Hindawi
Security and Communication Networks
Volume 2020, Article ID 8887596, 10 pages
https://doi.org/10.1155/2020/8887596

Research Article

A Comprehensive Trust Model Based on Social Relationship and Transaction Attributes

Yonghua Gong,[1,2] **Lei Chen**,[1] **and Tinghuai Ma**[3]

[1]*School of Management, Nanjing University of Posts and Telecommunications, Nanjing 210003, China*
[2]*Information Industry Integration Innovation and Emergency Management Research Center, Nanjing University of Posts and Telecommunications, Nanjing 210003, China*
[3]*Nanjing University of Information Science & Technology, Nanjing 210044, China*

Correspondence should be addressed to Yonghua Gong; gongyh@njupt.edu.cn

Received 6 July 2020; Revised 28 September 2020; Accepted 22 October 2020; Published 12 November 2020

Academic Editor: Victor S. Sheng

The existing approaches to predict trust values in social commerce are based on personal social relationships without considering historical transaction information about products in social commerce, which results in false recommendations, and deceptions cannot be differentiated. Trust values extracted from social links can improve the performance of trust and reputation mechanism, but the rates from these links in social commerce can be false because of the stakeholders' manipulation for personal interest. And the rates are also dynamic and inconsistent. Therefore, this paper proposes a comprehensive trust model by fully exploiting the effects of the transaction attributes and social relationships on users' trust. The proposed model refines the granularity of trust evaluation and improves the discrimination of recommended information. Experiments demonstrate that the proposed model performs better and predicts more accurately than the three models compared under the same circumstance.

1. Introduction

Social commerce provides the environment in which members could participate in social media-driven commercial activities such as reviewing, rating, and sharing products, recommending, and conversation [1]. For example, in order to reduce uncertainty, buyers often want to get their friends' opinions before making a purchasing decision [2]. However, uncertainty in social commerce is comparatively higher due to a large amount of user-generated content (UGC) and a lack of face-to-face interactions [3]. Although the secure and verifiable access control scheme is proposed to address the problems that existed in social networks such as data protection, privacy issues [4], which is similar to the certificate validation system proposed in [5, 6], the lack of fraud prevention, and punishment mechanism, malicious members can easily manipulate ratings or reviews to confuse consumers or attack other honest sellers to achieve the goal of reputation slander or reputation conspiracy. There are lots of trust crises and privacy leaks in the process of information exchange [7], which results in more obvious reputation fluctuation behaviour. Consumers have to reexamine product reviews and opinions posted by other social network members [8]. Trust mechanisms are applied to recommender systems to help users to make better purchase decisions from a number of alternatives. Trust mechanism can provide a solution for transaction reliability in response to the characteristics of trust ambiguity and uncertainty, thus improving users' purchase intentions and enhance word-of-mouth intentions [9].

Both explicit trust [10] and implicit trust [11] are addressed by solving the information reliability problem in social commerce. In the explicit trust mechanism, a user needs to designate a trusted user and demonstrate the degree of trust, which is difficult for the user to guarantee privacy. This mechanism is also time-consuming and energy-intensive. In the implicit trust mechanism, the user-item interaction is presented as ratings and the similarity relationships of user ratings are used to mine the trust relationships. However, both of the trust mechanisms cannot distinguish cheating behaviours such as fake reviews, credit hypes, and collusions. Buyers are driven to evaluate the purchasing opinions from social relationships. What's more, the new buyers usually have limited or no direct relationship with other buyers in social commerce. These problems are essential in the process of gaining actual feedback and estimating trust accurately.

Because both user's social relationships and commodity transaction records play important roles in the behaviour of users regarding ratings and making purchase decisions [12, 13], thus, this paper proposes a new comprehensive trust model for social commerce based on the social networks theory and consumer behaviour theory to improve the accuracy and reliability of trust calculation and prevent trust fraud. The main significant features of the model proposed in this paper are that both the users' purchasing behaviour and social relationships in social commerce are considered to explore the opinions in the social commerce and reduce the scarcity of data. Besides, the time sensitivity of trust and fraud penalty factors have also been used to reduce the dynamics of opinions and behaviours.

The remainder of this paper is organized as follows. Section 2 represents the existing literature related to trust and recommendation systems. Section 3 proposes the social commerce trust model which combines the social relationships and transaction attributes. Section 4 describes the experimental settings and the process. And Section 5 concludes our research contributions and future research directions.

2. Related Works

There is a sharp increase in consumers' participation in social commerce activities such as reviewing, recommending and discussing, and using these as a source of product-related information, which can be attributed to the rapid growth of Web2.0 [14, 15]. As a result, the interactions between users are the main information resources, which set social commerce apart from traditional e-commerce. The promotion of relationships between buyers and sellers is a common value in e-commerce [16]. As studied in the network theory, the representation of relations among discrete users is described, and transactions or services based on the social network are defined. More specifically, with the aid of correlation analysis of vertex and edge in graph theory, a node-oriented network can be transformed into a relation-oriented network, and the influence or importance of actors and how the actors are allowed to share resources and acquire opinions can be identified [17, 18]. In addition, the emotions or opinions of texts such as UGC can be predicted for target participation [19, 20]. The study [21] recommends similar users, as well as high-quality resources to other reliable users. Furthermore, relationship quality which is one of the social factors plays an important role in enhancing the intention to share and receive commercial information in social commerce. Besides, users' relationships are also vital for user retention and higher customer loyalty, which is consistent with existing literature [5, 22]. The study [23] points out that the relationships between users can be converted into similar relations. A two-stage partition algorithm is proposed to calculate the weights of subnetworks and their individual members by considering social behaviour factors [24].

The social commerce community allows users to review; users can easily express personal opinions on products or other users, which is similar to the reliance on information provided by others listed in [25]. There are still problems such as the fact that information shared between the parties involved in transactions is insufficient, which results in transaction risks [3]. Malicious users could make a dishonest evaluation of good providers [26]. One method to resolve that problem is to disguise and encrypt the real information [27, 28]. The risk can also be alleviated through trust [29]. The study [28] proposes a double-blind anonymous evaluation-based trust model to prevent malicious attacks in cloud computing. Trust and reputation systems can provide an evaluation of specific users and get a score based on comprehensive analysis, which gives users a reference on whether to conduct transactions or not. Various implicit and explicit pieces of information have been applied to trust and reputation mechanisms [3, 30], so that trust values from social links or users' preferences can be extracted. The implicit information method collects users' behaviour to demonstrate user preference and extract trust values from user-item ratings. When explicit information is unavailable, implicit ratings can be derived from transaction records to identify users' preferences [31]. The article [32] investigates users' reading behaviour by measuring the value of implicit parameters defined and comparing the grade of correlation between explicit feedback and implicit feedback. The paper [33] infers user preferences using implicit information, which indirectly reflects opinions by observing user behaviour such as searching patterns and purchase history, while explicit information denotes the trust values directly indicated by users. By analysing users' navigational history, the users' interest and preference models are generated, and feedback from users about reading preferences is collected so that personalized recommendation systems can be modelled [34].

The comprehensive consideration of a number of factors that reflect the trust metric can improve the accuracy of trustworthiness calculation [35]. Trust in social commerce has several dimensions, including impersonal and interpersonal [36]. In [37], multifactor and single-factor weight-based evaluation mechanism is proposed to evaluate the reliability of the information. The impersonal dimension is usually utilized to give prediction in user links that are positive or negative through the graphical structure of social networks [38]. The study [39] proposes local reputation which is a particular form of reputation instead of a global reputation to form effective groups in virtual communities. As social networks become increasingly popular, antecedents and consequences of users' trust have been studied; the results show that users' trust can positively affect purchase intentions [40]. Given the strong and positive relationship between trust and preference, the value of preference has been explored by trust and reputation systems. Factors like similarity and social influence are also investigated in trust systems [12]. Users who have common interests are connected by social network links; they usually purchase the same products even though they do not know each other [41]. The study [42] performs an in-depth analysis on the correlations between social friend relationships and user interest similarity, the similarity on friends of a specific user is related to the average similarity on other randomly selected users, and the users' preference similarity could be found through the products they have bought or the ratings they have made. The similarity measures such as Vector Space Similarity (VSS) and Pearson Correlation Coefficient (PCC) have been applied in trust-aware recommendation mechanisms [43].

The existing research on trust and reputation mechanism is based on users' personal observation to evaluate and calculate the trust values of users or ratings of products, which would deviate from the essential attributes of social commerce and make the trust mechanism unreliable. And for new users, the sparseness of data reflected by little or no social interaction will make the calculation and prediction of trust more difficult, while it will be easier to judge whether a user is trustworthy in social commerce with the help of recent transaction histories such as transaction price, transaction quality, and transaction time.

Our current study is inspired by the abovementioned studies. Thus, a new comprehensive trust model for social commerce based on the social networks theory and consumer behaviour theory is proposed to improve the accuracy and reliability of trust calculation and prevent trust fraud. This paper differs from previous studies in the following ways. Firstly, the trust model proposed an emphasis on both the social relationship data and transaction behaviour data. Secondly, comprehensive trust is based on transaction attributes trust and social relationship trust to reduce the influences of the scarcity of data. Finally, the accuracy of the trust prediction is enhanced when facing cheating behaviours in social commerce.

3. Trust Model Based on the Combination of Transaction Attributes and Social Relationships

Users in this social commerce network will screen out product providers in two ways although the products provided in social commerce look the same, with the same price, quality, or sales volume. The process of purchase decision making is like this. For example, Bob is a potential consumer, he has a transaction demand. If he has a few or even no direct transaction experiences with the product providers, then he would ask his friends or other users for advice, so the relationships between Bob and his friends are highly important for Bob to make a purchase decision. However, if Bob has some transaction experiences with the product providers, he may make the purchase decision according to his own judgement.

Therefore, the trust model proposed in this paper would reflect the transaction trust and social relationship trust between users in social commerce. The former denotes the trustworthiness after the transactions are completed, while the latter refers to trust in familiarity or similar preferences formed by social relationships such as user ratings or followership. A specific registered user u_i can perform several activities in the network, such as buying products or services, recommending products or services to other users, rating the users or products, and following other users, i.e., adding the user to the list of trusted friends, which can be seen in Figure 1. In Figure 1, users are represented by nodes, and the corresponding activities and social relationships are expressed by directed edges, which are valued by the weights of the directed edges. User u_i can gather available information about the transaction with the provider u_j (including transaction time, price, and amount), as well as extra information about the relationships between users and related activities (including the followership and rating records) before making a careful purchase decision. Then, consumers could increase trust in product providers through these behaviours and reduce trust when facing malicious transactions. The symbols used in this paper are listed in Table 1.

3.1. Measurement of Transaction Attributes Trust. The transaction attributes include price, quantity, time, amount, and logistic service, and different people value transaction attributes differently. Considering the social practice experience, the latest transaction records can reflect the trust relations more accurately; the larger the transaction price and quantity are, the more careful the buyers and the sellers are, and the evaluation after the successful transaction can reflect more real trust relationship. Obviously, transaction time, price, and quantity have a greater impact on the trust value. Therefore, the cumulative transaction coefficient, price, quantity, and time are considered in the trust model.

3.1.1. Cumulative Transaction Coefficient. Honest historical transaction behaviours are important in encouraging users to behave well and keeping users to continue future transactions on this social commerce platform. If we simply add the feedback score to calculate the trust value, then a malicious user may cover up the fact that he/she is cheating at a certain rate by increasing the number of transactions. The cumulative transaction coefficient is expected to give the number of transactions on the platform for a specific user to estimate the trust of the transaction attribute based on the most recent transaction or this transaction. If the user just entered the platform performed as a new user or has almost no transaction history, then the latest behavioural history accounts for a lot in the process of this trust evaluation. Otherwise, if the user has made many transactions before, then the weight of this transaction to be completed is larger. Let $Ac_{t_n}(u_j)$ denote the cumulative transaction coefficient; then,

$$Ac_{t_n}\left(u_j\right) = e^{-\left(1/An_{t_n}\left(u_j\right)\right)}, \tag{1}$$

where $An_{t_n}(u_j)$ is the number of transactions that have been performed by user u_j until time t_n.

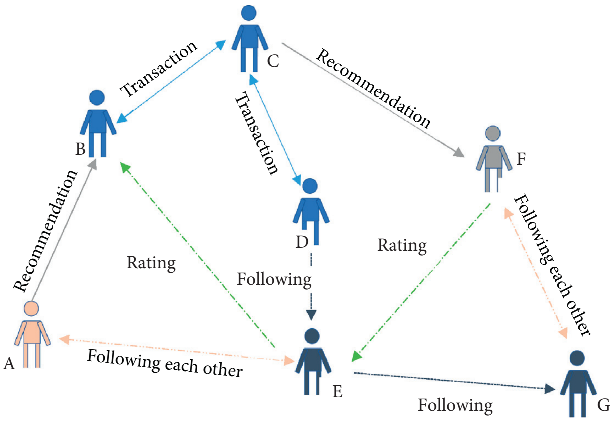


Figure 1: Simple network transaction diagram.

Table 1: Symbols used in the study.

Symbol	Notions	Illustration
$Ac_{t_n}(u_j)$	Cumulative trading coefficient	Symbol for determining u_j is a new user or has made many transactions before
$An_{t_n}(u_j)$	Number of transactions	The number of transactions performed by user u_j until time t_n
$Ap_{t_n}(u_j)$	Impact factor of transaction price	The impact of transaction price at time t_n on the transaction attribute trust
$P_k(u_i,u_j)$	Transaction price	The price of transaction performed by user u_j until time t_n
$Aq_{t_n}(u_j)$	Impact factor of transaction quantity	The impact of transaction quantity at time t_n on the transaction attribute trust
$Am_{t_n}(u_i,u_j)$	Transaction quantity	The quantity of products or services purchased by user u_j until time t_n
$\mathrm{Am}_{\mathrm{Max}}$	Maximum quantity	The maximum quantity of products or services purchased by user u_j during. $[t_0,t_n]$
$\mathrm{Fr}(u_j)$	Fraud penalty factor	Factor to prevent fraud behaviour
$\theta(\mathrm{DT}_{t_{n-1}})$	Damping function	Make changes in trust values smooth
$\mathrm{DT}_{t_n}(u_j)$	Transaction attribute trust	Transaction trust of five factors of user u_j until time t_n
$\mathrm{Pre}(u_j)$	Prestige degree	The reputation or popularity that user u_j has
$\mathrm{Fam}(u_i,u_j)$	Familiarity between users	Closeness between users
$\mathrm{Sim}(u_i,u_j)$	Rating similarity	Similarity of ratings of the same item or user by different users
$\mathrm{RT}(u_j)$	Social relationship trust	Social relationship trust of three factors of user u_j
$\mathrm{CT}(u_j)$	Comprehensive trust	Comprehensive trust of transaction attribute and social relationship attribute user u_j

3.1.2. Analysis of Transaction Price and Quantity. Transaction value is an important factor affecting transaction trust which is determined by transaction price $Ap_{t_n}(u_j)$ and transaction quantity $Aq_{t_n}(u_j)$. Greater transaction value means that both consumers and providers may have to face more risk that will make both of the parties default to honest behaviours such as paying on time and shipping with quality and quantity. Therefore, the greater transaction value can bring more trust value to both parties. On the other hand, the stable and reliable trust relationship established at a previous time will decay with time. What's more, it may vanish at the current time. The time difference between the current transaction and initial transaction will be considered in $Ap_{t_n}(u_j)$. While the price is more vital than time in the transaction history, we use square to increase the importance of price in evaluation factors:

$$Ap_{t_n}(u_j) = \frac{P_k^2(u_i,u_j)(t_k - t_0)}{\sum_{k=1}^{An_{t_n}(u_j)} P_k^2(u_i,u_j)(t_n - t_0)},$$
$$Aq_{t_n}(j) = \frac{Am_{t_n}(i,j)}{Am_{Max}}. \quad (2)$$

Here, $P_k(u_i,u_j)$ is the price of the transaction $k, k \in [1, \mathrm{An}_{t_n}(u_j)]$ between user u_i and u_j, and $[t_0,t_n]$ is the time interval for effective trading. $\mathrm{Am}_{t_n}(u_i,u_j)$ is the quantity of products or services successfully traded at time t_n. $\mathrm{Am}_{\mathrm{Max}}$ is the maximum quantity of products successfully traded during the time period $[t_0,t_n]$.

3.1.3. Analysis of Fraud Penalty Factor and Damping Function. The trust between people is slowly increasing and rapidly decreasing in real-life situations; the same is in the social commerce. People need to behave well to gain favour from others so that trust relationships will be built, but once malicious or fraud behaviour happens, although there is only one, it will be a great blow to the trust relationships established. More than that, the trust between two parties is always asymmetric, and it increases or decreases at different rates for different people. The fraud penalty factor is added to the model to reflect this feature. In the process of transaction, if the transaction is successful and there is no fraud on both consumers and providers, the fraud penalty factor will not work. Conversely, if there is a fraud, the trust value will be reduced by the fraud penalty factor $\mathrm{Fr}(u_j)$, and the punishment will become stronger as the number of frauds increases:

$$Fr\left(u_j\right) = f\left(u_j\right)DT_{t_{n-1}}\frac{\left(u_j\right)}{\left(1+e^{-n}\right)},$$
$$\theta\left(DT_{t_{n-1}}\right) = 1 - \frac{1}{1+e^{DT_{t_{n-1}}\left(u_j\right)-DT_{\text{Max}}}}, \tag{3}$$

where $f(u_j)$ represents a sign of fraud in transactions performed by u_j, and $f(u_j) = -1$ denotes that u_j is fraudulent; otherwise $f(u_j) = 0$. When there is a fraud during a transaction, the value of the fraud penalty factor will become negative to achieve the goal of decreasing trust value for a malicious user. $\theta(\mathrm{DT}_{t_{n-1}})$ is the damping function. $\mathrm{DT}_{\mathrm{Max}}$ is the maximum transaction attribute trust set in this model and is constrained to [0, 10].

In summary, transaction attributes trust can be divided into several factors: cumulative transaction coefficient, transaction price, transaction quantity, fraud penalty factor, and damping function. When $n=1$, this means that a new user u_j joins the social commerce currently, and its transaction attribute trust value is 0; that is, $\mathrm{DT}_0(u_j) = 0$, because there are no transaction history records for her or him. Then,

$$\begin{aligned}\mathrm{DT}_{t_n}\left(u_j\right) ={}& \left(1 - Ac_{t_n}\left(u_j\right)\right)\times \mathrm{DT}_{t_{n-1}}\left(u_j\right)\\ &+ Ac_{t_n}\left(u_j\right)\times\theta\left(\mathrm{DT}_{t_{n-1}}\right)\times Ap_{t_n}\left(u_j\right)\times Aq_{t_n}\left(u_j\right) + Fr\left(u_j\right).\end{aligned} \tag{4}$$

3.2. Measurement of Social Relationship Trust. The difference s social commerce and e-commerce is that the former involves communities and conversation between members, while the latter focuses on individual and one-way interaction, which means that the integration of relationship quality, users' experience, and intimacy of community members provides the basis for trust inference of users in social commerce, especially given the limited first-hand interactive information. Therefore, in addition to contextual features of commodity trading mentioned above, users' relationships that are shown by familiarity and reputation should also be considered.

3.2.1. Analysis of Prestige Degree of a User. Users with similar interests and tastes form a clique through lists of friends. And the user who has a higher reputation or more popular in social commerce is that we called Key Opinion Leader or person in authority; prestige degree could be a representative of it. In a social network, the more users point to a particular user, the more voice this user has. The prestige degree $\mathrm{Pre}(u_j)$ of user u_j denotes his/her social position and popularity in the specific scenario:

$$\mathrm{Pre}\left(u_j\right) = \frac{\left(|N(\text{follower})| + |N(\text{rating})|\right)}{2N}, \tag{5}$$

where $N(\text{follower})$ and $N(\text{rating})$ represent the number of the followers of user u_j and the users who have rated user u_j, respectively. The relationship existing in the trust model is composed of both followership and rating people. And N is the average number of active community users.

3.2.2. Analysis of Familiarity between Users. The lack of face-to-face interaction may cause users to doubt the authenticity of online transactions, and transactions with familiar people will increase users' willingness to buy. Trading experience can reduce uncertainty. User's relationship with connections and interactions play an important role in user behaviours. On the other hand, users are often influenced by trusted friends. Comments or purchase suggestions from trusted friends are easier for users to accept than anonymous friends. The familiarity between user u_i and user u_j is defined as

$$\mathrm{Fam}\left(u_i, u_j\right) = \frac{\left|F\left(u_i\right)\cap F\left(u_j\right)\right|}{\left|F\left(u_i\right)\cup F\left(u_j\right)\right|}, \tag{6}$$

where $F(u_j)$ denotes the set of friends of user u_j, which is composed of two relationships, i.e., the number of the followers of user u_j and the users who have rated user u_j.

3.2.3. Analysis of Rating Similarity. The similarity algorithm is applied to this model. The trust values extracted from similarity can be modelled by the weighted average rating of the users' similarity scores. Consequently, a connection with high similarity will have more impact on the user's rating. Users that have similar preferences tend to show interest in the same items or comments, and trust relationships probably exist between themselves. That is to say, users mostly trust others having similar attributes. The PCC algorithm utilizes the common items or comments that have been rated by both user u_i and u_j to compute similarity which is given by

$$\mathrm{Sim}\left(u_i, u_j\right) = \frac{\sum_{u\in F\left(u_i\right)\cap F\left(u_j\right)} R_{u_i,u}\cdot R_{u_j,u}}{\sqrt{\sum_{u\in F\left(u_i\right)\cap F\left(u_j\right)} R_{u_i,u}^2}\sqrt{\sum_{u\in F\left(u_i\right)\cap F\left(u_j\right)} R_{u_i,u}^2}}, \tag{7}$$

where $u \in F(u_i)\cap F(u_j)$ is the set of users that both u_i and u_j have rated; that is to say,u is the subset of $F(u_i)$ and $F(u_j)$. $R_{u_i,u}$ is the rating value of u_i to user u, and $R_{u_j,u}$ is the rating value of u_j to user u. The value of $R_{u_i,u}$ and $R_{u_j,u}$ will be randomly assigned in the experimental simulation.

The social relationship trust is the weighted average of prestige degree, the familiarity between users, and rating similarity shown in equation (8); the weight $\omega_1, \omega_2, \omega_3 \in [0,1]$:

$$\mathrm{RT}\left(u_j\right) = \omega_1\mathrm{Pre}\left(u_j\right) + \sum_{u_i\in F\left(u_j\right)}\left(\omega_2\mathrm{Fam}\left(u_i, u_j\right) + \omega_3\mathrm{Sim}\left(u_i, u_j\right)\right). \tag{8}$$

3.3. Measurement of Comprehensive Trust. The comprehensive trust value $\mathrm{CT}(u_j)$ is composed of both transaction attributes trust and social relationship trust that can be seen in equation (9). The value of the weight

$\alpha \in [0, 1]$ is determined by the user's personality, when the user is self-confident, she or he prefers to believe the transaction experiences, and the value of α is higher. When the user prefers to receive the recommendation from the social link, then the value of $\alpha$is lower:

$$\mathrm{CT}\left(u_j\right) = \alpha * DT_{t_n}\left(u_j\right) + (1-\alpha) * \mathrm{RT}\left(u_j\right). \tag{9}$$

4. Experimental Results and Discussion

The validity of the proposed trust model in malicious settings has been simulated in the context of social commerce given the comprehensive consideration of transaction attribute and social relationship. Three trust and reputation models have been compared with the trust model proposed above under the condition given by several influencing factors. The simulation platform is developed by MATLAB, and 500 users are generated in the experiment. Assume that the initial trust value of each user obeys uniform distribution on [0, 10]. In the beginning, those generated users have no prior experience with other users. Therefore, users are randomly selected to launch a transaction session with others. Each user completes 100 transactions in the simulation process, then users rate the transaction based on the service quality or his/her personal preference, and post-transaction rating feedback score follows a normal distribution with a mean value of users' rating and a standard deviation of 0.3. Every user can participate in four activities (recommendation, rating, following others, and transaction), and each user is identified with a unique and constant ID. Users could be divided into honest users and malicious users. In such simulation environment, honest users are presumed to behave always well in transactions, while malicious users could be fraudulent with a certain probability. We also adopt some factors such as price, quantity, rating, and deception that reflect the situation of transactions in real life. The detailed characteristic configuration is shown in Table 2. The experiments compare the proposed model with three other trust and reputation algorithms, namely, ST Model [12], STR Model [3], and Extended TIR Model [44].

The quality of a trust and reputation system is measured by the difference between its predicted reputation value and its true reputation value in future transactions. However, there could be two types of attack in the process of users' rating after the transaction is concluded: reputation defamation and reputation complicity which are under two conditions: users make decisions based on their respective experience without others' recommendation and make purchase decisions based on both pieces of information derived from their own experiences and others. We adopt a precision error index to reveal the difference between real and predicted trust values when the transaction succeeds or fails as follows:

$$\mathrm{PEI} = \sqrt{\frac{\sum_{u_i \in N} \left[\arctan \mathrm{CT}\left(u_i\right) * (1/\pi) - p\left(u_i\right)\right]^2}{N}},$$
$$p\left(u_i\right) = \begin{cases} 1, & u_i \text{ is an honest user,} \\ 1 - p_f, & u_i \text{ is a malicious user,} \end{cases} \tag{10}$$

where $\mathrm{CT}(u_i)$ represents the comprehensive trust value, $p(u_i)$ is the probability of u_i conducting an honest and real transaction, and p_f denotes the probability of fraud by a liar.

4.1. Comparison of Proposed Model and Other Reputation Models under Reputation Defamation. In this experiment, fraudulent members would maliciously rate the transaction target after the transaction is completed which results in reputation defamation. Therefore, it is necessary to measure how the prediction error will be affected when there are different proportions of fraudulent users. In the transaction behaviour conducted based on information such as the price, quantity, and accumulated number of transactions that existed in the historical records, malicious members will exaggerate their products or gross merchandise volume. Figure 2(a) presents the experimental comparison results of the proposed model, ST Model, STR Model, and TIR Model. The experimental results show that when the proportion of fraud users increases, the calculated prediction errors will present a downward trend to varying degrees. When the percentage of liars is smaller than 0.3, the prediction error of the proposed model in this paper is slightly weaker than the ST Model and TIR Model compared, the proposed model's defence against defamation is mediocre at this stage, and the changing trend reflected in Figure 2(a) is also relatively flat. But when the proportion of liars increases to approximately 50%, the performance of all four models compared shows a clear downward trend. However, the performance of the proposed model has been better than the three other models since the proportion increases to 50%. The outcome could be attributed to the factor that multi-influence factors such as price and quantity are taken into consideration, which improves the model's performance.

In Figure 2(b), we assume that users make purchase decisions based on both users' self-judgement of commodity transaction history and recommendations and reviews from other users in the social network. Based on this assumption, the proposed model is compared with several alternative reputation models in the situation of reputation defamation. The results show that the performance of these models has improved to varying degrees compared to that shown in Figure 2(a) when the percentage of liars is smaller than 0.5. The precision error of the proposed model, ST Model, and TIR Model has increased to some extent, while that of the STR Model remains basically unchanged when the

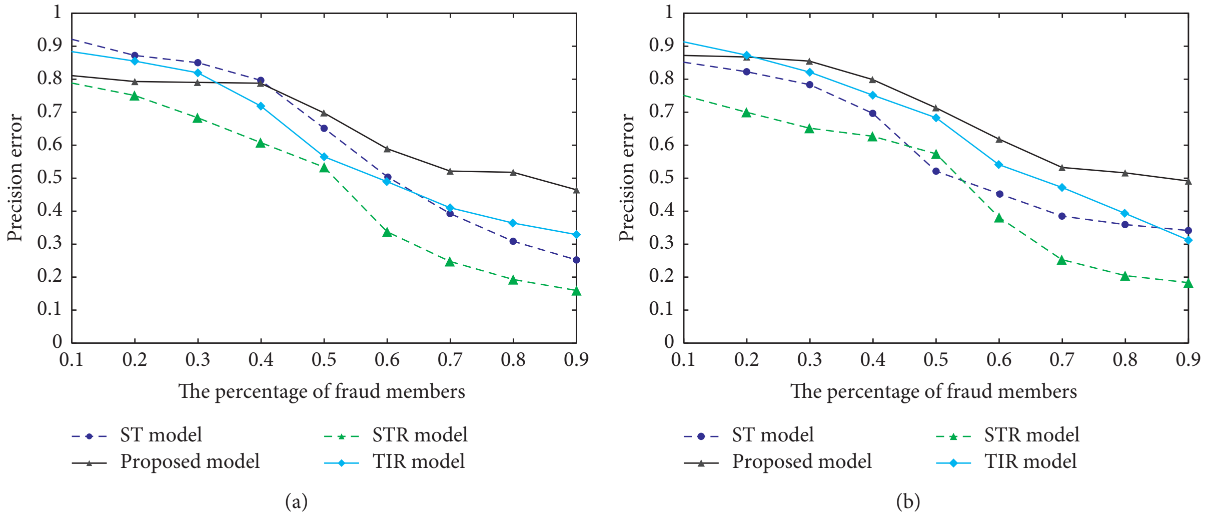


Figure 2: Comparison of trust precision errors of fraudulent users under reputation defamation.

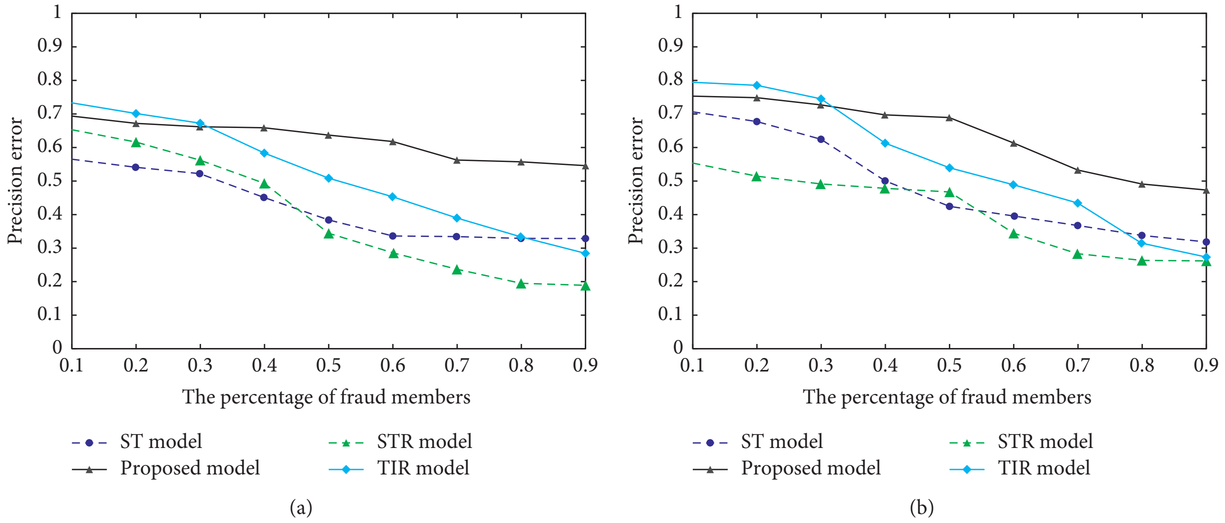
Table 2: Major variables in the experiment.

Variable	Symbol	Value
Total number of users	N	500
Average product price	$P_k(u_i, u_j)$	{10, 20, 30}
Number of simulation rounds		300
Maximum transaction amount	$\mathrm{Am}_{\mathrm{Max}}$	200
Number of followers of a user	N (follower)	[0, 20]
Number of raters of a user	N (rating)	[0, 20]
Ratio of fraudulent members		{0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9}
Rating value	$R_{u_i,u}$	{0,1,2,3,4,5}
Maximum of the trust value	$\mathrm{CT}(u_j)$	10
Probability of fraud	p_f	[0, 1]

percentage of liars is larger than 0.5. It is worth noting that due to the consideration of factors such as social relationships and user similarity, the performance of the proposed model and the TIR Model has improved a lot compared with the results seen in Figure 2(a). Overall, the proposed model above is more robust than the ST Model, STR Model, and TIR Model when facing the attack of reputation defamation.

4.2. Comparison of the Proposed Model and Other Reputation Models under Reputation Collusion. Reputation collusion refers to malicious members making high-scoring evaluations between each other after the transaction is completed while making group attacks and giving bad reviews to other honest users. As mentioned in Section 4.1, experiments are performed under two circumstances: users making decisions solely with their own judgements about products and with their own judgements and the recommendation information by other users. When considering only relying on historical transaction information, the changing trend reflected by the proposed model is relatively gentle, but the precision error is less than 0.7, which can be observed in Figure 3(a), which can be attributed to the user behaviour using a cumulative trading coefficient. The performance of the TIR Model is more effective than both the ST Model and STR Model. Although the data performance level of the ST Model is general, the experimental results show that its process is relatively stable. In addition, the performance of several algorithms compared has declined significantly when the percentage of fraud members is greater than 0.5. The cause of this phenomenon is that when the proportion of liars is greater, the resistance of these models will decrease. The experiment shown in Figure 3(b) takes a combination of transaction attributes and social relationships into account, which can explain the increase in the effectiveness of the proposed model when the percentage of liars is less than 0.5. When talking about the STR Model alone, we can find that the performance is even worse than the result shown in Figure 3(a). However, when the proportion of fraud members is greater than 0.5, the performance of the proposed model is even worse than that shown in Figure 3(a) which does not consider social relationships. One possible explanation is the higher tolerance for reputation complicity due to social relationships.

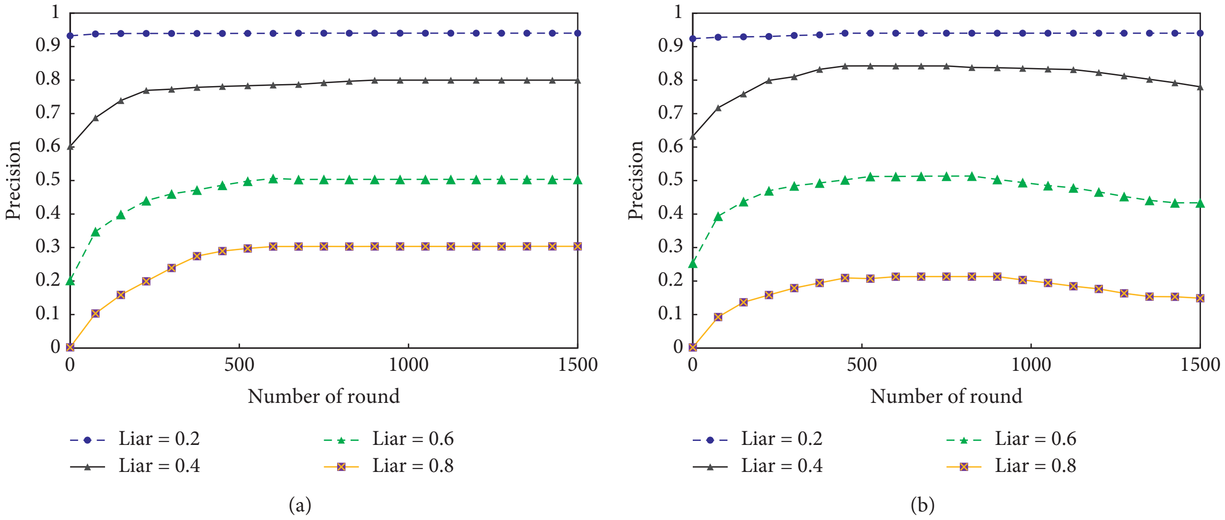
4.3. Precision of the Proposed Model under Different Numbers of Simulation Rounds. The precision level of the proposed model varies a lot when the ratio of fraudulent members is different. In Figure 4(a), the transaction attribute is added to



(a)

(b)

Figure 3: Comparison of trust precision errors of fraudulent users under reputation collusion.



(a)

(b)

Figure 4: The precision of the proposed model in a deceptive environment.

calculate the accumulated precision, while in Figure 4(b), both transaction attribute and social relationship are taken into consideration. As the number of simulations increases, the performance of the model tends to be more stable. The proposed model can behave well to resist the attacks when the ratio of liars is less than 0.4, we can conclude that the precision would stabilize above 0.8 as the number of rounds is more than 500 as shown in Figure 4(a). However, when the fraudulent members account for a lot in the community, the performance of the proposed model would decrease a lot and the precision value would be smaller than 0.5. When talking about Figure 4(b), the improvement of the model is considerable compared with Figure 4(a) as there are fewer malicious users. However, the performance of the model is getting worse as the liars become more, which can be owing to the fact that the interactions between honest users and fraudulent users are growing too much to disrupt the normal operation of the trust and reputation model.

5. Conclusions

When shopping online, people tend to view the historical information of the products, such as sales volume and historical price. After adding UGC to traditional commerce, people have an alternative method to seek suggestions and help from similar people, opinion leaders, and close friends. From this perspective, the consumers' trust in social commerce includes two parts: transaction attribute trust and social relationship trust. This paper proposes a comprehensive trust evaluation model, which can combat the influences of the stakeholders' cheating behaviours and the scarcity of data of the new user. The experiment demonstrates that the proposed model can obtain better and more accurate trust predictions compared to the three trust algorithms. It also shows higher calculation efficiency during the trust evaluation. In addition, the limitation of this paper is as follows: the values of the weights of ω_1, ω_2, and ω_3 are set equal to 1/3, and α equals 1/2. In the future study, we will discuss the sensitivity of the trust model proposed to the value of ω_1, ω_2, ω_3, and α. Several good methods to assign the values of parameters can be used for reference in future research, which include Taguchi's experimental design method [45], big bang-big crunch optimization, and particle swarm optimization [46].

Data Availability

The simulation results based on MATLAB used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was partly supported by the National Natural Science Foundation of China (No. U1736105), the Natural Science Foundation of NJUPT (Nos. NY220044 and NY218024), and Postgraduate Innovation Project in Jiangsu Province (No. KYCX20_0841).

References

[1] Y. Du, L. Qi, and M. Zhou, "Analysis and application of logical petri nets to E-commerce systems," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 44, no. 4, pp. 468–481, 2014.

[2] Y.-M. Li, C.-T. Wu, and C.-Y. Lai, "A social recommender mechanism for e-commerce: combining similarity, trust, and relationship," *Decision Support Systems*, vol. 55, no. 3, pp. 740–752, 2013.

[3] M. S. Featherman and N. Hajli, "Self-service technologies and e-services risks in social commerce," *Journal of Business Ethics*, vol. 1-19, 2015.

[4] C. Q. Hu, W. Li, X. Z. Cheng, J. G. Yu, S. L. Wang, and R. F. Bie, "A secure and verifiable access control scheme for big data storage in clouds," *IEEE Transactions on Big Data*, vol. 8, no. 12, pp. 364–375, 2019.

[5] A. Alrawais, A. Alhothaily, X. Cheng, C. Hu, and J. Yu, "Secureguard: a certificate validation system in public Key infrastructure," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, pp. 5399–5408, 2018.

[6] C. Q. Hu, Y. W. Pu, F. H. Yang, R. F. Zhao, A. Alrawais, and T. Xiang, "Secure and efficient data collection and storage of IoT in smart ocean," *IEEE Internet of Things Journal*, vol. 99, pp. 1–15, 2020.

[7] T.-P. Liang, Y.-T. Ho, Y.-W. Li, and E. Turban, "What drives social commerce: the role of social support and relationship quality," *International Journal of Electronic Commerce*, vol. 16, no. 2, pp. 69–90, 2011.

[8] H. Zou, Z. Gong, N. Zhang, W. Zhao, and J. Guo, "Trustrank: a cold-start tolerant recommender system," *Enterprise Information Systems*, vol. 9, no. 2, pp. 117–138, 2015.

[9] S. Kim and H. Park, "Effects of various characteristics of social commerce (s-commerce) on consumers' trust and trust performance," *International Journal of Information Management*, vol. 33, no. 2, pp. 318–332, 2013.

[10] M. Chowdhury, A. Thomo, and B. Wadge, "Trust-based infinitesimals for enhanced collaborative filtering," in *Proceedings of the 15th International Conference on Management of Data (COMAD*, Hyderabad India, January 2009.

[11] J. O. Donovan and B. Smyth, "Trust in recommender systems," in *Proceedings of the 10th International Conference on Intelligent User Interfaces (IUI)*, pp. 167–174, San Diego, CL, USA, January 2005.

[12] A. Davoudi and M. Chatterjee, "Social trust model for rating prediction in recommender systems: effects of similarity, centrality, and social ties," *Online Social Networks and Media*, vol. 7, pp. 1–11, 2018.

[13] J. W. Su and D. Manchala, "Building trust for distributed commerce transactions," in *Proceedings of 17th International Conference on Distributed Computing Systems*, pp. 322–329, Baltimore, MD. USA, May 1997.

[14] X. Lin, X. Wang, and N. Hajli, "Building E-commerce satisfaction and boosting sales: the role of social commerce trust and its antecedents," *International Journal of Electronic Commerce*, vol. 23, no. 3, pp. 328–363, 2019.

[15] B. Song, M. M. Hassan, A. Alamri et al., "A two-stage approach for task and resource management in multimedia cloud environment," *Computing*, vol. 98, no. 1-2, pp. 119–145, 2016.

[16] N. Hajli, J. Sims, A. H. Zadeh, and M.-O. Richard, "A social commerce investigation of the role of trust in a social networking site on purchase intentions," *Journal of Business Research*, vol. 71, pp. 133–141, 2017.

[17] C. Kiss and M. Bichler, "Identification of influencers - measuring influence in customer networks," *Decision Support Systems*, vol. 46, no. 1, pp. 233–253, 2008.

[18] Y. Cen, J. Zhang, G. Wang et al., "Trust relationship prediction in alibaba E-commerce platform," *IEEE Transactions on Knowledge and Data Engineering*, vol. 32, no. 5, pp. 1024–1035, 2020.

[19] H. Rong, T. Ma, J. Cao, Y. Tian, A. Al-Dhelaan, and M. Al-Rodhaan, "Deep rolling: a novel emotion prediction model for a multi-participant communication context," *Information Sciences*, vol. 488, pp. 158–180, 2019.

[20] T. H. Ma, H. Rong, Y. S. Hao, J. Cao, Y. Tian, and M. Al-Rodhaan, "A novel sentiment polarity detection framework for Chinese," *IEEE Transaction on Affective Computing*, vol. 9, 2019.

[21] P. D. Meo, A. Nocera, D. Rosaci, and D. Ursino, "Recommendation of reliable users, social networks and high-quality resources in a social internetworking system," *Ai Communications*, vol. 24, no. 1, pp. 31–50, 2011.

[22] D. Li, G. J. Browne, and J. C. Wetherbe, "Why do internet users stick with a specific web site? a relationship perspective," *International Journal of Electronic Commerce*, vol. 10, no. 4, pp. 105–141, 2006.

[23] H. Ma, M. R. Lyu, and I. King, "Learning to recommend with trust and distrust relationships," in *Proceedings of the 3rd ACM Conference on Recommender Systems*, pp. 188–196, New York, NY, USA, October 2009.

[24] T. Wu, K. Zhang, X. Liu, and C. Cao, "A two-stage social trust network partition model for large-scale group

decision-making problems," *Knowledge-Based Systems*, vol. 163, no. 1, pp. 632–643, 2019.

[25] B. Al-Otibi, N. Al-Nabhan, and Y. Tian, "Privacy-preserving vehicular rogue node detection scheme for fog computing," *Sensors*, vol. 19, no. 4, p. 965, 2019.

[26] P. Zhang, Y. Kong, and M. Zhou, "A domain partition-based trust model for unreliable clouds," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2167–2178, 2018.

[27] Y. Tian, M. M. Kaleemullah, M. A. Rodhaan, B. Song, A. Al-Dhelaan, and T. Ma, "A privacy preserving location service for cloud-of-things system," *Journal of Parallel and Distributed Computing*, vol. 123, pp. 215–222, 2019.

[28] P. Zhang, M. Zhou, and Y. Kong, "A double-blind anonymous evaluation-based trust model in cloud computing environments," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 9, pp. 1–12, 2019.

[29] A. Josang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems*, vol. 43, pp. 618–644, 2007.

[30] S.-R. Yan, X.-L. Zheng, Y. Wang, W. W. Song, and W.-Y. Zhang, "A graph-based comprehensive reputation model: exploiting the social context of opinions to enhance trust in social commerce," *Information Sciences*, vol. 318, pp. 51–72, 2015.

[31] K. Choi, D. Yoo, G. Kim, and Y. Suh, "A hybrid online-product recommendation system: combining implicit rating-based collaborative filtering and sequential pattern analysis," *Electronic Commerce Research and Applications*, vol. 11, no. 4, pp. 309–317, 2012.

[32] E. R. Núñez-Valdéz, "Implicit feedback techniques on recommender systems applied to electronic books," *Computers in Human Behavior*, vol. 28, no. 4, pp. 1186–1193, 2012.

[33] Y. Koren, R. Bell, and C. Volinsky, "Matrix factorization techniques for recommender systems," *Computer*, vol. 42, no. 8, pp. 30–37, 2009.

[34] H. Wen, L. Fang, and L. Guan, "A hybrid approach for personalized recommendation of news on the web," *Expert Systems with Applications*, vol. 39, no. 5, pp. 5806–5814, 2012.

[35] A. M. T. Ali-Eldin, "Trust prediction in online social rating networks," *Ain Shams Engineering Journal*, vol. 9, no. 4, pp. 3103–3112, 2018.

[36] D. H. McKnight and N. L. Chervany, "What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology," *International Journal of Electronic Commerce*, vol. 6, no. 2, pp. 35–59, 2001.

[37] Y. Pu, T. Xiang, C. Hu, A. Alrawais, and H. Yan, "An efficient blockchain-based privacy preserving scheme for vehicular social networks," *Information Sciences*, vol. 540, pp. 308–324, 2020.

[38] D. Liben-Nowell and J. Kleinberg, "The link-prediction problem for social networks," *Journal of the American Society for Information Science and Technology*, vol. 58, no. 7, pp. 1019–1031, 2007.

[39] G. Fortino, A. Liotta, F. Messina, D. Rosaci, and G. M. L. Sarne, "Evaluating group formation in virtual communities," *IEEE/CAA Journal of Automatica Sinica*, vol. 7, no. 4, pp. 1003–1015, 2020.

[40] M. N. Hajli, "The role of social support on relationship quality and social commerce," *Technological Forecasting and Social Change*, vol. 87, pp. 17–27, 2014.

[41] P. D. Meo, A. Nocera, G. Terracina, and D. Ursino, "Recommendation of similar users, resources and social networks in a social internetworking scenario," *Information Sciences*, vol. 7, pp. 1285–1305, 2011.

[42] H. Ma, "On measuring social friend interest similarities in recommender systems," in *Proceedings of the ACM SIGIR*, pp. 465–474, Xi'an, China, December 2014.

[43] J. S. Breese, D. Heckerman, and C. Kadie, "Empirical analysis of predictive algorithms for collaborative filtering," *Uncertainty in Artificial Intelligence*, vol. 18, pp. 43–52, 1998.

[44] Y. Asim, A. K. Malik, B. Raza, and A. R. Shahid, "A trust model for analysis of trust, influence and their relationship in social network communities," *Telematics and Informatics*, vol. 36, pp. 94–116, 2019.

[45] S. Gao, M. Zhou, Y. Wang, J. Cheng, H. Yachi, and J. Wang, "Dendritic neuron model with effective learning algorithms for classification, approximation, and prediction," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 30, no. 2, pp. 601–614, 2019.

[46] J. Wang and T. Kumbasar, "Parameter optimization of interval type-2 fuzzy neural networks based on PSO and BBBC methods," *IEEE/CAA Journal of Automatica Sinica*, vol. 6, no. 1, pp. 247–257, 2019.