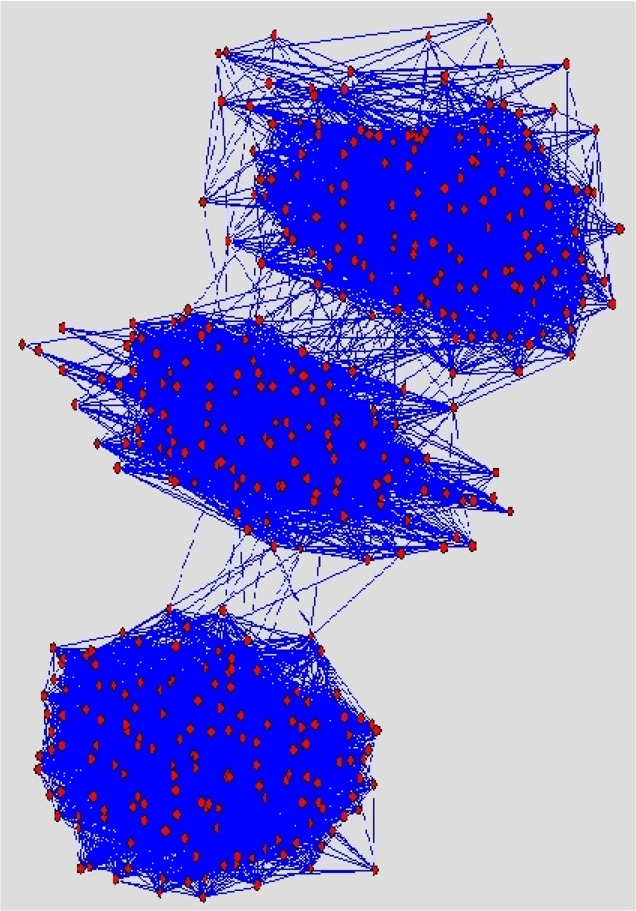

Figure 3: Random non-overlapped multimedia social network found by using YouTube

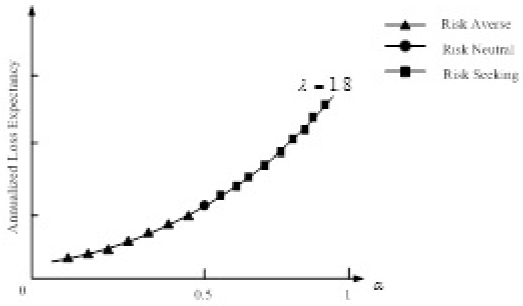

Figure 4: Effects of providers' risks opinions on ALE ($\lambda = 1.8$)

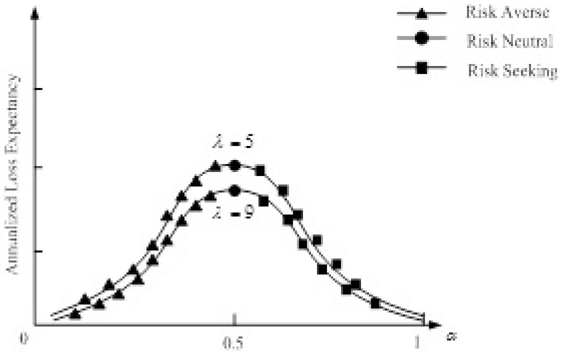

Figure 5: Effects of providers' risks opinions on ALE ($\lambda = 5$, $\lambda = 9$)

nities is involved with the random MSN, and they are written by C_1, C_2, and C_3, which are connected by some extra-community bridge edges called as weak ties compared with inner-community. We defined the size of the community followed by the "Rule of 150," which indicates that the node number of each sharing community is 150 or so for any user.

In Figure 3 networks, we accomplished the mining of the credible potential paths and their risk assessment. The experiment realizes that when two random nodes belong to different communities are input into MSN, all credible potential paths between these two nodes can be found, and risk loss expectation on the credible potential paths is evaluated.

Three groups of different data obtained from Equations (6), (7), and (8) are experimented. Tables 3, 4, and 5 show all credible potential paths from the starting point 123 to the end point 256 along with ALE experimental results. In the experiment, ALE is computed under VA=5000, EF=0.9 and UD=0.7. (Note: "-" in the table refers to it is not a credible potential path).

Table 3 show annual loss expectation ALE corresponding to three different risk preferences when $\lambda = 1.8$. The results show that in this conditions ALE will increases with α increasing.

Tables 4 and 5 show annual loss expectation ALE corresponding to three different risk preferences when $\lambda = 5$ and $\lambda = 9$, respectively. The results show that in these two conditions ALE will first increases and then decrease with α increasing. Based on the results listed by the tables above mentioned, we gained that ALE changing tendency as the following Figures 4 and 5, when λ is constant.

According to the above tables and figures, the experimental results are observed to be different. In the first case, when $\lambda = 1.8$, ALE will increases with α increasing. If the content providers are risk-averse, the loss is the lowest; if they are risk-neutral, the loss is larger; if they are risk-seeking, the loss is the maximum. In the second case, when $\lambda = 5$ and $\lambda = 9$, if the content providers are risk-averse, the loss is the lowest; if they are risk-seeking, the loss is larger; if they are risk-neutral, the loss is the maximum. In Poisson distribution, λ is average occurrence of random events within a limited time period. When the value of λ is higher, its probability distribution tends to show a standard normal distribution.

Thus, the relationships between risk loss and average risk occurrence, risk preference of content providers can be revealed: when the average risk occurrence is smaller, if the content providers are risk-averse, the loss is the

Table 2: Qualitative assessments

Target/Factor(s)	Assessment Scores						
	J1	J2	J3	J4	J5	J6	Weights
UD	82	58	73	38	95	75	-
Credible potential path length	88	39	79	50	69	85	0.6
The trust value of credible potential paths	77	84	92	30	81	52	0.4

Table 3: The credible potential paths and its ALE ($\lambda = 1.8$)

	The credible potential paths from point 123 to 256	ALE of credible potential paths ($\lambda = 1.8$)		
		$\alpha = 0.03$	$\alpha = 0.5$	$\alpha = 0.054$
1	$< 123, 341 >$, $< 341, 256 >$	47.2452	425.207	472.452
2	$< 123, 420 >$, $< 420, 256 >$	47.1301	424.171	471.301
3	$< 123, 381 >$, $< 381, 256 >$	47.0412	423.371	470.412
4	$< 123, 387 >$, $< 387, 256 >$	47.037	423.333	470.37
⋮	…	…	…	…
129	$< 123, 383 >$, $< 383, 256 >$	35.0675	315.608	350.675
130	$< 123, 353 >$, $< 353, 256 >$	34.6403	311.763	346.403
131	$< 123, 377 >$, $< 377, 256 >$	32.1209	289.088	321.209
132	$< 123, 256 >$	16.5939	149.345	165.939

Table 4: The credible potential paths and its ALE ($\lambda = 5$)

	The credible potential paths from point 123 to 256	ALE of credible potential paths ($\lambda = 5$)		
		$\alpha = 0.03$	$\alpha = 0.5$	$\alpha = 0.88$
1	$< 123, 341 >$, $< 341, 256 >$	62.9936	283.471	125.987
2	$< 123, 420 >$, $< 420, 256 >$	62.8401	282.781	125.68
3	$< 123, 381 >$, $< 381, 256 >$	62.7216	282.247	125.443
4	$< 123, 387 >$, $< 387, 256 >$	62.716	282.222	125.432
⋮	…	…	…	…
129	$< 123, 383 >$, $< 383, 256 >$	46.7567	210.405	93.5134
130	$< 123, 353 >$, $< 353, 256 >$	46.1871	207.842	92.3743
131	$< 123, 377 >$, $< 377, 256 >$	42.8279	192.726	85.6558
132	$< 123, 256 >$	22.1252	99.5633	44.2504

Table 5: The credible potential paths and its ALE ($\lambda = 9$)

	The credible potential paths from point 123 to 256	ALE of credible potential paths ($\lambda = 9$)		
		$\alpha = 0.01$	$\alpha = 0.5$	$\alpha = 0.98$
1	$< 123, 341 >$, $< 341, 256 >$	15.7484	204.729	31.4968
2	$< 123, 420 >$, $< 420, 256 >$	15.71	204.23	31.4201
3	$< 123, 381 >$, $< 381, 256 >$	15.6804	203.845	31.3608
4	$< 123, 387 >$, $< 387, 256 >$	15.679	203.827	31.358
⋮	…	…	…	…
129	$< 123, 383 >$, $< 383, 256 >$	11.6892	151.959	23.3784
130	$< 123, 353 >$, $< 353, 256 >$	11.5468	150.108	23.0936
131	$< 123, 377 >$, $< 377, 256 >$	10.707	139.191	21.414
132	$< 123, 256 >$	5.53129	71.9068	11.0626

lowest; if they are risk-neutral, the loss is larger; if they are risk-seeking, the loss is the maximum. However, under a higher average risk occurrence, if the content providers are risk-averse, the loss is the lowest; if they are risk-seeking, the loss is larger; if they are risk-neutral, the loss is the maximum.

7 Conclusion

As transmission and sharing of digital content information has some potential threats due to openness and dynamic characteristics of the multimedia social networks, risk assessment for digital right transmission is an effective way to address security problems. This article mainly evaluates security risks in the credible potential paths for the multimedia social networks, and then proposes a risk assessment method based on combination of quantitative and qualitative approaches. Next, an algorithm is designed and later used to evaluate the risks in the credible potential paths through simulation experiment. The experimental results show that the average risk occurrence and risk preference of content providers jointly influence the risk-associated loss. In the following work, we will provide the specific security risk control model based on the risk assessment results, so as to reduce piracy and misuse risks of the digital contents protected by copyrights in the multimedia social networks.

Acknowledgments

The work was sponsored by National Natural Science Foundation of China (Grant No. 61370220, No.61003234), Program for Innovative Research Team (in Science and Technology) in University of Henan Province Grant No.15IRTSTHN010, Plan for Scientific Innovation Talent of Henan Province (Grant No. 134100510006), Key Program for Basic Research of The Education Department of Henan Province (Grant No.13A520240, No.14A520048). We would like to thank the reviewers for their valuable comments, questions, and suggestions.

References

[1] C. Barbara, F. Elena, H. Raymond, and K. Murat, "Semantic web-based social network access control", *Computers and Security*, vol. 30, no. 2, pp. 108–115, 2011.

[2] C. Barbara, F. Elena, M. Sandrol and T. Davide, "A probability-based approach to modeling the risk of unauthorized propagation of information in on-line social networks", in *Proceedings of the 1st ACM Conference on Data and Application Security and Privacy*, pp. 51–62, San Antonio, United States, Feb. 2011.

[3] M. B. Chung and I. J. Ko, "Intelligent copyright protection system using a matching video retrieval algorithm", *Multimedia Tools and Applications*, vol. 59, no. 1, pp. 383–401, 2012.

[4] M. A. H. Dempster, *Risk Management: Value at Risk and Beyond*, Cambridge: Cambridge University Press, 2002.

[5] C. C. Huang, K. J. Farn, and F. Y. S. Lin, "A study on implementations of information security risk assessment: Application to chlorine processing systems of water treatment plants", *International Journal of Network Security*, vol. 16, no. 4, pp. 241–248, 2014.

[6] S. Q. Lian, X. Chen, and J. W. Wang, "Content distribution and copyright authentication based on combined indexing and watermarking", *Multimedia Tools and Applications*, vol. 57, no. 1, pp. 49–66, 2012.

[7] M. J. H. Lim, M. Negnevitsky, and J. Hartnett, "Personality trait based simulation model of the e-mail system", *International Journal of Network Security*, vol. 3, no. 2, pp. 172–190, 2006.

[8] J. Park, R. Sandhu, and Y. Cheng, "A User-Activity-centric framework for access control in online social networks", *IEEE Internet Computing*, vol. 15, no. 5, pp. 62–65, 2011.

[9] A. Sachan, S. Emmanuel, and M. Kankanhalli, "An efficient access control method for multimedia social networks", in *Proceedings of the 2nd ACM SIGMM Workshop on Social Media*, pp. 33–38, Firenze, Italy, Oct. 2010.

[10] W. Villegas, *A Trust-Based Access Control Scheme for Social Networks*, Montreal: McGill University, 2008.

[11] T. Wang, M. Srivatsa, D. Agrawal, and L. Liu, "Modeling data flow in socio-information networks: A risk estimation approach", in *Proceedings of the 16th ACM Symposium on Access Control Models and Technologie*, pp. 113–122, Innsbruck, Austria, June 2011.

[12] L. J. Yang, Z. Y. Zhang, and J. X. Pu, "Rough set and trust assessment-based potential paths analysis and mining for multimedia social networks", *International Journal of Digital Content Technology & Its Applications*, vol. 6, no. 22, pp. 640–647, 2012.

[13] L. Y. Yeh, Y. L. Huang, A. D. Joseph, S. W. Shieh, and W. Tsaur, "A batch-authenticated and key agreement framework for P2P-Based online social networks", *IEEE Transactions on Vehicular Technology*, vol. 61, no. 4, pp. 1907–1924, 2012.

[14] Z. Y. Zhang, Q. Q. Pei, L. Yang and J. F. Ma, "Security and trust in digital rights management: A survey", *International Journal of Network Security*, vol. 9, no. 3, pp. 247–263, 2009.

[15] Z. Y. Zhang, S. G. Lian, Q. Q. Pei, and J. X. Pu, "Fuzzy risk assessments on security policies for digital rights management", *Neural Network World*, vol. 20, no. 3, pp. 265–284, 2010.

[16] Z. Y. Zhang, "Digital rights management ecosystem and its usage control: A survey", *International Journal of Digital Content Technology & Its Applications*, vol. 5, no. 3, pp. 255–272, 2011.

[17] Z. Y. Zhang, Security, *Trust and Risk in Digital Rights Management Ecosystem*, Beijing: Science Press, 2012.

[18] Z. Y. Zhang and K. L. Wang, "A trust model for multimedia social networks", *Social Networks Analysis and Mining*, vol. 3, no. 4, pp. 969–979, 2013.

Zhiyong Zhang born in 1975, earned his Master, Ph.D. degrees in Computer Science from Dalian University of Technology and Xidian University, China, respectively. He has ever been post-doctoral fellowship of School of Management at Xi'an Jiaotong University, China. He is currently full-professor with Department of Computer Science, Henan University of Science & Technology, and his research interests include digital rights management and multimedia social networks, trusted computing and access control, as well as security risk management and soft computing. Recent years, he has published over 80 scientific papers on the above research fields, held 5 authorized patents and drafted 2 China National Standards. Prof. Zhang is ACM/IEEE Senior Member, IEEE Systems, Man, Cybermetics Society Technical Committee on Soft Computing, World Federation on Soft Computing Young Researchers Committee. Besides, he is responsible for Topic Editor-in-Chief, Associate Editor and Guest Editor for several international journals, and Chair/Co-Chair and TPC Member for numerous international workshops/sessions.

Lijun Yang born in 1988, is a postgraduate majoring in Computer Science, at Department of Computer Science, Henan University of Science & Technology. Her research interests include digital rights management and rough set and soft computing, multimedia social networks and security risk assessment.

Hanman Li born in 1990, is a postgraduate majoring in Computer Science, at Department of Computer Science, Henan University of Science & Technology. Her research interests include multimedia social networks analysis, mining and simulation.

Fei Xiang born in 1980, received her Master degree in Theory and New Technology of Electronic Engineering from Huaqiao University, and earned her PhD. degree in Circuits and Systems at the Electronic and Information Engineering College, South China University of Technology. She is nowadays an associate professor at Electrical Engineering College, Henan University of Science & Technology. Her research interests include Chaos cryptography and its applications.