applied sciences

MDPI

Article

Reliability Model Based Dynamic Multi-Level Trust Analysis

Li Zhang [1], Bin Zhang [1], Anqing Liu [1] and Liudong Xing [2,*]

[1] Software College, Northeastern University, Shenyang 110169, China; zhangl@swc.neu.edu.cn (L.Z.); zhangbin@mail.neu.edu.cn (B.Z.); 1871105@stu.neu.edu.cn (A.L.)

[2] Electrical and Computer Engineering Department, University of Massachusetts Dartmouth, North Dartmouth, MA 02747-2300, USA

* Correspondence: liudong.xing@umassd.edu

Received: 11 July 2020; Accepted: 14 August 2020; Published: 24 August 2020

Abstract: Trust assessment is of great significance to related issues such as privacy protection and rumor transmission in online social networks. At present, there are mainly two types of trust models: discrete type and continuous, type. Little work has been done on considering distrust and trust at the same time, especially on the propagation mechanism of distrust. To this end, this paper proposes a multilevel trust model and a corresponding trust evaluation method based on a reliability model called multivalued decision diagrams (MDDs). The proposed trust model combines characteristics of both discrete and continuous trust and considers the dynamic changing mechanism of the multilevel trust. The propagation of distrust and conflicts of opinions are also handled. Experimental results show that the proposed method outperforms other existing methods.

Keywords: dynamic trust; multi-level trust; reliability model; multivalued decision diagram

1. Introduction

Trust is an important reference data for both parties to interact in online social networks (OSNs). Objective and accurate trust can reduce the risk of interaction, such as the behavior of malicious users. It is quite difficult for the OSN users to estimate the risk of interacting with others in the networks before determining to perform interactions [1]. Therefore, an objective and reliable trust evaluation mechanism becomes particularly important for OSNs. But trust is a complex concept, which contains both sociological and psychological factors. Thus, it is often complex and difficult to model and quantify trust in OSNs [2].

Trust representation models usually include two types: discrete [3–11] and continuous [12–15]. Refs. [3,5,7] use multiple discrete trust degrees to describe the trust relationships, and edge sign is used in [6]. In particular, Refs. [8,10,11] express trust from multiple perspectives. Ref. [4] uses the matrix of trusts and the matrix of distrusts to complete the expression of trust between users. Refs. [13,15] generate the final trust value by integrating trust from multiple perspectives. Furthermore, Refs. [12,14] respectively introduce measurement and error propagation theory and network flow. The discrete multi-level trust model refers to a trust modeling method, which divides the trust relationship between users into multiple levels or perspectives to map the different degrees of description in the real-world [13]. The discrete multi-level trust model refers to a trust modeling method which divides the trust relationship between users into multiple levels to map the different degrees of description in the real-world [8]. After an interaction ends, the user can choose a trust level for the other party based on their feelings. Multi-level models based on this modeling approach [9–11] are convenient for users to give intuitive evaluations that fit their feelings. However, there are two problems with this approach: Firstly, this model can only rank trust and cannot obtain accurate trust. It is not accurate

enough to describe trust. Secondly, it is not easy to find a sound computational principle based on this model. The continuous trust model is just the opposite. The continuous model can more accurately describe the trust and is easier to calculate. However, the continuous model is not easy for users to accurately express their feelings as a real value. Therefore in [16], a multi-level trust representation model with probability values was proposed. A trust calculation method based on multi-valued decision diagram (MDD) was designed. Combining the characteristics of discrete and continuous models, this method not only can facilitate the rating by users, but also can express trust more accurately. However, the model of [16] treats distrust simply as a level of trust without considering characteristics of distrust. Thus, the propagation and computation rules for the distrust are assumed to be the same as those for trust.

In the actual interaction process, the information regarding not only who to trust but also who cannot be trusted is critical to minimize and even avoid risks [17]. Actually, it is often more important to predict distrust for a trust or to trustee [18,19]. Studies in [20,21] show that trust and distrust coexist in the human brain. Sometimes we have no or little contact with the predicted party, so simply classifying the party as being trustful or distrustful is biased. In Ref. [19], the authors talk about the concepts of trust and distrust. There are two perspectives of trust and distrust. One of the opinions is that distrust is the opposite of trust and the other one is distrust is not only the opposite to trust. The early approaches model the trust by a single real number, completely ignoring the difference between distrust and neutrality [22,23]. It is clear that the indiscriminate definition of distrust and neutrality as lack of trust is unreasonable [24]. Therefore, in addition to trust and distrust, there is also a type of information that expresses trust that is uncertain or unfamiliar. Distrust should be distinguished from neutrality, and at the same time be used as a description of the trust relationship between users like trust. In addition, propagation and combination calculation methods for distrust and neutral are also different from those for trust. Trust can be transmitted, but distrust cannot be propagated [18,25]. Therefore, in the trust model, distrust and uncertainty cannot be dealt with in the same way as trust; they should be handled separately.

Dynamicity is one of the properties of trust, which can change frequently with new experiences [26]. New experience is important, but its impact on trust can be neither too fast nor too slow. The dynamicity of trust can be formalized through trust update functions [27]. Reasonable dynamic changes can effectively curb the damage of malicious nodes to trust evaluation. Most of the researches on dynamic trust are for continuous or binary trust [27–32]. In fact, it is more practical to do dynamic trust and distrust aggregation in multi-level.

In view of the above problems, this paper proposes a multi-level trust model that takes into account distrust and uncertainty. This model combines the characteristics of continuous trust model and discrete trust model, which not only can facilitate data collection, but also can relatively accurately describe the trust of each level. At the same time, distrust and uncertain propagation and combination calculations are considered to complete accurate mapping of user trust descriptions in the real world. Based on the new trust model, we extend the MDD-based method of [16] for trust evaluation, which addresses the non-independent trust transfer path problem during the MDD model generation process.

Section 2 presents related work on trust modeling and evaluation for OSNs. Accordingly, we describe our trust model and the dynamic rules of trust relationships in Section 3. In Section 4, in order to validate our main thought, we conduct a series of experiments to analyze the performance of our algorithm. After a discussion of the results in Section 5, we conclude this study and provide some directions of future work in Section 6.

2. Related Work

Many literatures have established different trust models. Each model models trust from different angles and describes the trust in different ways. Refs. [4–7] describes the trust information as binary discrete values, that is, trust and distrust. This way is simple to describe and easy to calculate the combined trust, but the value is rough. Another form of discrete trust representation is multilevel

discrete values [9]. This way describes the trust just like "very trust, trust, distrust, very distrust". It can describe the trust more accurately and is easy for users to choose, but this method is not convenient for combined calculation of trust [26], so there is less research on it. Continuous trust information more intuitively and accurately represents the user's beliefs, probabilities, etc., but it is not good for users to accurately define their own trust. Therefore, in [16], a multi-level trust model based on probability values is proposed, which combines the characteristics of continuous model and discrete model.

Although many literatures indicate that using distrust information when calculating trust information can improve the accuracy of prediction, in fact, not many literatures deal with distrust alone. The two important issues in distrust research are distrust propagation and calculation [4,26,31]. Ref. [10] uses subjective logic to express trust information, which includes trust, distrust and uncertainty. Here distrust must be propagated by trust. Uncertainties in subjective logic are distinguished into the posteriori uncertainties and priori uncertainties in [32]. Ref. [33] regards distrust as a separate concept from trust. However, this model adopts the same calculation model for trust and distrust. An important difference in the calculation of distrust and trust is the difference in the way of propagation. In [4], the author discusses the transitivity of distrust and adopts the propagation rule of "the enemy of the enemy is a friend". "Don't take into account your enemies' opinions" is adopted in [34]. That is if A distrust B, then we can't adopt B's opinions. Ref. [34] introduced that not only trust and distrust are important, but lack of confidence also distinguishes distrust from low-level trust. Therefore, distrust needs to be considered separately and the dissemination mode of distrust is different from trust. In addition to trust and distrust, uncertainty is also an indispensable part of trust information.

Ref. [27] introduces six dynamic trust models, including blindly positive, blindly negative, slow positive, fast negative, balanced slow, balanced fast and slow negative, fast positive. In the real world, a good reputation is not easy to construct, but trust is easier to lose than to gain [27]. Ref. [28] designs a Bayesian based trust model, but it penalizes too strong. Ref. [27] proposes a SinAlpha trust aggregation engine which adopts trust increase slowly but decrease fast. DyTurst [35] considers the dynamics of trust from changes in time, and considers the changes in trust weights during the propagation process. However, the current research is aimed at binary trust and does not support the dynamic changes of multi-level trust.

In this paper, the direct trust relationship is modeled by multi-level trust model. The distrust propagation mechanism is discussed specially. A corresponding trust evaluation method, which is based on MDDs is proposed. This method combines the information on all paths between two parties within OSN, especially considering the propagation rules on one path and the integration rules on all the paths. The dynamic changes of different levels, especially on distrust and uncertainty are addressed.

3. Multi-Level Trust Model and Problem Statement

The multi-level trust representation model of [16] combines the merits of discrete trust representation and continuous trust representation. This section extends the model of [16] by considering distrust and uncertainty.

3.1. Multi-Level Trust Representation Model and Problem Statement

In this work, a social network is modeled as a probabilistic directed graph $G = (V, E)$, where V is nodes set and E is direct links set. All edges in E have corresponding probability values. Suppose p and q are two nodes in V and there is a direct link A between these two nodes. The trust information of A has $k + 1$ levels from trust Level 0 (totally distrust) to trust Level k − 1 and an uncertainty level u, as demonstrated in Figure 1.

Trust information vector of link A is indicated as $\mathrm{dir}(A) = \left(t_{A,0}, t_{A,1} \ldots, t_{A,k-1}, u_A\right)$, here $0 \leq t_{A,0}$, $t_{A,1} \ldots, t_{A,k-1}$, $u_A \leq 1$ and $\sum_{i=0}^{k-1} t_{A,i} + u_A = 1$. $t_{A,i}$ represents the trust probability of A occupying level i. Particularly, $t_{A,0}$ represents the probability of totally distrust. u_A is the probability of uncertainty (meaning that party p has no idea or is confused about party q).

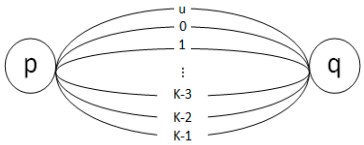


Figure 1. Multi-level trust model.

MDD is one of the reliability models. It consists of a set of decision branches and two sink nodes, which represents the system is in a certain state or not [36]. Usually a system includes many multi-state components. Suppose A is one of the multi-state components and x_A is corresponding multivalued variable. The MDD for A has k outgoing edges. The j-edge ($0 \le j \le k-1$) represents the jth value of x_A. Each non-sink node in the MDD encodes a multi-valued function using the case format as Equation (1):

$$\begin{aligned} F &= A_0 * F_{x_A = 0} + A_1 * F_{x_A = 1} + \ldots + A_{k-1} * F_{x_A = k-1} \\ &= case\left(A, F_{x_A = 0},\ F_{x_A = 1}, \ldots, F_{x_A = k-1}\right) \\ &= case(A,\ F_0,\ F_1, \ldots, F_{k-1}) \end{aligned} \tag{1}$$

The operating rules of MDD can be referred to in [37].

Figure 2 shows the MDD representation of link A with $k+1$ trust levels.

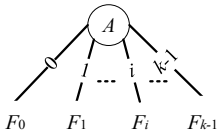


Figure 2. Multivalued decision diagram (MDD) for connection A.

Problem Statement

Given a social network $G = (V,\ E)$, $p, q \in \mathrm{V}$, $\exists$ for at least one path from p to q. The problem is to calculate the probability of each trust level toward user q from user p's perspective. The notations used in this paper are shown as Table 1.

Table 1. Notations.

Notation	Meaning
$dir(\mathrm{A}) = \left(t_{A,0},\ t_{A,1} \ldots, t_{A,k-1},\ u_A\right)$	The normalized trust information on the arc A. u_A is used to represent the probability of unknown (uncertainty).
$P_p^q(i) = \left(P_{i,0},\ P_{i,1} \ldots, P_{i,k-1},\ U_i\right)$	The trust information of the ith path from p to q.
$Totall(\mathrm{p}, \mathrm{q}) = \left(T_{(p,q),\,0},\ T_{(p,q),1} \ldots, T_{(p,q),k-1},\ U_{(p,q)}\right)$	The aggregated trust information of all the paths going from node p to node q.

3.2. Multi-Level Trust Evaluation

The trust evaluation between two users mainly includes two aspects. The first is how to evaluate the trust information of a path. The second is how to combine the trust information of multiple paths. Trust propagation and combination rules are keys to trust evaluation. In this paper, trust information includes trust, distrust and uncertainty. The propagation methods of these three types of information are different.

We take an example of three parties A, B and C (Figure 3) to illustrate the trust propagation rules in this paper.

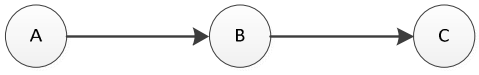


Figure 3. Example of the three parties' relationship.

Table 2 shows the propagation rules between these three parties, where T represents trust at any of levels 1 to $k-1$, D is distrust or Level 0, U is level uncertainty. In the case of T, Table 3 shows the detailed propagation rules.

Table 2. Trust propagation rules between three parties.

Situation	A→B	B→C	A→C
1	T	T	T
2	T	D	D
3	T	U	U
4	D	T	D

Table 3. Trust propagation rules of T in detail.

Case	A→B	B→C	A→C
1.1	i ($0 <= i < k-1$)	j ($i <= j$)	i
1.2	i ($0 < i <= k-1$)	j ($j < i$) $i >= j$	j

For Situation 1 in Table 2, most of the literatures adopt the principle of "friend's friend is a friend". Trust is propagated to C through B, then A trust C with a decaying degree. For multi-level trust, there are two cases in Table 3. When the trust level of a link is less than that of the other link in Figure 3, the smaller one is selected as the final trust level.

For Situation 2 in Table 2, we adopt "friend's enemy is enemy", that is if A trusts B, B distrusts C, then A distrusts C with a decaying degree.

For situation 3 in Table 2, if A has a clear opinion on B, but B does not have a certain opinion on C, then A's trust in C is uncertain.

The principle an "enemy's friend is enemy" is adopted in Situation 4, so A distrusts C.

However, we don't give a specific solution to the problem of whether or not the distrust can be propagated by means of the distrust, that is, how the enemy of the enemy should deal with it. Refs. [6,34] treat enemy's enemies as friends and [3,4] treat them as enemies. There is no certain result for this kind of propagation behavior. We cannot determine whether the enemy of the enemy can become our ally. As mentioned in [25], according to the results in the Epinion dataset, the enemy of the enemy has a 50% chance of being an ally, 50% chance of being an enemy. Therefore, our model conservatively chooses to treat the enemy of the enemy as uncertainty. It means that if a competitor whom you distrust tells you to distrust someone, you might be not able to decide which kind of attitude to take, so you likely choose to be neutral. That is, there are two or more links with distrust on a path, only uncertain trust information (uncertainty) can be generated.

In addition, for the advice of strangers, we adopt a way that is consistent with our daily life: ignore it. Corresponding to our model, when there is a link in a path that uses uncertainty trust, this path can only generate neutral trust no matter how the other links on this path choose. That is, if a stranger tells you the attitude he holds towards someone, you might decide not to take into account his opinion and keep neutral because you do not know him sufficiently.

In our model, trust can be propagated by trust and distrust, but distrust can only be propagated by trust. Based on the above situations, we make the following definitions:

Definition 1. *Multi-level trust propagation operator $\oplus$ in Equation (2) is defined as:*

$$P_A^B(A \to B \to C) = dir(A,B) \oplus dir(B,C) \tag{2}$$

1. *If A trusts B on level i ($0 \le i \le k-1$, k is the number of levels) and B trusts C on level j ($i \le j \le k-1$), then the trust level of A to C is i; if B trusts C on level i ($0 \le i \le k-1$, k is the number of levels) and A trusts B on level j ($i \le j \le k-1$), then the trust level of A to C is i. The probability of level i ($0 <= i <= k-1$) on this path is shown as Equation (3):*

$$P_{(A,C),\,i} = t_{<A,B>,i} * \sum_{j=i+1}^{k-1} t_{<B,C>,j} + t_{<A,B>,i+1} * t_{<B,C>,i+1} + t_{<B,C>,i} * \sum_{j=i+1}^{k-1} t_{<A,B>,j} \quad (3)$$

2. *If A distrusts B and B distrusts C, then the trust level of A to C is uncertainty. If the trust level of A to B or B to C is uncertainty, then the trust level of A to C is uncertainty. Then the probability of level uncertainty on this path is shown as Equation (4):*

$$U_{A,B,C} = t_{<A,B>,0} * t_{<B,C>,0} + u_{<A,B>} * (1 - u_{<B,C>}) + u_{<B,C>} * (1 - u_{<A,B>}) \quad (4)$$

Definition 2. *The trust level and probability on a path:*

1. *The trust level of path i is j, if and only if at least one link has trust level j, and the remaining links have a trust level higher than j.*
2. *The trust level of path i is uncertainty, if and only if at least two links on the path has trust level 0 or at least one link has trust level of uncertainty.*

Suppose the ith path from A to B with nodes sequence $A, q_{1,} q_2 \ldots, q_n, B$. Then the trust calculation on this path can be calculated as Equation (5).

$$P_A^B(i) = dir(p, q_{1,}) \oplus dir(q_1, q_2) \oplus \ldots \oplus dir(q_n, r) \quad (5)$$

3.3. Multipath Combination

In social networks, there is not only one reachable path between two nodes; in most cases, there are often multiple communication paths between two reachable nodes in the network. Moreover, the multiple paths may not be independent. Therefore, we need to integrate the trust information on multiple independent/dependent paths for accurate trust evaluation.

Consider two paths from A to C. If the trust level of any paths is uncertainty, then the trust information of the other path is adopted; if neither path is uncertainty, the lower trust level of the two roads is used. Table 4 shows the combination rules.

Table 4. Trust combination rules of two paths from A to C.

Case	Path 1	Path 2	Combined Trust
1	i ($0 < i <= k-1$)	j ($i <= j$)	i
2	D	D	D
3	T	D	U
4	D	T	U
5	T/D/U	uncertainty	T/D/U
6	uncertainty	T/D	T/D

For cases where the paths are not independent and have links dependencies, the dependencies can be addressed when performing a logical AND or OR operation on the two paths during the MDD model generation process, which is described in [16]. Suppose $T_{(p,q),\,i}$ represents the overall trust score at level i from p to q in social network G. Using the heuristic method in [36,37] to order the links at first, generating the MDD model for level i from the social network G.

We can traverse the graph to find all the paths from the source node p to the sink node q. Then the MDD of trust level i for each path can be generated by Definition 2. Generate the final MDD model by performing logic operations on path MDDs according to Table 4. Evaluate $T_{(p,q),\,i}$ according to Equation (3).

4. Dynamic Changes in Trust

Trust information is continuously accumulated during the interaction process. Therefore, trust information will continuously change as time proceeds. Moreover, changes in the trust information

between two users may affect the trust information of other users related to them. Assume User A wants to check the trust level and probability of another User B. There are two different situations. The first one is A has no relation with B and A's friends have no relation with B too; the second one is A has no relation with B, but A's friends have relations with B. When some events happened between A and B, then A will rate B on a trust level. The rate will dynamically affect the trust scores on each level of both A on B and A's friends on B.

When B is a new user or A has no relation with B, then A has uncertainty about B. The initial trust information of A to B is $dir((A,B)) = (0,\ 0\ldots,0,\ 1)$, that is all the trust probabilities are 0 but uncertainty probability is 1.

After a transaction or some events, A will have an impression on B. A rates B on trust level i. Then A's direct trust scores on all levels to B will change. Assume there are k levels. $t_{A,i}$ $(i = 0, \ldots\ k-1)$ represents the probability of trust level i of link A. Generally, "trust growing slower, declining faster" and "slow negative but fast positive", if a rating/vote on level i happens, $t_{A,i}$ is increased by Equation (6).

$$\begin{gathered} t_{A,i} = \alpha_1.sigmoid(\beta_i) + \alpha_2\ 0 < \alpha_1 \le 1,\ 0 \le \alpha_2 \le 1 - \alpha_1 \\ \beta_i = \beta_i + \delta \times \tfrac{(k-i)}{kn}\ 0 < \delta \le 5 \end{gathered} \tag{6}$$

In Equation (6), α_1 and α_2 are constant values. β_i ranges from -5 to 5, allowing for $t_{A,i}$ within the range [0,1]. The incremental step of β_i is also shown in Equation (6). $\delta \times \frac{i+1}{(k++1)n}$ represents the growth pace of β_i. n is the numbers of transactions. The higher i is, the smaller the increase is. That is the trust information will converge to 1.

The updates should guarantee $t_{A,0}+t_{A,1} + \ldots t_{A,k} + u_A = 1$. If t_{Ai} is increased by Δt_{Ai}, the probabilities of other levels should be decreased by Δt_{Ai}. u_A is the probability of uncertainty which means the transactions are not enough to eliminate uncertainty. We define the dynamic decrease of uncertainty as follows:

1. if $u_A > \Delta t_{Ai}$, then $u_{\mathrm{A}} = u_A - \Delta t_{Ai}$ and $\Delta t_{Ai} = 0$;
2. if $u_A \le \Delta t_{Ai}$, then $u_A = 0$ and $\Delta t_{Ai} = \Delta t_{Ai} - u_A$.

The lower level trust decreases faster than the higher level trust, and the uncertainty score turns to 0 faster with lower level ratings. Therefore, good transactions are encouraged.

The changes of $t_{Aj}(0 \le j < k, j \ne i)$ depends on the distance between j and i. For level $i-1$ is closer to level i than level $i-2$, the change in $t_{A,\,i-2}$ will be greater than the change in $t_{A,\,i-1}$. Therefore, $t_{Aj}(0 \le j < k, j \ne i)$ is changed as Equation (7).

$$t_{A,j} = t_{i,\,j} - \frac{\Delta t_{Ai}}{i^2 - i + \frac{k^2}{2} - k * i}\left|i - j\right|, 0\ \le j! = i \le k-1 \tag{7}$$

5. Examples

Consider an example OSN showed in Figure 4, which involves four parties and four direct links [16].

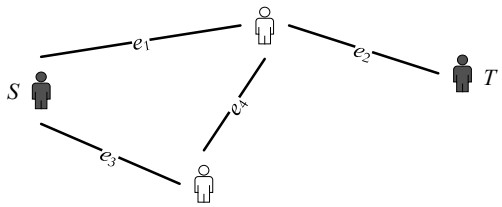


Figure 4. Social network example.

To simplify the illustration, we assume that trust distribution is identical in both directions of a direct link. So the example can be simplified to an undirected graph. Suppose every link has four trust levels. The initial trust scores on all the direct links are (0, 0, 0, 1), which means only uncertainty has probability of 1, other levels have probability of 0.

Assume e_1, e_2, e_3 received rates on Level 0, Level 1, Level 2, respectively. e_4 received five rates on Level 0, Level 1, Level 2, Lvel 2, Level 2. Then the trust score of the links are updated using Equation (6) as shown in Table 5. Here we set $\alpha_1 = 0.1$, α_2= 0.05, $\delta = 4, k = 3$, and initial value of β_i is 4.

Table 5. Updated trust scores/probabilities.

Link	Level 0	Level 1	Level 2	Uncertainty
1	0.584	0	0	0.416
2	0	0.215	0	0.785
3	0	0	0.122	0.879
4	0.543	0.376	0.081	0

From Table 5, the increase of trust score of Level 0 is always faster than other levels. Only two rates on Level 0 will make it fully distrust. However, for Level 2, it needs at least 10 rates on Level 2 so that the uncertainty can be eliminated. For e_4, a rate on Level 0 is not easy to be eliminated by few times rates on other levels, especially the first few rates.

Assume Table 6 shows the direct trust scores of example.

Table 6. Trust score distribution of the example social network.

Link	Level 0	Level 1	Level 2	Uncertainty
1	0.1	0.5	0.4	0
2	0.2	0.5	0.3	0
3	0	0.6	0.4	0
4	0	0	1	0

Following the method in Section 3.3, the links should be sorted at first. Assume we obtain the order of $e_1 < e_2 < e_3 < e_4$.

In Step 2, two paths are identified: $P_1 = \{e_1, e_2\}$ and $P_2 = \{e_3, e_4, e_2\}$. We take $T_{(S,T),\,1}$ and $T_{(S,T),u}$ as examples to show the MDD generating process and trust evaluation process in Equation (8).

$$\begin{aligned} T_{(S,T),\,0} &= P_{1,0} \times P_{2,0} + P_{1,u} \times P_{2,0} + P_{1,0} \times P_{2,u} \\ T_{(S,T),\,1} &= P_{1,1} \times P_{2,1} + P_{1,1} \times P_{2,2} + P_{1,2} \times P_{2,1} \\ T_{(S,T),\,2} &= P_{1,2} \times P_{2,2} + P_{1,u} \times P_{2,2} + P_{1,2} \times P_{2,u} \\ T_{(S,T),\,u} &= P_{1,u} \times P_{2,u} + P_{1,0} \times (P_{2,1} + P_{2,2}) + P_{2,0} \times (P_{1,1} + P_{1,2}) \end{aligned} \tag{8}$$

Assume $M_{i,j}$ represents MDD of the ith path with trust level j. The overall MDD of trust level 1 is obtained as Equation (9):

$$\begin{aligned} M_{(S,T),\,1} = (M_{1,1} \text{ AND } M_{2,1}) \text{ OR } (M_{1,1} \text{ AND } M_{2,2}) \text{OR } (M_{1,2} \text{ AND } M_{2,1}) \\ \text{OR}(\ (M_{1,u} \text{ AND } M_{2,1}) \text{ OR } (\ (M_{1,1} \text{ AND } M_{2,u}) \end{aligned} \tag{9}$$

Similarly, the overall MDD of other trust levels from S to T can be obtained. And all the overall MDDs are shown in Figures 5–8.

Figure 5. MDD for $T_{(S,T),\,0}$.

Figure 6. MDD for $T_{(S,T),\,1}$.

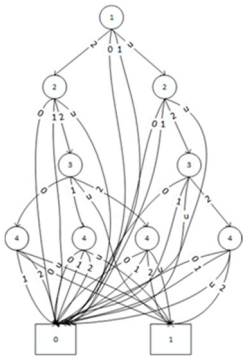


Figure 7. MDD for $T_{(S,T),\,2}$.

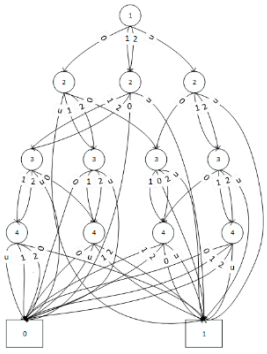


Figure 8. MDD for $T_{(S,T),\,u}$.

Finally, the trust probability of different levels can be predicted as:

$$T_{(S,T),\,0} = 0.0568,\ T_{(S,T),\,1} = 0.484,\ T_{(S,T),\,2} = 0.2888,\ T_{(S,T),\,3} = 0.1704.$$

6. Experiment

We evaluate the performance of the proposed method through experiments by using a real-world dataset in [38]. We compare our method with subjective logic (SL) based method [10].

The dataset was collected in a French high school in 2011 and 2012. The network consists of 1828 nodes and 502 edges, and each edge (u, v) means that user u has an opinion about user v. There is a corresponding weight W (u, v) on each edge in the range of [1,4], which represent the strength of opinion. Since the edge weights in the dataset are ordinal data, we convert ordinal values into opinion vectors using the linear transformation technique [11]. Original trust data are transformed to 3-dimension opinion vectors composed of decimals, ranging from 0 to 1. The machine configuration

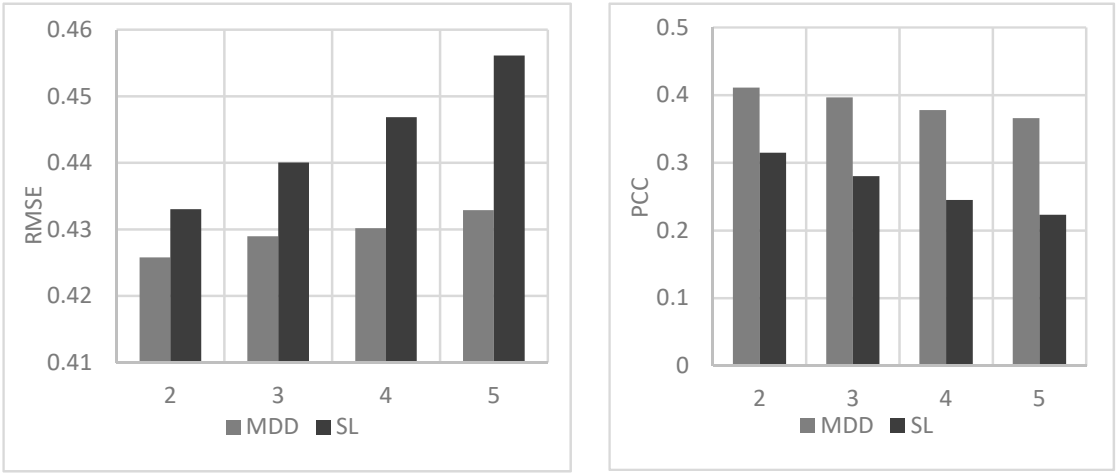
used for the experiment is: an Intel CORE i7-4790K 4.0 GHz CPU, 16G memory (Kingston, China) and 256G SSD hard drive (Kingston, China).

6.1. Accuracy

As recommended in [37], our study uses a combination of metrics to assess the accuracy of models. First, we randomly select a link connecting a pair of users u and v in the dataset. We treat the trust information of the link as the actual trust from u to v. Then we remove the edge (u, v) from the datasets and run two algorithms to infer the trust from u to v, respectively. At last, we compare the inferred trust to the actual trust information.

For a comprehensive comparison, we measured the accuracy of these algorithms using both root mean squared error (RMSE) and Pearson correlation coefficient (PCC). Figure 8 shows the RMSE and PCC. The x axis represents different hops from start node. To make a fair comparison, we took the average of RMSE and PCC of all levels as the computed result, respectively. Simultaneously, we repeat the experiment 20 times to get statistically significant results.

In Figure 9, we find MDD-based trust achieves a higher accuracy compared to subjective logic based method. It can be observed that as the paths between users become longer (more hops can be chosen), the prediction accuracy decreases under both methods; but the proposed method is significantly less affected. This is because as the length of the optional path between users increases, the dependency between paths enhances. Meanwhile, the noise along the path will also expand due to the extension of the propagation distance. But our proposed method can alleviate the impact of these problems because of its unique MDD-based trust information combination mechanism (described in Section 3.3).



(**a**) (**b**)

Figure 9. Accuracy of subjective logic based and MDD-based method: (**a**) root mean square error (RMSE); (**b**) Pearson correlation coefficient (PCC).

6.2. Execution Time

The execution time includes the MDD generation time and MDD evaluation time. The MDD generation time is showed in Figure 10. The x axis represents different hops from start node. It can be observed that the longer the path, the longer the MDD generation time. However, the MDD evaluation complexity is linear to the size of the MDD model generated. Figure 10 shows the MDD evaluation time in comparison to subjective logic algorithm.

From Figures 10 and 11, it is not difficult to find that the generation of MDD takes a certain amount of time, but once the MDD is generated, the time for trust evaluation will be greatly shortened, and it will not be seriously affected by the length of the paths.

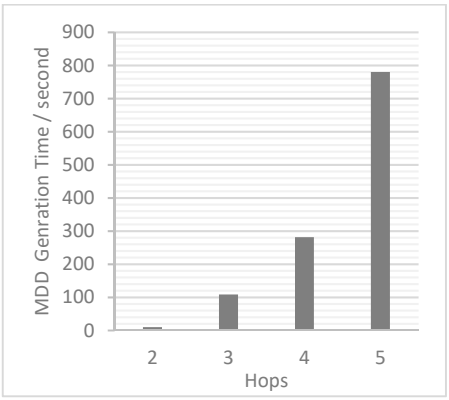


Figure 10. MDD average generation time.

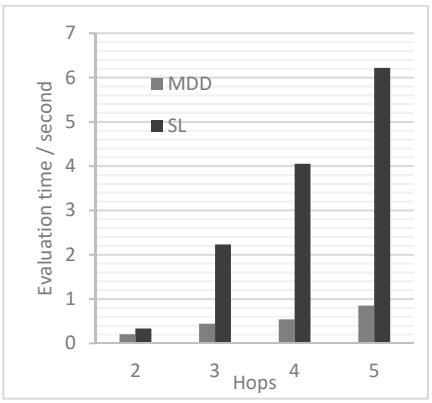


Figure 11. Evaluation time.

6.3. Dynamic Changes Evaluation

In this section, we designed experiments to verify the rationality of the dynamic algorithm. An example of a four-levels trust modeling approach is demonstrated, including uncertainty level. The parameters are set as: $\alpha_1 = 0.15$, $\alpha_2 = 0$, $\delta = 2$, $k = 3$. Furthermore, $\beta_i = 3.5$. According to Equations (5) and (6), the changes of uncertainty opinion under different ratings are showed as Figure 12. Here the x axis represents rating times. The y axis is the corresponding trust.

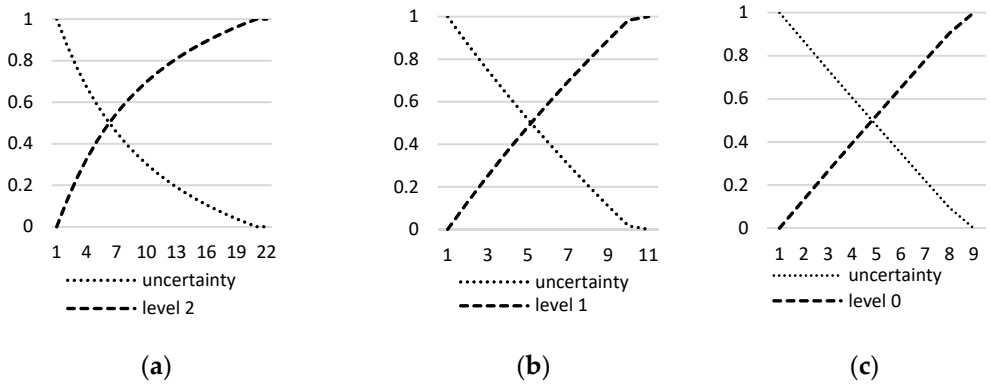


Figure 12. The dynamic changes of uncertainty: (**a**) dynamic changes of uncertainty under ratings in Level 2; (**b**) dynamic changes of uncertainty under ratings in Level 1; (**c**) dynamic changes of uncertainty under ratings in Level 0.

A completely uncertainty view can become full trust after 20 times of ratings on Level 2, and turn to full 1-level trust with 10 times ratings on Level 1. However, for distrust, it only need 8–9 times

ratings on Level 0. This corresponds to the situation in our lives: trust builds slowly, but distrust shapes quickly.

Figure 13 shows the impact of trust and distrust on each other.

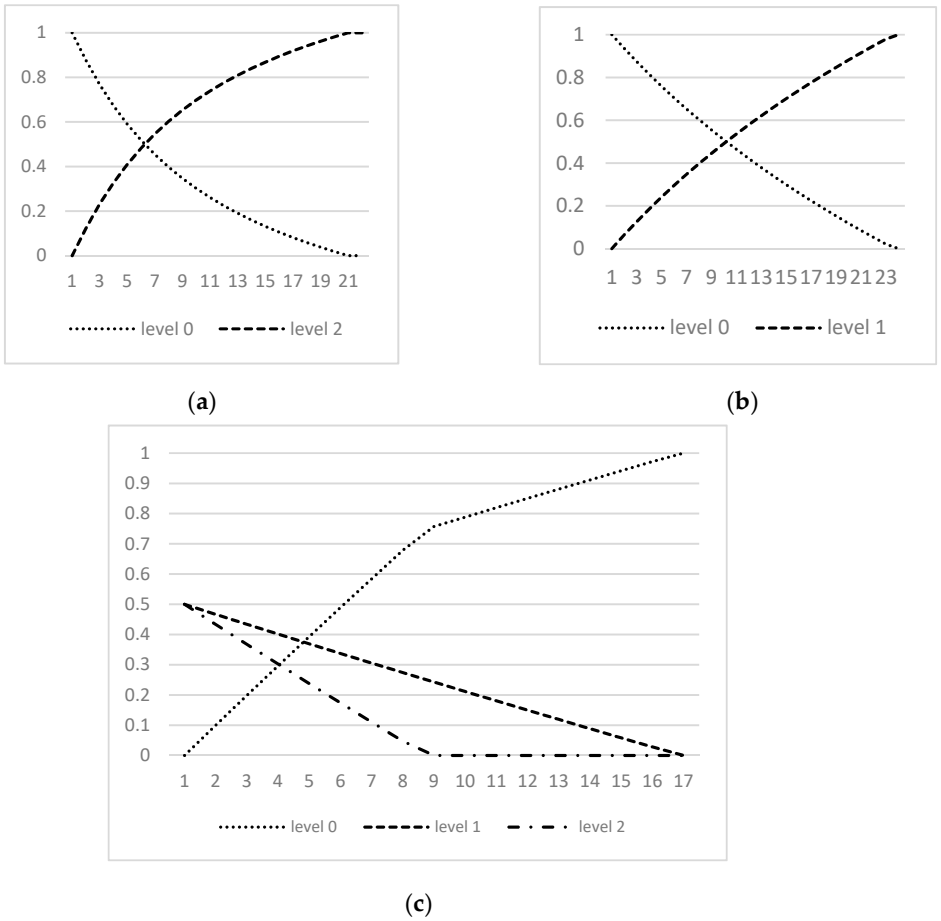


Figure 13. The impact of trust and distrust on each other: (**a**) dynamic changes of completely distrustful point of view under ratings in Level 2; (**b**) dynamic changes of completely distrustful point of view under ratings in Level 1; and (**c**) dynamic changes of completely trustful point of view under ratings in Level 0.

Figure 13a shows the changes of a completely distrustful viewpoint (0, 1, 0, 0) under the two-level ratings. It can be seen that when 20–21 times two-level trust ratings are received, distrust will be wholly eliminated. However, as Figure 13b displays, the same effect requires 23–24 times 1-level evaluations to achieve. This is consistent with our expectation: the higher the level of trust, the greater its impact on distrust. Correspondingly, Figure 13c demonstrates the impact of distrust on trust. When 17 times 0-level ratings are received, a completely trustful viewpoint (0, 0, 0.5, 0.5) becomes absolutely distrustful. It is worth noting that when 8–9 times distrust ratings are received, the top-level trust has been entirely offset. This indicates that distrust has a greater impact on trust. Furthermore, this also conforms to the rules: trust growing slower, declining faster, and it is difficult to eliminate the distrust ratings. Based on the above experiments, we conclude that the MDD-based trust analysis method is an efficient and accurate solution to the multi-level trust evaluation problem.

7. Conclusions and Future Work

This paper proposes an MDD-based algorithm for the multi-level trust evaluation. It considers not only the trust information, but also distrust and uncertainty information. We design the propagation rules for distrust especially. Meanwhile, the aggregation rules of different paths which solve the

opinions conflict are also proposed. For the dynamicity of trust relationships, a dynamic change function is designed which follows the rules: distrust increases rapidly, but decreases slowly and trust increases slowly but decreases rapidly.

Experiments show that the proposed method has better performance in terms of accuracy and calculation speed. When the path is longer, there are more dependencies between paths, leading to a decrease in the accuracy of most methods. However, due to the aggregation mechanism of MDD, the dependence between paths is reduced, so MDD-based method is not greatly affected by path length and path number. As for the execution time, after the MDD is generated, the execution time of proposed method is linear complexity. However, the time complexity of the MDD generation process is exponential. Since most of the networks are relatively stable, the MDD generation process does not need to be performed online and in real time. It only needs to be updated regularly, so it is acceptable for the entire running time. Finally, the propagation rules of trust, distrust and uncertainty proposed have been shown through experiments to conform to normal laws. That is, a poor rating has a much higher impact on trust than a rating of trust, which prevents dishonest transactions to a certain extent.

The method proposed in this paper performs well on small-scale data, but for large-scale data, especially the MDD generation process, the time complexity is relatively high. In the future, we will try to reduce the complexity of MDD generation. Distrust is a complex concept, some researches consider it as an independent construct of trust. We will research on distrust levels in the future.

Author Contributions: Conceptualization, L.Z. and B.Z.; Methodology, L.Z. and L.X.; Performing experiments and analyzing data, A.L.; Writing—Original draft preparation, L.Z. and L.X. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China under Grants grant number No. U1908212.

Conflicts of Interest: The authors have no conflict of interest to declare.

References

1. Jiang, W.; Wang, G.; Bhuiyan, M.Z.A.; Wu, J. Understanding graph-based trust evaluation in online social networks. *ACM Comput. Surv.* **2016**, *49*, 1–35. [CrossRef]
2. Stephen, M. Formalising Trust as a Computational Concept. Ph.D. Thesis, University of Stirling, Stirling, Scotland, UK, 1994.
3. Abdulrahman, A.; Hailes, S. Supporting trust in virtual communities. In Proceedings of the 33rd Annual Hawaii International Conference on System Sciences (HICSS-33), Maui, HI, USA, 4–7 January 2000; pp. 4–7.
4. Guha, R.V.; Kumar, R.; Raghavan, P.; Tomkins, A. Propagation of trust and distrust. In Proceedings of the 13th International Conference on World Wide Web (WWW), New York, NY, USA, 17–20 May 2004; pp. 403–412.
5. Golbeck, J.; Hendler, J.A. Inferring binary trust relationships in Web-based social networks. *ACM Trans. Internet. Technol.* **2006**, *6*, 497–529. [CrossRef]
6. Leskovec, J.; Huttenlocher, D.P.; Kleinberg, J. Predicting positive and negative links in online social networks. In Proceedings of the 19th International Conference on World Wide Web (WWW), Raleigh, NC, USA, 26–30 April 2010; pp. 641–650.
7. Zhang, R.; Mao, Y. Trust Prediction via Belief Propagation. *ACM Trans. Inf. Syst.* **2014**, *32*, 15. [CrossRef]
8. Wang, Y.; Hang, C.; Singh, M.P. A probabilistic approach for maintaining trust based on evidence. *J. Artif. Intell. Res.* **2011**, *40*, 221–267. [CrossRef]
9. Cho, J.; Chan, K.; Adali, S. A Survey on Trust Modeling. *ACM Comput. Surv.* **2015**, *48*, 28. [CrossRef]
10. Jøsang, A.; Hayward, R.; Pope, S. Trust network analysis with subjective logic. In Proceedings of the Computer Science 2006, Twenty-Nineth Australasian Computer ScienceConference (ACSC2006), Hobart, Tasmania, Australia, 16–19 January 2006; pp. 85–94.
11. Liu, G.; Chen, Q.; Yang, Q.; Zhu, B.; Wang, H.; Wang, W. OpinionWalk: An efficient solution to massive trust assessment in online social networks. In Proceedings of the Conference on Computer Communications (INFOCOM), Atlanta, GA, USA, 1–4 May 2017; pp. 1–9.
12. Zhang, P.; Durresi, A. Trust management framework for social networks. In Proceedings of the International Conference on Communications (ICC), Ottawa, ON, Canada, 10–15 June 2012; pp. 1042–1047.

13. Hiltunen, J.; Kuusijarvi, J. Trust Metrics Based on a Trusted Network Element. In Proceedings of the TrustCom/BigDataSE/ISPA, Helsinki, Finland, 20–22 August 2015; pp. 660–667.
14. Jiang, W.; Wu, J.; Li, F.; Wang, G.; Zheng, H. Trust Evaluation in Online Social Networks Using Generalized Network Flow. *Trans. Comput.* **2016**, *65*, 952–963. [CrossRef]
15. Zhan, J.; Fang, X. A Novel Trust Computing System for Social Networks. In Proceedings of the PASSAT/SocialCom 2011, Privacy, Security, Risk and Trust (PASSAT), Third International Conference on and Third International Conference on Social Computing (SocialCom), Boston, MA, USA, 9–11 October 2011; pp. 1284–1289.
16. Zhang, L.; Xing, L.; Liu, A.; Mao, K. Multivalued Decision Diagrams-Based Trust Level Analysis for Social Networks. *IEEE Access* **2019**, *7*, 180620–180629. [CrossRef]
17. Massa, P.; Avesani, P. Controversial users demand local trust metrics: An experimental study on Epinions.com community. In Proceedings of the Twentieth National Conference on Artificial Intelligence and the Seventeenth Innovative Applications of Artificial Intelligence Conference, Pittsburgh, PA, USA, 9–13 July 2005; pp. 121–126.
18. Akilal, K.; Slimani, H.; Omar, M. A very fast and robust trust inference algorithm in weighted signed social networks using controversy, eclecticism, and reciprocity. *Comput. Secur.* **2019**, *83*, 68–78. [CrossRef]
19. McKnight, H.D.; Chervany, N.L. Trust and distrust definitions: One bite at a time. In *Trust in Cyber-Societies*; Springer: Berlin, Germany, 2001.
20. Ashtiani, M.; Azgomi, M.A. Contextuality, Incompatibility and Biased Inference in a Quantum-like formulation of Computational Trust. *Adv. Complex Syst.* **2014**, *17*, 1–61. [CrossRef]
21. Dimoka, A. What does the brain tell us about trust and distrust? evidence from a functional neuroimaging study. *MIS Q.* **2010**, *34*, 373–396. [CrossRef]
22. Cao, J.; Fu, Q.; Li, Q.; Guo, D. Discovering hidden suspicious accounts in online social networks. *Inf. Sci.* **2017**, *394*, 123–140. [CrossRef]
23. Chen, C.C.; Wan, Y.H.; Chung, M.C.; Sun, Y.C. An effective recommendation method for cold start new users using trust and distrust networks. *Inf. Sci.* **2013**, *224*, 19–36. [CrossRef]
24. Chen, S.; Wang, G.; Jia, W. κ-FuzzyTrust: Efficient trust computation for large-scale mobile social networks using a fuzzy implicit social graph. *Inf. Sci.* **2015**, *318*, 123–143. [CrossRef]
25. Gao, P.; Miao, H.; Baras, J.S.; Golbeck, J. STAR: Semiring Trust Inference for Trust-Aware Social Recommenders. In Proceedings of the 10th Conference on Recommender Systems, Boston, MA, USA, 15–19 September 2016; pp. 301–308.
26. Sherchan, W.; Nepal, S.; Paris, C. A survey of trust in social networks. *ACM Comput. Surv.* **2013**, *45*, 47. [CrossRef]
27. Urbano, J.; Rocha, A.P.; Oliveira, E. Computing Confidence Values: Does Trust Dynamics Matter? In Proceedings of the Progress in Artificial Intelligence, 14th Portuguese Conference on Artificial Intelligence (EPIA), Aveiro, Portugal, 12–15 October 2009; pp. 520–531.
28. Melaye, D.; Demazeau, Y. Bayesian dynamic trust model. *LNCS* **2005**, *3690*, 480–489.
29. Wang, W.; Zeng, G. Bayesian cognitive trust model based self-clustering algorithm for MANETs. *SCI China Inf. Sci.* **2010**, *53*, 494–505. [CrossRef]
30. Sun, Y.X.; Huang, S.H.; Chen, L.J.; Xie, L. Bayesian decision-making based recommendation trust revision model in ad hoc networks. *JSW* **2009**, *20*, 2574–2586. [CrossRef]
31. Ziegler, C.N.; Lausen, G. Propagation Models for Trust and Distrust in Social Networks. *ISF* **2005**, *7*, 337–358. [CrossRef]
32. Liu, G.; Yang, Q.; Wang, H.; Lin, X.; Wittie, M.P. Assessment of Multi-Hop Interpersonal Trust in Social Networks by Three-Valued Subjective Logic. In Proceedings of the Conference on Computer Communications (INFOCOM), Toronto, ON, Canada, 27 April–2 May 2014; pp. 1698–1706.
33. Aghdam, N.H.; Ashtiani, M.; Azgomi, M.A. An uncertainty-aware computational trust model considering the co-existence of trust and distrust in social networks. *IS* **2020**, *513*, 465–503.
34. Ortega, F.J.; Troyano, J.A.; Cruz, F.L.; Vallejo, C.G.; EnríQuez, F. Propagation of trust and distrust for the detection of trolls in a social network. *Comput. Netw.* **2012**, *56*, 2884–2895. [CrossRef]
35. Ghavipour, M.; Meybodi, M.R. A dynamic algorithm for stochastic trust propagation in online social networks: Learning automata approach. *CCJ* **2018**, *123*, 11–23. [CrossRef]
36. Miller, D.M. Multiple-valued logic design tools. In Proceedings of the 23rd International Symposium on Multiple-Valued Logic (ISMVL), Sacramento, CA, USA, 24–27 May 1993; pp. 2–11.

37. Mastrandrea, R.; Fournet, J.; Barrat, A. Contact patterns in a high school: A comparison between data collected using wearable sensors, contact diaries and friendship surveys. *PLoS ONE* **2015**, *10*, e0136497. [CrossRef]
38. Xing, L.; Amari, S.V. *Binary Decision Diagrams and Extensions for System Reliability Analysis*, 1st ed.; Wiley-Scrivener: Boston, MA, USA, 2015; pp. 22–30.