Soc. Netw. Anal. Min. (2013) 3:969–979
DOI 10.1007/s13278-012-0078-4

ORIGINAL ARTICLE

A trust model for multimedia social networks

Zhiyong Zhang · Kanliang Wang

Received: 25 February 2012 / Revised: 17 June 2012 / Accepted: 28 June 2012 / Published online: 18 July 2012

Abstract In the emerging multimedia social networks environment, the trust relationship among users has a direct impact on the sharing and transmission mode of digital contents. To effectively assess direct or recommended trust between users, this paper proposed a multimedia social networks trust model based on small world theory. By introducing some share character factors, such as credible feedback of digital contents, feedback weighting factor and user share similarity, this model proposed a direct trust calculation window mechanism, recommended path finding algorithm, and multiple recommendation trust synthetic strategy. The simulation experiment showed that the model can dynamically update the trust value between users in real time, effectively measure the trust relationship, correctly identify malicious sharing users, and recommended trust synthesis mechanism can be adapted to trust evaluation of different types of risk scenarios.

Keywords Social networks · Small world theory · Trust evaluation · Trust model · Digital rights management

Z. Zhang (✉)
School of Management, Xi'an Jiaotong University,
Xi'an 710049, People's Republic of China
e-mail: z.zhang@ieee.org

Z. Zhang
Electronics Information Engineering College,
Henan University of Science and Technology,
Luoyang 471003, People's Republic of China

K. Wang
School of Business, Renmin University of China,
Beijing 100872, People's Republic of China

1 Introduction

As communication networks and information technology evolved, the next generation of high-speed Internet networks, 3G, 4G wireless communication networks, were gradually deployed and applied. In general, many intelligent terminals (i.e., cell phone, PDA, and panel computer) have an amazing capacity for data processing and information storage. Users can utilize all kinds of terminal units via network carriers to share copyrighted digital contents (i.e., e-book, digital image, audio and video, and Java class mobile application software) in emerging multimedia social networks (i.e., YouTube, GoogleVideo, and Youku) anytime and anywhere. This trend gave rise to serious copyright protect and security threat issues, such as the following: digital content abuse and malicious distribution (Zhiyong 2011); non-secure (embedded with malicious codes), non-credible (discrepancy between content and user claim) digital contents fragment (van Rooy and Bus 2010). Traditional ID authentication, encryption and digital watermark technologies fail to meet DRM requirements in open and distributed networks environment (Rosenblum 2007).

Multimedia social network (MSN) is an emerging network application of the typical small world theory which was established based on trust relationship between people in a realistic society. MSNs provided a platform for maintaining their social relations network for users (Le et al. 2010). Users share digital content in MSNs based on a certain relationship of trust, and trust relationship has a direct impact on the sharing and transmission mode of digital contents. Therefore, in order to correctly evaluate trust relationship between users and reduce violations and security threats in the sharing process, trust relationship in the sociology is introduced in a situation where digital content is shared in multimedia social networks to evaluate user credibility by sharing history and

other potential trust information. This paper proposes a multimedia social networks trust model (MSNTM) based on small world theory. Finally, a simulation experiment is used to verify the effectiveness of the model.

The structure of this study is as follows. The second part covers related works of trust model. The third part provides related definitions on the sharing situation of digital contents in the MSN environment, and establishes the MSNTM. The fourth part realizes MSNTM, and proposes a trust calculation window mechanism and related algorithm. The fifth part creates a three-part simulation experiment of the model by combining trust evaluation algorithm, and analyzes the results. The sixth part gives the conclusion and recommends areas for further study.

2 Related works

In the context of natural property owned by human society, trust is generally understood as a subjective and intuitive concept without a uniform definition. In sociology, trust is defined as the reliable dependence of characteristic, ability, power, and honesty of a person or thing. In information technology areas, in 1994 Marsh discussed the formal problem of trust systematically from the concept of trust. He differentiated trust content from the level of trust, and proposed a mathematical model to measure trust starting from the subjectivity of trust. This effort laid the foundation for a trust application in computers (Marsh 1994). Subsequently, Blaze et al. (1996) proposed the concept of trust management for solving security problems in internet network services. The underlying principle of the concept is to admit that safety information in an open system lacks integrality, and safety decisions of the system need to rely on a trusted third party to supply additional safety information. The authors proposed a safety decision-making framework suitable to the open, distributed, and dynamic characteristics of the web application system.

Moreover, Gambetta (2000) redefined trust in connection with the application of trust relation in an open network system. He described trust as one entity balancing the subjective probability of another entity to carry out a special conduct within a given time range and under special contextual conditions. Trust is a measurement of the credibility of a target entity before the occurrence of a special behavior. The trust model provides a relatively soft management mechanism and safety measurement method for network system by measuring and evaluating potential trust information among entities in all kinds of network environments (Rasmusson and Jansson 1996). Subsequently, more scholars have initiated deeper studies on trust model, trust evaluation, and trust managing technology from different aspects and in various application scenarios.

Luo et al. (2009) proposed an RFSTrust, a trust model based on fuzzy logic in mobile self-organizing network environments. They evaluated the trust value between nodes by establishing a fuzzy subordination function to look for a selfish node in the network and encourage the cooperation of nodes to improve network properties. This feature ensures that the RFSTrust embodies the subjectivity of trust better. But if mobile self-organizing networks are large-scale, the model can consume large resources of the network and becomes difficult to achieve. To simplify complicated transactions between users within an e-business network, Bharadwajk and Al-Shamri (2009) established the integrated fuzzy computing model covering trust and credibility. They proposed a two-stage filtering method by applying mutual benefit and historical experience to trust modeling. They enriched and expanded the concept of trust and credibility, but Bharadwajk left out data sparsity and expansibility of the model. In addition, Caverlee et al. proposed the SocialTrust trust model to guarantee the safety management of credible social information for social information system in large-scale information management. They made use of feedback from trust groups to distinguish trust relationship quality among users, and reasoned and traced transferring of trust relationship (Caverlee et al. 2010). The anti-attack capacity of SocialTrust has much room for improvement. Different from the computation method for numerical value mentioned above, Agudo et al. (2010) considered the semantic meaning of trust, and proposed a trust model based on a trust scale. They divided trust relationship into several levels. They indicated the strength of trust relationship using semantic labels for easy understanding, and to provide individual trust recommendation for users.

Moreover, domestic scholars Tang Wen et al. proposed a subjective trust model based on fuzzy set theory. They proposed a derivation rule of trust relationship by defining connecting and integrating operator calculation trust vector, and established a trust management framework in an open network scenarios (Wen and Zhong 2003). Unlike Wen, Junmao et al. (2005) proposed a trust model in a P2P and Grid mixed calculation environment based on evidence theory. They expressed trust relationship according to the concept of the confidence level of definitions. Xiaoyong and Xiaolin (2007) pointed out that static trust mechanism, based on certificate authority (CA) in public key infrastructure (PKI), cannot adapt the requirements of P2P, grid, and other large-scale distributed application systems. After comparing and analyzing the main research problems and dynamic trust relationship methods, they proposed the idea of dynamic trust modeling and management.

Small world theory, known as the six degrees of separation theory, describes an interesting phenomenon where everyone is no more than six degrees away from anyone in

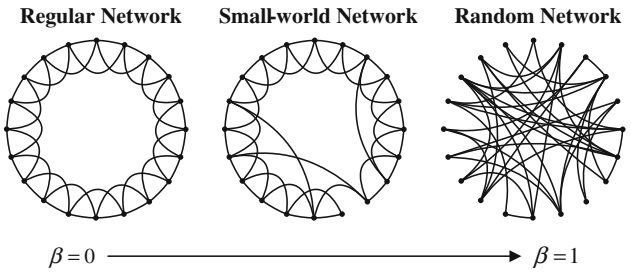


Fig. 1 WS small world network graph model (Watts and Strogatz 1998)

this world. Watts and Strogatz (1998) described small world network in the form of a graph, and established the Watts–Strogatz model (WS model), as shown in Fig. 1. A small world network is a network between a regular and random network. Small world network has two remarkable properties, namely, larger clustering coefficient and shorter characteristic path length. The larger clustering coefficient shows that the network node connection is relatively closer. The shorter characteristic path length shows that the shorter path length between optional two nodes in a network is merely required to establish the connection. Yuan et al. (2010a, b) pointed out that the trust network is the network formed based on trust relationship between nodes. They verified dynamically that trust network is a small world network. Small world characteristics are used to improve the traditional trust aware recommendation system TARS, and to reduce the time complexity of traditional TARS and improve trust prediction accuracy.

The comprehensive analysis of the above existing trust model shows that trust relationship is characterized mainly by subjectivity, dynamic variability, and weakening with path time. Trust evaluation refers to one entity measuring the behavior and capacity credibility of another entity before any special behavior occurs, based on the theoretical method of nature science. Trust models provide valuable trust referenced information for the entity, and facilitate safe and effective interaction among entities. Trust models vary, but they are limited to all kinds of particular scenes. At present, trust modeling in the digital content sharing scene remains a new challenge in the DRM field during open and distributed network times, based on the MSN environment. Therefore, this paper analyzes the digital content sharing scene characteristics according to the property of trust relationship. The research establishes the MSNTM in the Multimedia Social Networks using small world theory.

3 Establishment of the MSNTM

The MSNTM mainly includes direct trust model and recommendation trust model. First, relative definitions are given. The direct trust and recommendation trust models are then established. Finally, an overall MSNTM is proposed.

Definition 1 *User entity*. Users are divided into two types based on different sharing roles of digital content: content sharer (CS) and content requester (CR). A user can be a CS and a CR at the same time.

Definition 2 *Share session* (*SS*). The CR requests from the CS the necessary digital content. The CS responds selectively to the CR based on grasped digital content or corresponding right. The CR can also selectively receive digital content that the CS responds to. When the CR receives digital content or corresponding rights from the CS, the exchange is recorded as a share session. A share session where users obtain necessary and safe digital content or rights is called a normal share session; otherwise, it is a malicious share session.

Definition 3 *Direct trust* (*DT*). Direct trust is that trust evaluation entity according to the historical experience of digital content share from itself and the evaluated entity which obtains trust relationship from the target entity. DT is established based on the historical experience shared by the evaluating entity and evaluated entity. In comparison with trust information from other resources, the evaluating entity tends to conduct a trust evaluation on the target entity based on its own historical experience. In the MSN environment, if among users with direct digital content sharing history is direct trust relation, $DT \in [0, 1]$.

Definition 4 *Recommend trust* (*RT*). (Feng and Jian 2002). The evaluating entity indirectly obtains trust relation from the target entity based on the recommendation of another intermediate entity, which is known as indirect trust, $RT \in [0, 1]$. In the MSN environment, it is impossible for one user to directly share digital content or right with all other users in the network. Therefore, when sharing digital content with a stranger is necessary, recommended trust makes users evaluate the credibility of a stranger through the recommended information of other users.

Definition 5 *Small world trust network* (*STN*). (Yuan et al. 2010b). Users in the multimedia social network share digital contents based on a certain trust relation in the real society, and the sharing behaviors are usually restricted in a small familiar and relatively stable circle that is called user-centered STN. The nodes in a STN refer to share users; edges in the network refer to the presence of direct share relations of digital contents, and also show direct trust relation between two share users.

Definition 6 *Virtual community* (*VC*). A series of share STN can form a share virtual community based on a shared fondness and habit for digital content. Figure 2 is a share virtual community composed of four share STNs.

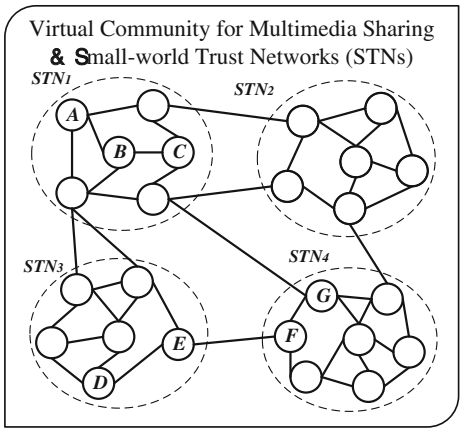


Fig. 2 Virtual community and small world trust network

According to the above definition, the relationship between user A and B in the community is a direct trust relationship within the same STN. The relation between A and C is a recommend trust relationship. The relation between user E and F is a direct trust relation among different STNs. The relation between D and G is a recommend trust relation among different STNs. This paper aims to study direct trust relation, and recommend trust relation between users in the same share community.

3.1 Usage scene of trust evaluation

In share virtual community, trust evaluation can be applied to the following two scenarios:

1. Active share user conducts a trust evaluation of the target share user based on its own historical share information, or the information recommended by another sharer before sharing digital content. According to the trust value of each user, user then decides whether to share relative digital content with every target user or not.
2. User asks for special digital content and conducts a trust evaluation of the many users who responded to the request. They obtain the required digital content selectively from users with high trust value.

3.2 MSNTM direct trust model

In a STN of digital content, there is direct digital content share history and direct trust relation between user V and U. The trust evaluation of user V and U is direct trust evaluation. As shown in Fig. 3, Dt_u^v shows direct trust value from V to U.

Considering the nature of trust and the digital content share scene characteristics, credible feedback of digital content, feedback weighting factor, time decay function, and user share similarity are introduced to evaluate direct trust Dt_u^v between user V and U.

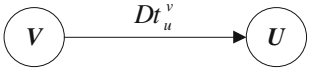


Fig. 3 Direct trust evaluation

Definition 7 *Credible feedback of digital content Rc.* After each share session, a user can feedback based on the safety credibility of the shared digital content. $Rc \in \{0, 1\}$, where 1 means that the shared digital content is safe and meets the statement of sharer about digital content, and 0 means shared digital content is not credible and not safe.

Definition 8 *Feedback weighting factor Fb.* In a share small world network, there are malicious share users. These users always give exaggerated or false feedback on digital content and depart from the realness of share session to improve trust value mutually or denigrate other normal share users. Therefore, feedback weighting factor *Fb* is introduced to balance digital content feedback credibility, $Fb \in [0, 1]$.

In direct trust evaluation, users use their credible feedback information of digital content in share session to conduct trust evaluation on other users. The value of *Fb* is 1 at this moment. In recommend trust, users conduct trust evaluation based on the recommendation of a mid-user. At this point, *Fb* relies on the trust value of the feedback user from the previous sharing period for feedback credibility.

Definition 9 *Time decay function* $\omega(t)$. The strength of trust relation changes continuously with the change of time based on the dynamics of trust and decay by time. The latest share behaviors best reflect the current credibility of users. The earlier share session has less impact on the current trust evaluation and its credible feedback. The share history information has smaller weight in trust evaluation. Therefore, time decay function $\omega(t)$ is defined as Eq. (1).

$$\omega(t) = \lceil (t_{\text{present}} - t_{\text{share}})/\delta \rceil \tag{1}$$

t_{present} refers to current time, t_{share} refers to sharing cycle where share is located, and δ refers to trust decay period, which shows trust relation decays one time every other δ sharing cycle, $\delta \geq 1$. Users can define the size of δ according to the detailed share scene. If δ is bigger, the decay of trust relation is slower with sharing cycle. If δ is smaller, the decay of trust value is faster with sharing cycle.

Definition 10 *User share similarity Sm.* In a virtual community of sharing digital content, users want to share digital content with users who have the same hobby. Establishing trust relation among users who share the same or similar hobbies is easier. As satisfactory digital content is shared, trust relation increases rapidly. Users share hobby is represented by multi-component system $\vec{p}$, as shown in Eq. (2).

$$\vec{p} = (k_1, k_2, \ldots, k_n) \tag{2}$$

n refers to type of shared digital content in share scene, and k_i refers to the sharing times proportion of digital content type i to total sharing times of users $k_i \in [0, 1]$. The share similarity of user V and U $Sm(v, u)$ can be represented by cosine similarity, as shown in Eq. (3).

$$Sm(v,u) = (\vec{p}_v \cdot \vec{p}_u)/(|\vec{p}_v||\vec{p}_u|) \quad Sm \in [0,1] \tag{3}$$

For each share session, suppose use saved the above relative share information by itself. Based on an overall consideration of the six aspects above mentioned, if the total number of share sessions of V and U is N_t, direct trust value between V and U can be shown in Eq. (4):

$$\mathrm{DT}_u^v = \frac{1}{N_t}\sum_{i=1}^{N_t}\frac{Sm(v,u) \times Fb(v,u) \times Rc_i(t)}{\omega_i(t)} \tag{4}$$

3.3 MSNTM recommend trust model

In the MSN environment, the trust relation between user U and V is recommend trust if user U does not share history with user V. To evaluate recommend trust between user U and V, V needs to ask adjacent share users and another share user to find mid-users who have a sharing history with U to establish trust recommend path. The trust value between user U and V is obtained through recommend path. Figure 4 is a schematic diagram of recommend trust. There is no direct trust relation between U and V, but there are many trust recommend paths. There is direct trust relation between adjacent users on each recommend path. Therefore, the MSNTM recommend trust model is given based on the MSNTM direct trust model.

In the MSNTM recommend trust model, the maximum recommended path length and recommended weight are introduced to obtain recommend trust value in each trust recommend path based on direct trust value between adjacent users on recommend path. According to different synthetic strategies of recommend trust, recommend trust on all recommend paths is synthesized to derive recommend trust value between U and V.

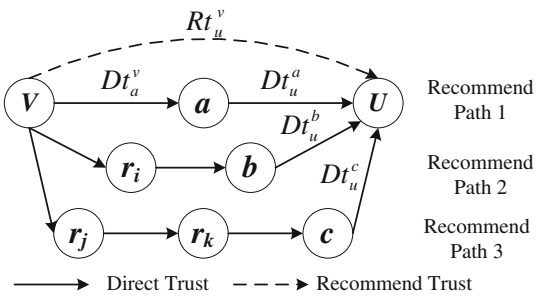


Fig. 4 Recommend trust evaluation

Definition 11 The maximum recommended path length $D_{\max}$ (Yuan et al. 2010b). In the recommend trust model, the trust recommendation path from the evaluating user to the user to be evaluated is searched. For large-scale share networks, searching all trust recommend path from evaluating user to the user to be evaluated needs higher searching time complexity. If only a small quantity of shorter trust recommend paths is selected, time complexity is reduced. However, it becomes easy to lose recommend trust information integrity, and the accuracy of recommend trust evaluation is influenced. Therefore, the maximum recommend path length $D_{\max}$ is introduced to balance the recommend trust model complexity and the accuracy of recommend trust evaluation. The recommend trust model only chooses the recommend trust path less than and equal to $D_{\max}$ to create recommend trust evaluation.

According to small world theory, trust relationship between two random share users can be established by a small quantity of trust transfer, or recommendation in a STN of digital content sharing. Therefore, the special path length of the small world network is taken as the maximum recommend path length. If l_{sw} is a special path length of sharing STN, the maximum recommendation path length is shown in Eq. (5).

$$D_{\max} = l_{\mathrm{sw}} \approx \ln(n_{\mathrm{sw}})/\ln(k) \tag{5}$$

n_{sw} refers to the scale of small world network, and k refers to the average degree of small world network.

Definition 12 Trust recommend weight is Wd. Trust has decay characteristics with recommend path length. If trust recommend distance is longer, decay of trust value increases. As the distance between recommend user and evaluating user V increases, its stated trust value to the user to be evaluated U has less weight in recommend trust evaluation. If d_r^v is the path distance from evaluating user V to recommend user R, R has direct trust relation to U. Weight that recommend user R accounts for in evaluation is shown in Eq. (6), $Wd \in (0, 1)$:

$$\mathrm{Wd}(v,r) = (D_{\max} - d_r^v + 1)/D_{\max} \tag{6}$$

Therefore, recommend trust value of V and U obtained on each trust recommendation path is shown in Eq. (7).

$$\mathrm{RT}_i(v,u) = Wd(v,r_i) \times \mathrm{RT}(v,r_i) \times \mathrm{Dt}_u^{r_i} \tag{7}$$

Different trust recommended paths gain different recommend trust values. This paper proposes a risk-averse strategy, risk-neutral strategy, and risk tolerance strategy to synthesize trust values obtained from different recommendation paths. These values are based on the user tolerance degree to potential tortious acts or safety threats during the digital content share process, until a recommend

trust value is obtained. If there is m trust recommendation paths between V and U, recommend trust value on each trust recommendation path is $\mathrm{RT}_i(v, u)$. The three recommendation trust synthetic strategies are as follows:

1. *Risk-averse strategy* Users avoid risks and safety threats that may occur during digital content sharing. They adopt the cautious recommend trust synthetic strategy, or the minimum recommend trust value on all trust recommend path is used as the final recommend trust value. This is shown in Eq. (8).
$$\mathrm{RT}_u^v = \bigwedge_{i=1}^{m} \mathrm{RT}_i(v, u) \tag{8}$$
2. *Risk-neutral strategy* Users reduce facing potential risks and safety threats during the sharing process while increasing their digital content sharing opportunities. Users adopt an eclectic recommend trust synthetic strategy, and take the average value of all available recommend trust on recommend path. This is shown in Equation (9).
$$\mathrm{RT}_u^v = (1/m) \sum_{i=1}^{m} \mathrm{RT}_i(v, u) \tag{9}$$
3. *Risk tolerance strategy* Active share users concentrate more on pursuing greater share space and share opportunity amidst potential risks and safety threats during the sharing process. They adopt an active recommend trust synthetic strategy where the maximum recommend trust on all recommend paths is used as final recommend trust value. This is shown in Eq. (10).
$$\mathrm{RT}_u^v = \bigvee_{i=1}^{m} \mathrm{RT}_i(v, u) \tag{10}$$

In the recommend trust evaluation process, user can only choose one of these strategies to synthesize the final recommend trust values at some time, according to user's tolerance degree to sharing risks.

3.4 Comprehensive trust model MSNTM

Comprehensive trust model MSNTM is given based on the above direct trust model and recommend trust evaluation model. The trust value from user V to U is represented by Eq. (11).

$$T_u^v = \alpha \times \mathrm{DT}_u^v + \beta \times \mathrm{RT}_u^v \tag{11}$$

α, β is regulatory factors, $\alpha, \beta \geq 0$ and $\alpha + \beta = 1$. If $\alpha = 1$, the trust value between V and U is obtained from direct trust. If $\beta = 1$, the trust value between V and U is obtained from recommend trust. Users can create self-definitions for α, β. Direct and recommend trust are comprehensively considered to obtain the trust value between V and U.

4 Achievement of the MSNTM and related algorithm

4.1 Direct trust calculation window mechanism

In the MSNTM direct trust evaluation model, if all share session information among users was considered to evaluate direct trust value, we faced the following problems:

1. The model had a higher calculating complexity, because too many numbers of share sessions were used to calculate many weighting factors.
2. The obtained trust value lacked comparability, because the total number of historical share sessions among different users was different.
3. Reflecting the dynamic variability of trust value was difficult, because the trust value changed continuously with the change of share cycle.
4. There were too many historical share records that accounted for a larger proportion of trust evaluation. It was difficult to reflect the small number of malicious share sessions to change trust value, and the model showed an insensitive response to malicious share.
5. The trust computing weight of historical share information long time ago was smaller due to trust time decay function. Although it had punitive impact on historical malicious share, trust value under the condition of influencing normal share session of user was easy to generate many normal share sessions without increasing trust value.

Wu et al. (2010) proposed a dual window sliding mechanism to solve the achievement problems of the trust evaluation of trust model. The mechanism used the trust difference between recent window and historical window to indicate the variable quantity of trust relation. However, this mechanism faced higher computing complexity. The present research simplified and improved the dual window sliding mechanism, and proposed a direct trust calculation window mechanism. This is shown in Fig. 5.

In direct trust calculation window mechanism, a trust calculation window with length of L_w is used to intercept L_w times of digital content share sessions between recent users. The MSNTM direct trust model is used to calculate direct trust value between users. In the new share cycle of the share virtual community, users generate new share sessions; the trust calculation window slides to the right with each share cycle to capture new share sessions and evaluate trust relation between users. The trust calculation window mechanism can reduce the MSNTM calculating complexity and improve trust evaluation effectiveness. This model can be used for a larger-scale share virtual community for digital content.

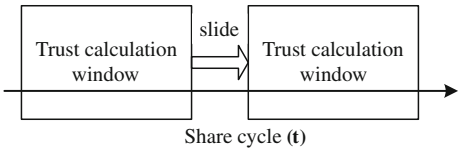


Fig. 5 Direct trust calculation window mechanism

If the number of share sessions between users in the initial situation is smaller than the length of calculation window L_w, the evaluating user can distribute a lower system trust initial value to the user to be evaluated. As the share sessions increase, the trust calculation window mechanism is gradually used to evaluate direct trust value between users.

4.2 Search algorithm of recommend path

In the MSNTM recommend trust model, initially searching and evaluating the trust recommend path between users is necessary. Then, the recommend trust value between different trust recommend paths is calculated. This study improves the depth-first search algorithm of the graph. It introduces the maximum recommendation path length D_{max} and gives the trust recommendation path searching algorithm. The description of the algorithm is following as:

4.3 MSNTM trust evaluation algorithm

This study proposes the MSNTM comprehensive trust evaluation algorithm by integrating the MSNTM direct trust model with recommend trust model, plus direct trust calculation window mechanism with recommend path finding algorithm:

Input: Adjacency matrix of sharing network A_M, user share historical information S_H, evaluating users V, and users to be evaluated U.

Output: Trust value from V to U.

1. Searching for the historical share information of V and U S_H. If the direct share session between two parties is not less than the direct trust evaluation threshold ($\text{Threshold}_{DT} = L_w$), it proceeds to the second step; otherwise, it proceeds to the third step.
2. Share historical information S_H is used to calculate share preference similarity of V and U S_m. Trust time decay factor δ is defined to calculate direct trust value DT, for evaluating subject V against the object to be evaluated U using direct trust window mechanism.
3. Calculating recommendation trust RT between users based on the direct trust relation DT.

   3.1 Calculate corresponding maximum trust propagation distance D_{max}, based on adjacency matrix of share network A_M.

Input: Share user V (starting point), U (ending point), and adjacency matrix of user share network A_M

Output: From V to U, it meets the maximum trust recommend distance path $RP_1, RP_2, \cdots, RP_m$

```
While, (Null!=Stack.top)              //the stack of the recommended route is not empty.
{If (Stack.top->number==U)
  {If (Len<= D_max +1)                //meet the maximum recommendation distance D_max
    {record this path;}
   Stack.pop();
   States[U]=0;
   Next[U]=-1;}
  Else,
   {Cur_node=Stack.top->number;
    If (neighbor (Cur_node)!=Null)
     {Node *d=neighbor(Cur_node);
      Next[Cur_node]=d->number;       //find new node
      Cur_node=d->number;
      Stack.push(Cur_node);
      States[Cur_node]=1;}
     Else,                            //do not find new recommendation node
      {Stack.pop();
      States[Cur_node]=0;
      Next[Cur_node]=-1; }
   }
}
Return RP_1, RP_2, ..., RP_m
```

3.2 In a share network scene where V and U are located, trust recommendation path finding algorithm is used to find all trust recommendation paths with lengths less than $D_{\max}$, recorded as RP_1, RP_2,…,RP_m.

3.3 For each trust recommendation path RP_i, calculate trust recommend distance decay factor Wd. Based on the direct trust value between adjacent users on trust recommendation path, it can work out the recommend trust value RT_i of path RP_i.

3.4 Final recommendation trust value RT is calculated according to different recommend trust synthetic strategies.

4. To calculate final trust value based on defined α, β regulatory factors: $T = \alpha \times DT + \beta \times RT$.
5. Return trust value T.

5 Simulation experiment and analysis of results

The simulation computer system configuration was as follows: CPU is AMD Athlon (tm) X2 240 Processor 2 with 2G RAM. Microsoft Windows 7 Ultimate OS, Ucinet 6 software package, and Microsoft Visual Studio 2005 platform were used to establish the simulation environment. Ucinet 6 is one of the more popular social network analysis softwares. This package has strong matrix analysis functions, such as algebra of matrix and multiple statistical analyses; it includes center analysis, subgroup analysis, role analysis, and statistical analysis based on replacement and other social network analysis methods.

According to the definition of the STN, there are two trust evaluation scenarios in multimedia social networks: trust relationships within STN and the trust relationships between users in different STNs. The social networks follow the "Rule of 150", and this means that the node number of the STN is 150 or so for any user.

Using the Ucinet 6 software package, we construct a typical share virtual community with two STNs. As shown in Fig. 6, each STN contains 150 nodes, and the virtual community includes all the trust evaluation scenarios in Multimedia social networks. STNs are recorded as STN1 and STN2, and the share virtual community is marked as VC. The corresponding small world parameters are shown in Table 1. They all have larger clustering coefficients and shorter characteristic path lengths.

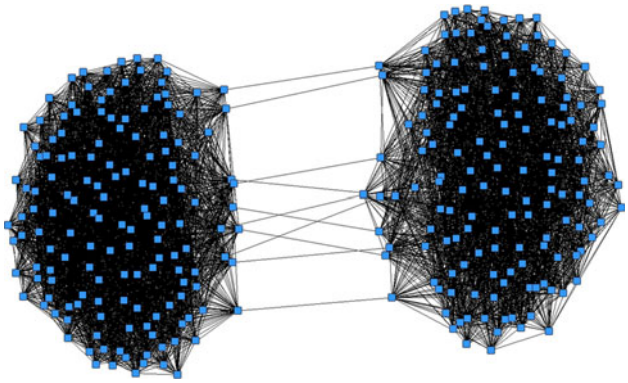


Fig. 6 Share virtual community created by Ucinet

Based on the virtual community created by Ucinet 6, C++ language programming is used to achieve trust window mechanism, search algorithm of trust recommend paths, and trust evaluation algorithm. Then, we simulate digital content share process in 100 share cycles within the virtual community.

Simulation experiments are designed as bellow:

1. In the direct trust calculation window mechanism, the length of calculation window has not been fixed, in order to improve the applicability and flexibility of the trust model; first, we should find out how the length settings of the window influence the model and confirm it.
2. Then, we verify the sensitivity of direct trust evaluation to the malicious sharing and malicious users.
3. At last, we verify, contrast and analyze effectiveness of the three recommendation trust synthetic strategies with different sharing risk types, and validate the sensitivity of the recommend trust evaluation to the malicious sharing or malicious users.

The related simulation parameters settings:

1. One share session is generated between users with share relation in one share cycle, trust decay cycle $\delta = 1$.
2. If the number of share sessions between users is less than direct trust calculation window length L_w and cannot find available recommendation trust paths,

Table 1 Network parameters of the virtual community

Network	Number of nodes	Network degree	Average	Clustering coefficient	Characteristic path length
STN1	150	5590	37.3	0.247	1.75
STN2	150	6843	45.6	0.303	1.694
VC	300	12444	41.5	0.279	2.532

users can be given a lower initial trust value T_{initial}, here we set $T_{\text{initial}} = 0.5$.

3. User can set trust threshold $T_{\text{threshold}}$ in terms of share demand and choose the users whose trust value are big than $T_{\text{threshold}}$ to share the digital contents, $T_{\text{threshold}} < T_{\text{initial}}$.
4. If share users have direct trust relationships, we set $\alpha = 1$, $\beta = 0$; if share users have recommend trust relationships, we set $\alpha = 0$, $\beta = 1$; otherwise, we set the user's trust value $T = T_{\text{initial}}$.

The simulation process is shown as description of trust evaluation algorithm. The following verifies the model property from three aspects, including direct calculation window mechanism, direct trust evaluation, and recommend trust evaluation.

In direct trust calculation window mechanism, different lengths of L_w have different impacts on trust value establishment. This simulation takes window lengths as 10, 20,…,90. It updates and calculates normal user-generated share sessions in 100 share cycles in real time. It records and observes any change in the trust value.

Figure 7 shows the impact of window length on direct trust relation establishment. The figure accumulates trust value sequence in a different length window, and makes a parallel move up to one unit for easier differentiation and observation. The simulation result shows users have only one lower trust initial value when all windows are in their initial condition. As the number of normal share sessions increases, the window mechanism updates the trust value between users in real time. Trust value increases continuously, and stabilizes gradually. This outcome reveals that trust is an accumulated process, and length of window directly impacts the establishing speed of direct trust. If the window length is longer, the share cycle required by trust value to reach a stable state is longer.

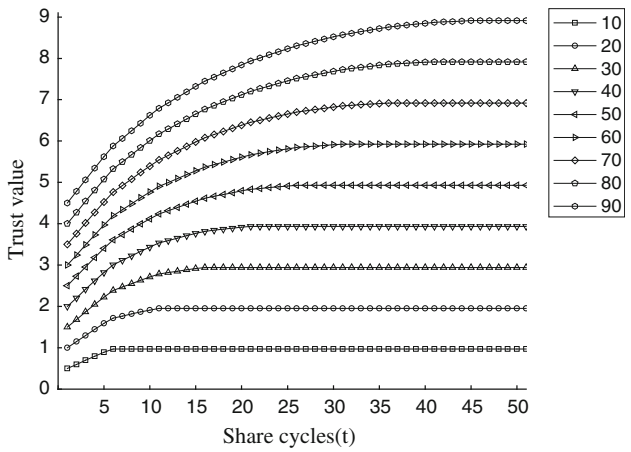
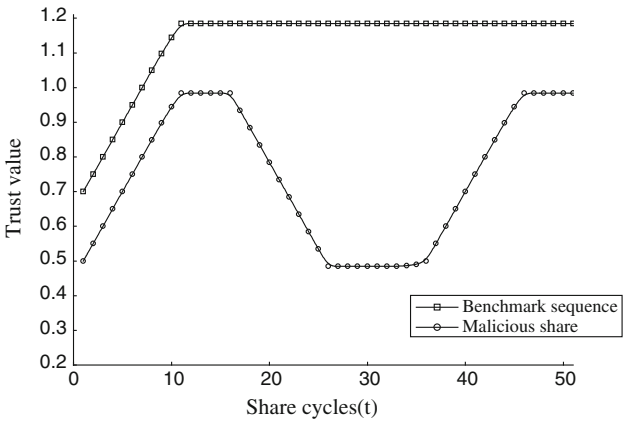


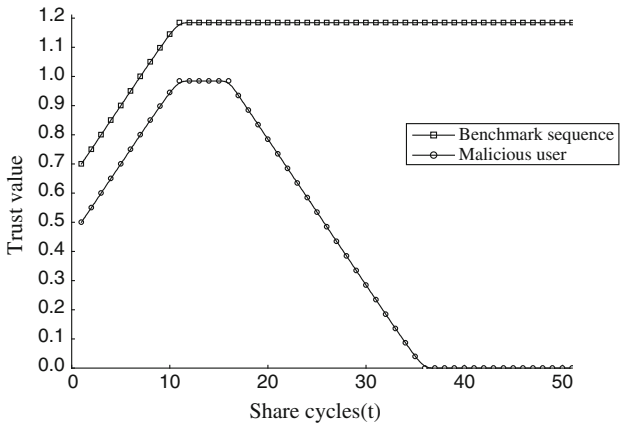
Fig. 7 Impact of window size on direct trust

In practical application, the model can decide the length of trust calculation window based on share frequency degree of digital content in share scenes. If share degree in share virtual community is more frequent, a longer trust calculation window is selected. This study regards L_w as 20 to guarantee the rapid establishment of trust relation, and to create the direct trust and recommend trust contrast experiment. This aspect reduces model calculation complexity, and reflects the gradual accumulation of trust relation better.

Figure 8 illustrates the impact of malicious share on direct trust value. For this group of simulation experiments, the complete normal share session is generated in 100 share cycles to obtain basic trust sequence. Then different numbers of malicious share sessions are added to compare the change in trust value. For easier observation, basic trust sequences in two groups of experiments make parallel moves up to 0.2 trust unit. In Fig. 8a, trust value showed an obvious downtrend as compared with basic trust sequence after a small quantity of malicious share session was added. When users create normal share session again, the trust value does not improve immediately. Direct trust regains its



(A) Effects of malicious sharing on direct trust



(B) Changes of malicious user's direct trust value

Fig. 8 Contrast simulation experiment of direct trust

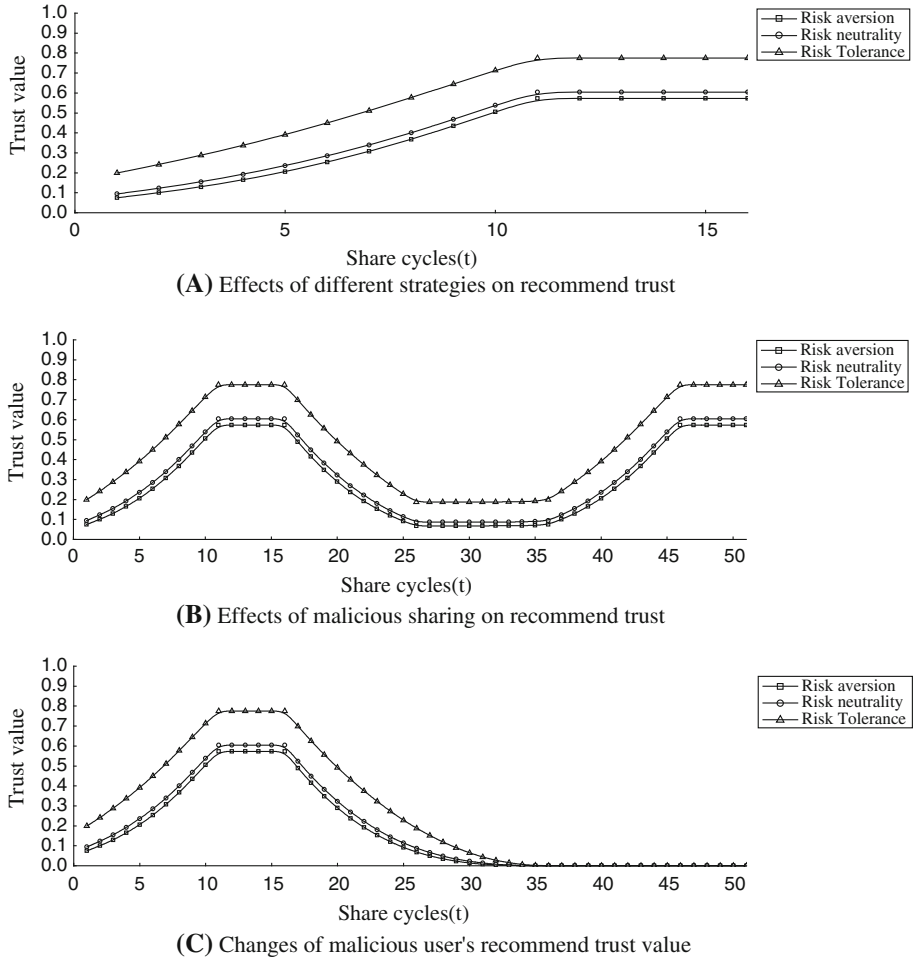


Fig. 9 Contrast simulation experiment of recommend trust

(A) Effects of different strategies on recommend trust

(B) Effects of malicious sharing on recommend trust

(C) Changes of malicious user's recommend trust value

state of basic sequence only after many normal share sessions. This condition shows that the MSNTM is sensitive to malicious share and carries a certain punitive impact. It also suggests that trust relation is easily destroyed and difficult to reestablish. Figure 8b illustrates that when malicious share users create many malicious share sessions, their trust value is reduced gradually until it closes at 0. Therefore, for different share scenes in a virtual community, the lower trust threshold $DT_{threshold}$ can be set to accurately identify malicious share users, e.g. $DT_{threshold} = 0.2$. To reduce tortious acts and safety threats in the share process, a user with trust value less than 0.2 can be removed from the share virtual community as a malicious user.

Figure 9 is contrast simulation experiment of recommend trust. Based on the above contrast simulation experiment of direct trust, a recommend trust chart between users in all share cycles under different strategies has been obtained. Figure 9a shows that recommend trust values obtained by three kinds of recommend trust synthetic strategies are on a lower level as compared with direct trust value. Risk-averse strategy has a stricter requirement for users, the obtained user recommend trust value is always in the lowest level. Whereas the recommend trust under risk tolerance strategy is obviously higher than the other two strategies. This aspect indicates that under the same share trust threshold, risk tolerance strategy easily promotes share sessions between users and provides more share opportunities for active users. Figure 9b illustrates that a malicious share session added in a share cycle rapidly lowers recommend trust under three kinds of synthetic strategies. Users must accumulate enough normal share sessions to restore recommend trust. This indicates that the recommend trust model is also sensitive to malicious share, and encourages normal share sessions between users. Figure 9c indicates that too much of malicious share in a share cycle rapidly lowers recommend trust value to 0. Setting corresponding recommend trust threshold $RT_{threshold}$ can still identify malicious share user effectively and accurately.

The above simulation experiment shows that the MSNTM can dynamically update trust value between users in real time. It adapts share scenarios of digital content in different risk types. The window mechanism has an excitation effect. The mechanism can promote users to share

digital content legally and safely based on the trust value supplied by the model; a user can share digital content with a user of higher trust value to obtain safe digital content. Trust threshold $T_{\text{threshold}}$ can be used to accurately identify a malicious share user, and reduce tortious acts and safety threats during the sharing process. This condition leads to creating a healthy and harmonious share community for digital content.

6 Conclusions

In the multimedia social network environment, the sharing methods for digital content and rights are flexible, making them vulnerable to severe tortious acts and safety threats. Trust relationship between share users has a direct impact on the sharing and transmission method of digital content. To correctly evaluate trust relationship between users, this study proposes a MSNTM based on small world theory. This model distinguishes direct trust and recommendation trust relationship between users. This research proposes a direct trust computing window mechanism and trust recommend path finding algorithm according to the decay characteristics of trust with time and path, and comprehensively considering credible feedback of digital content, feedback weighting factor, user share similarity, and other share characterization factors. The simulation experiment shows that the trust calculation window mechanism can accurately evaluate and dynamically update trust relationship between users. It has more reference and comparability to users. Multiple recommend trust synthetic strategy makes the model adaptable to digital content share scenarios with different types of risks. It also makes it sensitive to malicious share; it boycotts malicious share behavior and promotes a normal, safe digital content, or right share between users. In trust evaluation algorithm, trust threshold $T_{\text{threshold}}$ is introduced to enable MSNTM to effectively identify malicious share users, and helps create a better multimedia social network share environment. The key point for future work is to conduct further studies on the anti-attack capacity and effectiveness of the MSNTM by integrating the trust mechanism proposed in this study.

Acknowledgments The work was sponsored by the National Natural Science Foundation of China (Grant No. 61003234), Program for Science & Technology Innovation Talents in Universities of Henan Province (Grant No. 2011HASTIT015), China Postdoctoral Science Foundation (Grant No. 20100471611), and Henan University of Science & Technology Doctors Research Fund (Grant No. 09001470).

References

Agudo I, Fernandez-Gago C, Lopez J (2010) A scale based trust model for multi-context environments. Comput Math Appl 60:209–216

Bharadwajk KK, Al-Shamri MYH (2009) Fuzzy computational models for trust and reputation systems. Electron Commer Res Appl 8:37–47

Blaze M, Feigenbaum J, Lacy J (1996) Decentralized trust management. In: Proceedings of the 17th symposium on security and privacy. IEEE Computer Society Press, Oakland, pp 164–173

Caverlee J, Liu L, Webb S (2010) The SocialTrust framework for trusted social information management: architecture and algorithms. Inf Sci 180:95–112

Feng X, Jian L (2002) Research and development on trust management of web security. J Softw 13(11):2057–2064 (in Chinese)

Gambetta D (2000) Can We Trust Trust? In: Gambetta D (ed) Trust: making and breaking cooperative relations. Department of Sociology, University of Oxford, pp 213–237

Junmao Z, Shoubao Y, Jianping F, Mingyu C (2005) A grid & P2P trust model based on recommendation evidence reasoning. J Comput Res Dev 42(5):797–803 (in Chinese)

Le K, Jiwu J, Yuewu W (2010) The trust expansion and control in social network service. J Comput Res Dev 47(9):1611–1621 (in Chinese)

Luo J, Liu X, Fan M (2009) A trust model based on fuzzy recommendation for mobile ad-hoc networks. Comput Netw 53:2396–2407

Marsh SP (1994) Formalizing trust as a computational concept. University of Stirling, Scotland

Rasmusson L, Jansson S (1996) Simulated social control for secure internet commerce. In: Proceedings of the 1996 new security paradigms workshop. ACM, New York. doi:10.1145/304851.304857

Rosenblum D (2007) What anyone can know: the privacy risks of social networking sites. IEEE Secur Priv 5(3):40–49

van Rooy D, Bus J (2010) Trust and privacy in the future internet—a research perspective. Identity Inf Soc 3:397–404

Watts DJ, Strogatz SH (1998) Collective dynamics of 'small-world' networks. Nature 393:440–442

Wen T, Zhong C (2003) Research of subjective trust management model based on the fuzzy set theory. J Softw 14(8):1401–1408 (in Chinese)

Wu F, Li HH, Kuo YH (2010) Reputation evaluation for choosing a trustworthy counterparty in C2C e-commerce. Electron Commer Res Appl 10:428–436

Xiaoyong L, Xiaolin G (2007) Research on dynamic trust model for large scale distributed environment. J Softw 18(6):1510–1521 (in Chinese)

Yuan W, Guan D, Lee YK (2010a) Improved trust-aware recommender system using small-worldness of trust networks. Knowl-Based Syst 23:232–238

Yuan W, Guan D, Lee Y-K, Lee S (2010b) The small-world trust network. Appl Intell. doi:10.1007/s10489-010-0230-7

Zhiyong Z (2011) Digital rights management ecosystem and its usage controls: a survey. Int J Digit Content Technol Appl 5(3):255–272