IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 9, 2020, accepted October 27, 2020, date of publication November 9, 2020, date of current version November 19, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3036716

Trust Research on Behavior Evaluation Based on Fuzzy Similarity

LIMIAO LI[1], JIAYIN FENG[2], HUI YE[1], AND XIN LIU[1]
[1]School of Computer Engineering and Applied Mathematics, Changsha University, Changsha 410003, China
[2]School of Mathematics and Information Science and Technology, Hebei Normal University of Science and Technology, Qinhuangdao 066004, China

Corresponding author: Jiayin Feng (feng_ada2000@163.com)

This work was supported in part by the Natural Science Foundation of Hunan Province under Grant 2020JJ4647 and Grant 2020JJ6064, in part by the Outstanding Youth Project of the Hunan Education Department under Grant UQ19B056 and Grant 18B410, in part by the General Project of the Hunan Education Department under Grant 19C0171, in part by the General Project of the Changsha Technology Bureau under Grant KC1809015, and in part by the Teaching Research Project of the Hebei Normal University of Science and Technology under Grant SZYB202014.

ABSTRACT As the society and technology are developing, people tend to spend more time online in daily life frequently, such as shopping, reading novels, sharing files and so on. However, how to guarantee the safety of their online behaviors has been a topic of public concern, and the trust of node behaviors in the network has become one of the significant guarantees. A trust model based on fuzzy similarity is proposed in this article in accordance with the features of node behaviors. Firstly, the evaluation message is given to various nodes, and the theory of fuzzy similarity is applied to process the evaluation message. Through integrating these evaluation message, the rules of node behaviors are obtained, Besides, for the malicious and selfish nodes, the trust update algorithm is proposed. Simulation results show the effectiveness and scientific of the mode proposed.

INDEX TERMS Trust model, fuzzy similarity theory, trust, node behavior.

I. INTRODUCTION

In recent years, people come to share message and resources to the fullest and participate in various activities by taking advantage of network, such as a downloading field, communication, shopping, watching voices. However, success relies on the activities that every node cooperates with and trusts each other in the network. Because every node is highly autonomous and dynamic in an open network environment, related security problems triggered by this have been increasingly significant. Because network nodes are not managed uniformly, a lot of nodes are able to enter or leave the network, so that some illegal nodes may provide the resources with errors or virus and even make fraudulent practices, making people feel unsafe for online activities and fail to obtain reliable and effective services [1]. In this way, every node in the network can't share message and normally interact with every other, which greatly damage the normal network environment and kill people's enthusiasm for applying the Internet [2], [3].

The academic researchers have been focused on completely eradicating the potential security hazards for researching network security, including some frequently used strategies about authentication, access control, and encryption and so on. However, more traditional security technology is required. Wang *et al.* [4] proposed a traditional technology which could only protect network security to a certain extent instead of stopping malicious nodes from providing unsafe and unreliable service and preventing malicious nodes from exchanging message. Hence, it is urgent to find an effective method which can protect network security and restrain the behaviors of malicious nodes in the network, so as to ensure people's safe online behaviors [5].

Among the existing schemes of network security, Marsh [6] introduced a significant approach that the trust model of node stopped the malicious behaviors of online nodes by setting up the trust of the node model. For this scheme, the trust value of the node is calculated, and the behaviors of the node are predicted in accordance with trust value. Andersen *et al.* [7] proposed a method that good behaviors of a node were promoted to stop and punish the behaviors of malicious nodes very early, and the trust values

The associate editor coordinating the review of this manuscript and approving it for publication was Rongbo Zhu.

is taken as the basis, so that people can exchange message by choosing nodes. However, there are several deficiencies in the existing trust models.

- There are biases in trust calculation: a lot of factors exert an influence on trust evaluation, and the current trust models do not consider the factors of trust evaluation comprehensively, which will result in inaccurate evaluation of the trust values and affect the accurate access of transaction risks by entity users [8]–[10].
- For the current trust models, the credibility of the node can't be compared, so as to dynamically and effectively evaluate the message recommended. Jake *et al.* [11] proved that in case of giving some message about nodes evaluation for the competition with the node or for malicious purposes, malicious nodes are likely to make unfair and even negative evaluation, so that the trust value can't be evaluated precisely [12], [13].
- In the existing models, some dynamic malicious nodes can't be withstood. For example, some nodes can operate well at a specific time; however, after increasing their trust, some malicious behaviors will be made.

Hence, this article will take advantage of the theory of fuzzy similarity, which calculate the node trust value and the node behavior evaluation given by other nodes.

To solve the above-mentioned problems, we propose a trust evaluation based on node's behavior scheme which guarantees and calculates the node's current trust value by fuzzy similar processing of the node's evaluation level, and the Kalman principle is used to update the trust. Theoretical analysis and simulations verified the performance shifting than existing mechanisms. The main contributions of this article are summarized as follows:

(1) Fuzzy similar processing is carried out on the information of node evaluation, instead of only fuzzy processing or similar processing.

(2) the trust value of the node is updated using the Kalman principle, which eliminate the unmatched trust evaluation caused by the existence of Gaussian nois.

The rest of the paper is organized as follows. Related model schemes and trust evaluation algorithms are introduced in Section II. The problem formulation and the model are illustrated in Section III. Detailed design of the proposed trust model scheme is presented in Section IV. The trust update is illustrated in Section V. trust security algorithm is realized in Section VI. We evaluate the performance of trust model in Section VII. Finally, Section VIII concludes the paper.

II. RELATED WORK

This section investigates several trust models. Most of the models are more updated and applied as the basis of other models, for example, Poblano used the Abdul-Rahman formulas to compute the trust on basis of recommendation, and defined the cooperative threshold in accordance with [14]. Liang *et al.* [15] proposed a model where SECURE set up a shared message mechanism under the business background and demonstrated a scheme of trust delegation by digital certificates on basis of the A.JΦsang's model. In addition, a detailed risk model is set up to support trust decision. According to the introduction by Deepa and Swamynathan [16], the trust decision is on basis of cost-benefit analysis, and it includes the cost of combining risk and the probabilities of every possible outcome of a behavior. the trust decision is calculated the expected benefits and standard deviations. Fachrunnisa *et al.* [17] proposed Bayesian network-based trust model, which is based on multi-dimensional trust, and nodes should evaluate trust according to a node's ability from different perspectives. This model calculates trust by applying Bayesian network and Bayesian probability. With regard to the main disadvantage of this model, the authors assume that it is unrealistic that every node is equipped with similar Bayesian network structure because different nodes with different demands result in different network structures. While gathering recommendations from other nodes, it is assumed that every node is true in offering their feedback. Besides, this assumption is not practical because malicious nodes will often offer false feedback to other nodes, so as to damage the system [18]. Therefore, Mekouar *et al.* [19] planned to add a "dealer" of secrets during the process of setting up trust to improve it. As a centralized and known entity, this dealer sends own list of secrets to every node. This list includes k entries (i.e. identity and public key) on basis of the group scale n. Then, k certificates are issued by every node [20]. Pramod *et al.* [21] proposed that a new node must obtain two certificates issued by current members at least. Because a central authority is relied on, this method is not suitable for the opportunistic network.

Bergamini *et al.* [22] proposed a double trust measurement method which includes two trust metrics namely service trust and feedback trust, and the method could isolate service trust from feedback trust to fully use the service abilities of all the nodes even in the face of changing feedbacks. Recommendations are gathered through local broadcasting (limited by the TTL field) in this model, which is really time-consuming and in addition, recommendations shall originate from the nodes with first-hand experience of the respective target nodes [23], [24]. Wang *et al.* [25] proposed a model namely SFTrust which calculated service trust as a weighted average of local trust and recommendation trust. However, because the weight is static, the experience gained can't be properly accommodated by evaluating nodes over time. Maity and Ghosh [26] proposed TrustBAC, a model to evaluate trust relationships for access control, which strengthened RBAC like DSmTTrust [27]. Kui *et al.* [28] introduced that the model applies a trust vector with three elements: experience, knowledge, and recommendation under a specific background. A numeric value ranging from $[-1, 1]$ is used to express the value of elements. Meanwhile, these values will change because of the past effects or trust decay. The calculation of every vector component is more complicated than PTM. Based on Omnipresent Formal Trust Model (FTM), malicious nodes are prevented from taking part in any interaction, which include several issues on basis of PTM such as formalizing properties of trust, classifying trust values by applying fuzzy logic, and defining a recommendation protocol. FCTrust defines the credibility of a recommendation offering feedback by using transaction density and similarity measurement instead of weighing the quality of feedbacks by using global trust. FCTrust distinguishes the effect of offering feedbacks from that of offering services. Nevertheless, in terms of FCTrust's major flaw, all the transactions carried out within a time frame are retrieved during the process of computing direct trust, which adds storage overhead. In addition, the simple averaging function applied to define local trust assigns all the transactions with equal weight; however, recently, realistic transactions should be more important than the past transactions. For another flaw of FCTrust, reward and punishment during the computation of similarity is assigned equally, but the punishment shall be heavier than reward. Li *et al.* [29] proposed a model that Objective Trust Management Framework (OTMF) evaluates the trust taking part in nodes under a recommendation framework. OTFM is on basis of a modified Bayesian method and beta distribution function from direct and indirect message. As old observations exponentially expire, the trust is applied as the weight for indirect message. In OTFM, it is necessary for nodes to supervise the behavior of its neighbors, which can keep away from the simplicity demand further.

Other trust models are on basis of reputation. Li *et al.* [30] proposed a decentralized middleware of trust management on basis of reputation, so as to recognize reliable and unreliable peers. Every peer's reputation message is kept in its neighbors and piggy-backed on its replies to the requests for data or services. Zhao *et al.* [31] proposed a data management framework on basis of trust, so that mobile devices can access to the distributed computation available, storage and sensory resources, which also includes a reputation system according to the past encounters. At the end, it is stated that as an essential basis of security mechanisms (such as core management and safe transmission) [32], the model of nodes' trustworthiness is set up on basis of the views of their neighbors; therefore, trust is set up by a local voting scheme.

III. PROBLEM FORMULATION

For convenience, the definitions of the main symbols involved in this article are shown in Table 1.

TABLE 1. Definition of Key Mathematical Notations.

Symbol	Defination
Q_n	The evaluation information
Q	The set of evaluation information
P_n	The evaluation metrices
P	The set of evaluation metrics
W_m	The weight metrices
W	The set of weight metrices
X_{nm}	The evaluation attribute value
X_k	The result for evaluation
U	The membership matrix of R(X) collective language
u_{mn}	The membership of each evaluation language
$S(F,f)$	The degree of fuzzy similarity of evaluation results
S	The set of properties for a node
S_m	The properties for a node
TR	The sequence of evaluated times
tr_n	The evaluation in a time
Y_i	The degree of abnormality at a point
H_{AB}	The degree of emotion between node A and node B
$T(tr_i)$	The trust evaluation credibility
$V_{ab}(t+1)$	The trust change value between t and t+1
H_{AB}	The sentiment between two nodes
$V_a(t)$	The trust value at time T
$G_a(t)$	The possible trust change value at T and T+1
$U_{ab}(t)$	The trust measure of the node
$\xi_{ab}(t)$	The trust measurement error
η_{na}	Uncorrelated white Gaussian noise sequence
Q_a	Variance caused by Gaussian white noise
$\hat{V}_a(t+1/t)$	The Local trust estimate
$W_a(t)$	The total trust measurement

The message of every online node is evaluated by a lot of nodes after the transaction, and it is considered to evaluate node behavior involved in and compute the node's trust according to n pieces of message, and the definition of n pieces of evaluation message is shown below:

$$Q = \{Q_1, Q_2, \cdots Q_n\} \tag{1}$$

Suppose that there is m evaluation metrices for node behavior, it is indicated as:

$$P = \{P_1, P_2, \cdots P_n\} \tag{2}$$

where m evaluation metrics evaluate the above n pieces of evaluation message, and because every metrics expresses the different attributes of the node behavior message evaluation, a complete system is formed by m evaluation metrics of nodes behavior evaluation. Every evaluation metrics p_z $(z = 1, 2, 3 \ldots\ldots, m)$ includes the metrics P_{zi} $(I = 1, 2, 3 \ldots\ldots, \mathit{offers})$ of the next layer. The significance of indicators and relationship with the weight vector are described below:

$$W = (\mathrm{W}_1, \mathrm{W}_2, \mathrm{W}_3, \cdots \mathrm{W}_\mathrm{m})^\mathrm{T} \tag{3}$$

node master the situation in accordance with their evaluation and researches every evaluation message, which is more suitable for message analysis, and obtains the above evaluation matrix:

$$\mathrm{X_k} = \begin{bmatrix} X_{11}, X_{12}, \cdots, X_{1m} \\ X_{21}, X_{22}, \cdots, X_{2m} \\ \cdots, \cdots, \cdots, \cdots \\ X_{n1}, X_{n2}, \cdots, X_{nm} \end{bmatrix} \quad (k = 1, 2, \ldots\ldots g) \tag{4}$$

where X_k refers to the evaluation outcome which node g give out in accordance with n evaluation message correlated with m evaluation metrics and metrics weight.

Practically, everyone is accustomed to make evaluations in words and intuitively show the satisfaction degree of the evaluators. Therefore, it is considered that language is used to describe the evaluation attribute of value X_{nm} for every piece of evaluation message, and the language is divided into nine grades as defined below:

Definition 1: $R(X)$ denotes evaluation language set for X_{nm}, $Tk \in R(X)$ $(-4 < k < 4)$ is a subset of every evaluation level; the meaning of *Tl* is as follows:

$$\{T4, T3, T2, T1, T0, T\text{-}1, T\text{-}2, T\text{-}3, T\text{-}4\}$$

T4 represents full trust, *T3* represents a lot trust, *T2* represents very trust, *T1* represents more trust, *T0* represents trust, *T-1* represents more distrust, *T-2* represents very distrust, *T-3* represents a lot distrust, *T-4* represents full distrust.

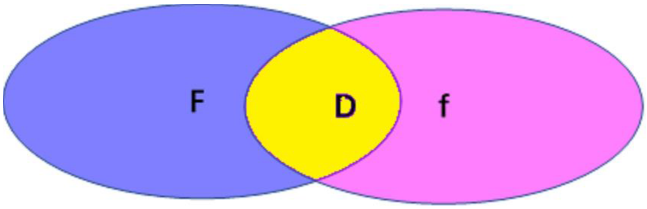


FIGURE 1. Evaluation language description of fuzzy members.

We express the evaluation message of the below uncertain fuzzy language $R(X)$ with fuzzy number respectively and determine the membership form of fuzzy numbers in this article [33]. According to Figure 1, trust *T1* and more trust *T0* for fuzzy numbers are represented by F and f respectively, and D is applied to express the intersection part of the figure between F and f areas; it can be said that the membership function belonging to $R(X)$ language means that *T1* is for $(F\text{-}D)$ / $(F\text{-}f)$, and the T0 is for $(D\text{-}f)$ / $(F\text{-}f)$.

therefore, the membership matrix of the f $R(X)$ is shown below:

$$U = (\mathrm{u_{ij}})_{m\times n} = \begin{bmatrix} u_{11}, u_{12}, \ldots, u_{1n} \\ u_{21}, u_{22}, \ldots, u_{2n} \\ \ldots, \ldots, \ldots, \ldots \\ u_{m1}, u_{m2}, \cdots, u_{mn} \end{bmatrix}$$
$$(i = 1, 2, \cdots, m; j = 1, 2, \cdots n) \quad (5)$$

While starting the evaluation, node taking part in evaluation makes an initial election evaluation of the message in trusted computation; if the evaluation message value of every metrics is greater than the rest of the Q_n value, the Q_n message value will lose to take part in trusted computation. Through the above method, the evaluation message in trusted computation is obtained, namely $Q = \{Q_1, Q_2 \ldots, Q_n\}$. With different advantages respectively, every evaluation message is non-substitutable by every other [28]. We want to deal with the similarity comparison of the evaluated message and consider every evaluation metrics in a comprehensive and systematic way, otherwise the message value will not count.

IV. MODEL DESIGN

During the node behaviors value counted, after a transaction is completed, every node will compare evaluation message of the attribute of every node behavior, so as to select the evaluation language suitable for the evaluation of this transaction, which indicates an association among nodes; the relationship is shown in Fig. 2. If node A, node B and node C have the same emotion, node A is friendly to node C, node B is friendly to node C. The following after the transaction among node A, node B and node C, the same language maybe used to evaluate node C. Hence, this kind of emotion relationship is described as similarity as a fuzzy language applied for evaluation. Therefore, the similarity is also a fuzzy similarity defined below:

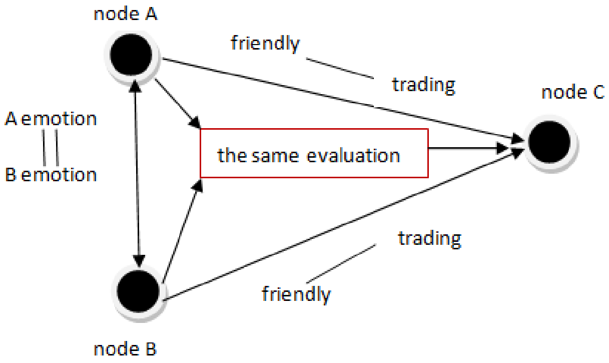


FIGURE 2. Relationship and evaluation between nodes.

Definition 2: after the transaction between node A, node B and node C, node C is evaluated in consideration of the metrics P of message evaluation by applying message from Q, the following formula gives the fuzzy similarity of evaluation outcomes:

$$S(F,f) = {D(F\cap f, 0)}/{D(F\cap f, 0) + M} \qquad (6)$$

where $M = \lambda[D'(F,f) + D''(F,f) + \beta[D'(f,F) + D''(f,F)]$

Fig. 1 D shows the above $D(F,f)$, and it is the same part where node C is evaluated by node A and node B; where $0 <= \lambda, \beta < 1$, the good impression for node A and node B to the node C determines the coefficients value of the two after the transaction. The attributes of S are shown below

(1) $0 <= S(F, \mathrm{f}) <= 1$

(2) $S(F, \mathrm{f}) = S(\mathrm{f}, F)$

(3) $1 = S(F, \mathrm{f}) <=> F = f$

Assume that g nodes in the network are trading with node C all the time after trading with the node C, the node C is evaluated in the language set $R(X)$ in consideration of the same asset, and there are Q message in total. Assume that node C has the following attributes set

$$S = \{S_1, S_2, \cdots, S_\mathrm{m}\} \qquad (7)$$

the weight vector for the attributes is shown below

$$W = (W_1, W_2, \cdots W_\mathrm{m})^T \qquad (8)$$

where W_m refers to the weight vector of the first m metrics and where $\sum_{i=1}^{m} W_i = 1$ a lonely node evaluates the node C with n pieces of evaluation message for the evaluation of integrated fuzzy similarity:

$$S_c(F,f) = \frac{S_{mn}(F,f)}{\sum\limits_{n=1}^{m} w_n S_{mn}(F,f) + Tr_0} \tag{9}$$

If $S_c(F,f) = 1$, it is denoted to that there is no difference that the node uses n pieces of evaluation message to evaluate the attributes of node C, and Tr_0 stands for the primary trust value. If $S_c(F,f) = 0$, it is denoted that there is no great difference that the node applies n pieces of evaluation message to evaluate the attributes of node C.

Therefore, it is observed that n pieces of evaluation message n pieces of evaluation messages will be more consistent if the value of $S_c(F,f)$ is bigger, and it is better to evaluate node C by reflecting the true situation. Hence, node trust is indicated as below:

$$Tr = \int_{t1}^{t2} {}^{S_c(F,f)\times Q\times U}/_{nt} \tag{10}$$

where t_1 stands for the last evaluation, *and* t_2 refers to the current evaluation.

V. TRUST UPDATE

Due to the influence of various factors, node trust is dynamic; this article manages the changes in the trust by applying the Kalman principle. It is assumed that with a sensor, every node in the feedback integrates the trust value. On basis of the past transactions among the nodes, the trust value is got. Under general circumstances, although the trust value will not be changed a lot between two transactions, minor fluctuations will be accompanied. The below equation defines the changes in the trust:

$$TT_{ab}(t+1) = {}^{TT_a(t)+G_a(t)}/_{\lfloor TT_a(t)+G_a(t)\rfloor} \tag{11}$$

where $TT_a(t)$ represents the trust value at time t, and $G_a(t)$ refers to the changes in the trust value of node a in the moments of t and $t + 1$. Suppose that it means a Gaussian white noise for the change, the change variance is set as Q_a, at the time of t, and the unequal time intervals between t and $t + 1$ only represent the transaction interval of nodes.

All the transactions between node b and node a are applied as a pass-through to measure the trust of node a, and the above equation shows the measurement function:

$$TC_{ab}(t) = {}^{TT_a(t)+\xi_{ab}(t)}\Big/\sqrt{TT_a(t)+\xi_{ab}(t)}, \quad a = 1, 2, 3 \ldots\ldots n \tag{12}$$

where n represents the total number of transactions with node a at time t; $a = 1, 2, 3 \ldots\ldots n$ is applied to indicate the number of nodes trading with node b. The number of nodes transaction with each other is kin to the number of nodes in the P2P network. $TC_{ab}(t)$ means that the measured trust value of node b relative to node a, namely, the trust of node a will be calculated by node b after node b transaction with node a. $\xi_{ab}(t)$ stands for the errors of measurement caused by the situations of the network or other conditions randomly, and the error is set as irrelevant white Gaussian noise sequence, and the variance is assumed as η_{ab}

$$W_a(t) = \left[{}^{TC_{ab}(t)}/_{\lfloor \mathrm{t}+1\rfloor}, \ldots\ldots, {}^{TC_{na}(t)}/_{\lfloor t+1\rfloor}\right]^T \tag{13}$$

$$\xi_a(t) = \left[{}^{\xi_{1a}(t)}/_{\lfloor t+1\rfloor}, \ldots\ldots, {}^{\xi_{na}(t)}/_{\lfloor t+1\rfloor}\right]^T \tag{14}$$

$$F_a(t) = \left[{}^{1}/_{\lfloor t+1\rfloor}, \ldots.., {}^{1}/_{\lfloor t+1\rfloor}\right]^T \tag{15}$$

Afterwards, the total measurement equation is indicated as below:

$$W_a(t) = {}^{F_a(t)TT_a(t)+\xi_a(t)}\Big/\sqrt{F_a(t)TT_a(t)+\xi_a(t)} \tag{16}$$

where $W_a(t)\epsilon W^{n\times 1}$, $\xi_a(t)\epsilon W^{n\times 1}$, $F_a(t)\epsilon W^{n\times 1}$, $\xi_{ab}(t)$ is the Gaussian white noise sequences unrelated, and the covariance matrix stands for $H_a = \mathrm{diag}\{\eta_{1a} \ldots\ldots, \eta_{na}\}$. For the trust value, in accordance with the changes in the trust Eq. (11) and the total trust measurement Eq. (16), predicted equation and variance equation on basis of Kalman filter are indicated below respectively:

$$\overset{\wedge}{TT}_a(t+1/t) = \frac{1}{\lfloor t+1\rfloor}\overset{\wedge}{TT}_a(t+1/t) \tag{17}$$

$$X_a((t+1)/t) = \frac{1}{\lfloor t+1\rfloor}X_a(t/t) + Q_a \tag{18}$$

In very moment, a feedback is given by the predicted estimation and variance after integrating the system to every passed of professional knowledge node. At any time t, the Kalman filter on basis of predicted estimation equation and variance equation are indicated below respectively:

$$X_{ab}((t+1)/t) = \frac{\lceil t\rceil}{\lfloor t+1\rfloor}X_a((t+1)/t) \quad a = 1, 2, 3, \ldots\ldots n \tag{19}$$

$$\overset{\wedge}{TT}_{ab}(t+1/t) = \frac{\lceil \mathrm{t}\rceil}{\lfloor t+1\rfloor}\overset{\wedge}{TT}_a(t+1/t) \quad a = 1, 2, 3, \ldots\ldots, n \tag{20}$$

The below updated trust equation of every node is obtained in accordance with the change of Eq. (11) and measurement of Eq. (12):

$$\begin{aligned}\overset{\wedge}{TT}_{ab}(t/t) &= \frac{1}{\lfloor t+1\rfloor}\overset{\wedge}{TT}_a(t+1/t) + (t+1)_{ab}(t+1) \\ &\quad \times [\frac{1}{\lceil t\rceil}TC_{ab}(t+1) - \frac{1}{\lfloor t+1\rfloor}\overset{\wedge}{TT}_a(t+1/t)] \\ &= \frac{1}{\lfloor t+1\rfloor}(1-(t+1)_{ab}(t+1))\overset{\wedge}{TT}_a(t+1/t) \\ &\quad + \frac{1}{\lceil t\rceil}(t+1)_{ab}(t+1)TC_{ab}(t+1)\end{aligned} \tag{21}$$

$$\begin{aligned}&(t+1)_{ab}(t+1) \\ &\quad = \frac{1}{\lceil t+1\rceil}X_{av}((t+1)/(t+1))/\eta_{ab}\end{aligned} \tag{22}$$

$$\begin{aligned}&X_{ab}^{-1}((t+1)/(t+1)) \\ &\quad = \frac{\lceil \mathrm{t}\rceil}{\lfloor t+1\rfloor}X_a^{-1}((t+1)/t) + 1/\eta_{ab}\end{aligned} \tag{23}$$

After the above conclusion, the total estimation function is indicated below:

$$\overset{\wedge}{TT}_{ab}((t+1)/(t+1)) \quad \text{and} \ \overset{\wedge}{TT}_{a}((t+1)/t)$$

as follows:

$$\begin{aligned}
&\overset{\wedge}{TT}_{a}((t+1)/(t+1)) \\
&\ = \frac{1}{\lfloor \mathrm{t}+1 \rfloor} X_a((t+1)/(t+1))[\sum_{i=1}^{n} X_{ab}^{-1}((t+1)/(t+1)) \\
&\quad -(n-1)X_a^{-1}((t+1)/t)\,\overset{\wedge}{TT}_{a}((t+1)/t)]
\end{aligned} \tag{24}$$

where

$$\begin{aligned}
&X_a^{-1}((t+1)/(t+1)) \\
&\ = \frac{\lfloor t \rfloor}{\lceil t+1 \rceil} \sum_{i=1}^{n} X_{ab}^{-1}((t+1)/(t+1)) - (n-1)X_a^{-1}((t+1)/t)]
\end{aligned} \tag{25}$$

$$\begin{aligned}
&\overset{\wedge}{TT}_{b}((t+1)/(t+1)) \\
&\ = \frac{1}{\lfloor t \rfloor} X_b((t+1)/(t+1)) \\
&\quad \times \frac{1}{\lceil t+1 \rceil}[\sum_{i=1}^{n} X_{Lb}^{-1}((t+1)/(t+1)\,\overset{\wedge}{TT}_{L}((t+1)/(t+1)] \\
&\quad -(L-1-\theta) \times X_b^{-1}((t+1)/t)\,\overset{\wedge}{TT}_{b}((t+1)/t)]
\end{aligned} \tag{26}$$

$$\begin{aligned}
&X_b^{-1}((t+1)/(t+1)) \\
&\ = {}^{\lfloor t \rfloor}/_{\lceil t+1 \rceil} \sum_{i=1}^{n} X_{Lb}^{-1}((t+1)/(t+1)) \\
&\quad -(L-1-\theta)X_b^{-1}((t+1)/t)]
\end{aligned} \tag{27}$$

VI. TRUST SECURITY

Our model security is analyzed by setting taobao.com as an example. On taobao.com, after the transactions among nodes, the trust value of transaction nodes may be defamed or exaggerated by malicious nodes, namely, the trust feedback greatly deviates from the actual value of the transaction node. Here, the above approach is designed to avoid malicious nodes.

It is set that node a saves the trust of node b, and four-tuple (TT_b, X_b, Q_b, b) is used to define the relationship message; TT_b stands for the recent trust value of node b, X_b refers to estimated error variance; Q_b means the changes variance in the trust of equations. In accordance with equation(17)(18), before node b takes part in transactions, the trust value of node b is predicted as TT_b, and the forecasting variance means $X_b + Q_b$ at next time in case of h nodes trading with node b; the nodes $L(L = 1, 2, \ldots\ldots h)$ get the TT_b and $X_b + Q_b$ by first visiting the node a after the transaction with node b. Node L obtains the evaluation TT_{Lb} of node b in accordance with the transaction and gets TT_{Lb} and X_{Lb} by combining Eq. (21) with Eq. (23), and node L reports the results to node a. Hence, if node L reports the trust, node L is a simple malicious inhibition node to compare TT_{Lb} with TT_b. For the specific threshold ρ_i, if TT_{Lb} satisfies $|TT_b - TT_{Lb}| \prec \rho_i$, node L is not malicious, but oppositely, node L is a malicious node, where

$$\begin{aligned}
&\overset{\wedge}{TT}_{b}((t+1)/(t+1)) \\
&\ = \frac{1}{\lfloor t \rfloor} X_b((t+1)/(t+1)) \\
&\quad \times \frac{1}{\lceil t+1 \rceil}[\sum_{i=1}^{n} X_{Lb}^{-1}((t+1)/(t+1)\,\overset{\wedge}{TT}_{L}((t+1)/(t+1)] \\
&\quad -(L-1-\theta) \times X_b^{-1}((t+1)/t)\,\overset{\wedge}{TT}_{b}((t+1)/t)]
\end{aligned} \tag{28}$$

$$\begin{aligned}
&X_b^{-1}((t+1)/(t+1)) \\
&\ = \frac{1}{\lceil t+1 \rceil} \sum_{i=1}^{n} X_{Lb}^{-1}((t+1)/(t+1)) \\
&\quad -(L-1-\theta)X_b^{-1}((t+1)/t)]
\end{aligned} \tag{29}$$

According to the above, the below description of Algorithm 1 description can be used.

Algorithm 1 The Inhibition for Malicious Nodes

```
Require: node L provide the message $(TT_{Lb}, X_{Lb})$ to node b after trading and the total message h.
Ensure: evaluation rank is updated
Initialization parameters $\theta = 0, M = \phi$
Set the number of messages from L = 1 to h
If $|TT_b - TT_{Lb}| \geq 3(X_b + Q_b)$
    then $\theta = \theta + 1$
Node L is marked as malicious node
set $M = M \cup \{L\}$
Let
  $U_X = [\sum_{L \notin M} X_{Lb}^{-1} - (h-1-\theta)(X_b + Q_b)^{-1}]$
  $U_{TT} = U_X[\sum_{L \notin M} X_{Lb}^{-1} TT_{Lb} - (h-1-\theta)(X_b + Q_b)^{-1} TT_b]$
update $X_b = U_X$
update $TT_b = U_{TT}$
End If
```

The recourses and services in the P2P networks provided by the node determine the trust evaluation of a node provided by the trade partners. In the node, trust and reputation records are kept. For the first one, the trust evaluation is recorded on basis of the services that this node gives. Regarding the second one, the reputation value provided by other nodes is recorded. Two records denote the total trust values of other nodes. A reliable node is selected to trade with the node.

The total trust value update for node is related to the trust level after mutual trading. Meanwhile, the outcomes of the trade rely on requestor pertinent. After that, the requestor is going to Re-given a weight level for the evaluations and compute the total value of node's new trust in accordance with the outcomes, the packet losing, the delay and so on for other trade conditions.

The true situation of the nodes is showed by the total trust value of TT_{ab} in case of successfully completing the transaction. In addition, if TT_{ia} is near TT_{ab} among all the intermediate nodes, node i is conducive to the transaction or node i is analogous to this node to a certain degree. Ander such circumstances, the weight of node i will be increased, and vice versa. The below pseudo code is used to describe the evaluation rank trust Algorithm 2.

Algorithm 2 Node's Trust Update

```
Require: Be prepared to trust the parameters used in
         the update including $\sigma$, $\lambda$, $\xi$, $\eta$
Ensure: TT, update trust.
if ($TT_a(t) \neq 0TT_a(t)$ and $G_a(t) \neq 0$) then
    Compute $TT_{\mathrm{ab}}(t+1)$;
    for $t = 1$ to $n$ do
        compute $TC_{\mathrm{ab}}(t)$);
        $TT[t+1] \longleftarrow -TT[t+1]/2 + TT[t]$;
        Compute equation (17);
        Compute equation (20);
    end for
else
    Compute (21);
    for $t = 1$ to $n$ do
        Compute (24)(25)(26);
        $TT_{\mathrm{a}}[t+1] \longleftarrow -TT_{\mathrm{a}}[t+1]/2 + TT_{\mathrm{a}}[t]$
        $TT_{\mathrm{b}}[t+1] \longleftarrow -TT_{\mathrm{b}}[t+1]/2 + TT_{\mathrm{b}}[t]$
        Compute (27);
        output TT[];
    end for
end if
Using Kalman filter theory to update trust;
Output new trust
```

The weight for every trade partner will be updated in a timely in accordance with the evaluation rank trust algorithm. Assuming that the weight of a node is less than the threshold value, the trade is denied, so that the success rate of trades is enhanced, and as a result, the network load has been significantly reduced.

VII. EXPERIMENTAL EVALUATION

This section evaluates our recommender model experimentally on a social platform with 1000 nodes which are fallen into goodwill nodes, malicious nodes, and selfish nodes; the number of goodwill nodes account for 0~50%, the number of malicious node account for 30%; the number of selfish nodes account for 20%. While revering the trust value, the node can answer service requests. Test scenarios are an arrangement of resource sharing with 2000 kinds of resources distributed randomly; the amount of benign resources accounts for 80%, the amount of malicious resources accounts for 15%, and the amount of selfish resources is randomly. Goodwill node primarily refers to the provision of normal services, and according to the evaluation, other nodes are authentic. Unreliable resources are provided by malicious nodes, and false evaluation of nodes is given by the transactions with nodes. Selfish node does not share node resources. The value of Tr_0 is 0.5. Under this experiment environment, trust model is compared to measure and analyze the performance of our model on basis of fuzzy theory, trust model and similarity theory.

The experimental simulation parameters are shown in Table 2.

TABLE 2. Simulation Parameters.

Parameters	Initial Value
Resource	2000
δ	0.5
ε	0.5
Node	1000
Malicious nodes	30%
Goodwill nodes	50%
Selfish nodes	20%
Benign resources	80%
malicious resource	15%
Selfish resource	5%

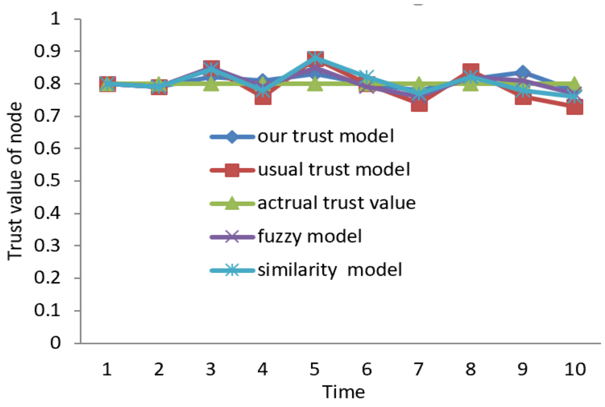


FIGURE 3. Trust value comparison.

A. TRUST VALUE COMPARISION

The value of node trust in different trust models is displayed in Fig. 3. In this article, the same node makes the same number of transactions under the experimental environment, and trust evaluation calculation is carried out for our trust models of fuzzy theory and similarity theory and the model with no mechanism, that is, common trust model. It is assumed that trust value in line with actual conditions (named real value) for the evaluated node is 0.8, and Fig. 3 shows the evaluation outcomes obtained after the transactions. According to Fig. 3, although the trust evaluation value of nodes obtained slightly changes around the actual message under the framework of the proposed model, the values given by common trust model greatly fluctuate around the actual value. In addition, the trust value of node in other two models fluctuate more greatly than that in our trust model but fluctuate more slightly, ore slightly than the common trust model. To sum up, it is indicated that our trust model comes near the actual situation, and the trust value can be used as the judgment of node selection objects to transaction with, and meanwhile, the effectiveness of model proposed by us is shown. Our trust model is more optimal than others because it considers the influence of the trust value of combining factors with feedback mechanisms.

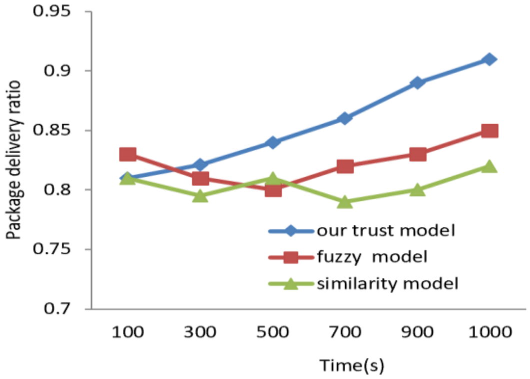


FIGURE 4. Comparison of package delivery ratios.

B. PACKAGE DELIVERY COMPARISION

The packet delivery ratio as time passes for the same transaction of three models is shown in Fig. 4. It is considered that the packet delivery ratio is the percentage of packets which are transmitted successfully. Fig. 4 indicates the case: in our trust model, the packet delivery ratio is efficiently and significantly improved by comparing with other two models. Under this circumstance, the trust value of nodes in our trust model is obtained by considering the factors influencing the real value calculated in other two models. Hence, the trust value of our model comes near the true situation, and the success rate will be higher, so that high trust value nodes will be selected in case of a transaction, and it is clearly stated that the rate of packet transfer in our model will be better than that in other models. Moreover, our model calculates the effect of one-step increase in the trust value by featuring a feedback algorithm.

C. REQUEST COMPARISION

The success request of every node for three different models with different ratios of malicious nodes is shown in Fig. 5. If three models have a smaller ratio of malicious nodes, the rate of success requests will be almost the same. Nevertheless, as malicious nodes increase, a greater advantage is reflected by our model. Other two models have a similar outcome, especially, the same outcome will be obtained when the number of malicious nodes accounts for 50% in the models.

D. ANTI-ATTACK CAPABILITY

The more reliable node trust, the stronger the node's anti-attack ability, here we construct the experiments to prove it.

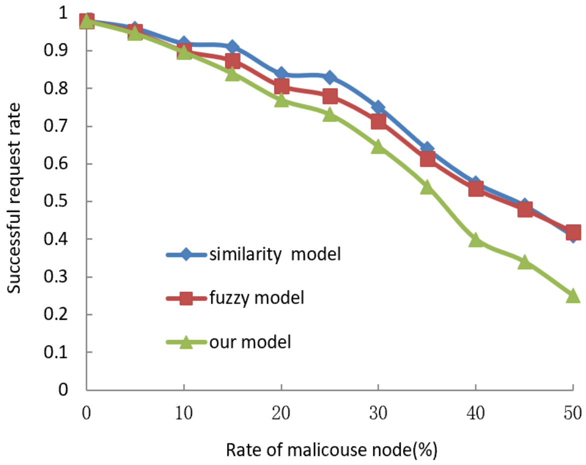


FIGURE 5. Comparison of successful request ratios.

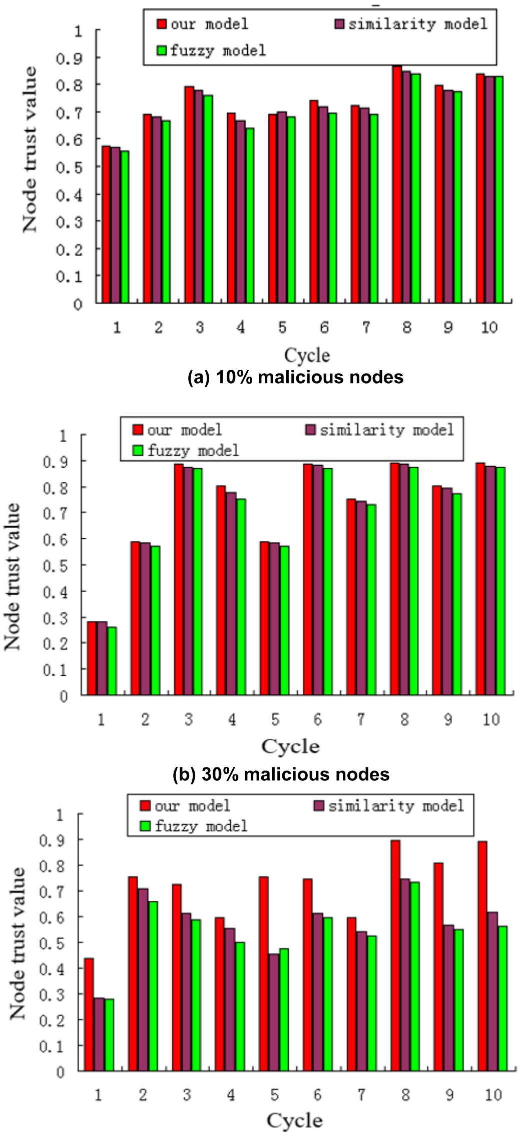
Suppose that there are 10%, 30%, and 50% malicious nodes in the network. In our model, the trust value of the first experiment node and the ratio of malicious nodes exert an influence on the performance of our model. According to the outcomes in Fig.6, different ratios of malicious nodes exert an influence on the trust value of nodes. As shown in Fig. 6(a), the trust value of nodes is greater by comparing with those in Fig. 6(b) and Fig. 6(c), which indicates that our model is equipped with poor anti-attack ability in case of the rising ratios of malicious nodes in the system. Nevertheless, by comparing Fig. 6(b) with Fig. 6(c), it is observed that our model effectively restrains the activities of malicious nodes to obtain higher trust value of nodes in case of 50% of malicious nodes.

E. TRANSACTION SUCCESS RATE

Fig. 7 shows the comparison of the node transaction success rate between our model and the fuzzy model and similarity model trust model with the increasing of selfishness nodes in a cycle. Based on Fig. 7, we can see that the node evaluation in our model comes near the actual situation because the success rate of choosing a node with a high degree of trust for transactions is much higher than that of a trust model with only a fuzzy model or a similarity model. The fuzzy model and the similarity model only deal with the uncertainty of the trust evaluation and the similarity of the evaluation message, while our model deals with the uncertainty of the trust evaluation and the uncertainty evaluation given by every node. After evaluating similar processing, the trust value obtained is more accurate, and the transaction success times selected nodes is better than the trust model of fuzzy model and similar model.

F. TRASACTION DELAY COMPARISON

Fig. 8 shows the comparison of the node transaction delay time between our model and the fuzzy model and similarity model trust model as malicious nodes increase. On the basis



(a) 10% malicious nodes

(b) 30% malicious nodes

(c) 50% malicious nodes

FIGURE 6. Anti-attack capability comparison.

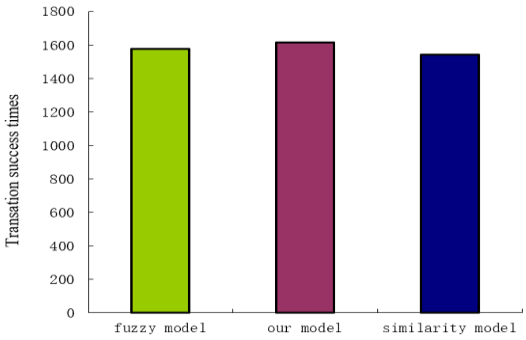


FIGURE 7. Transaction success comparison.

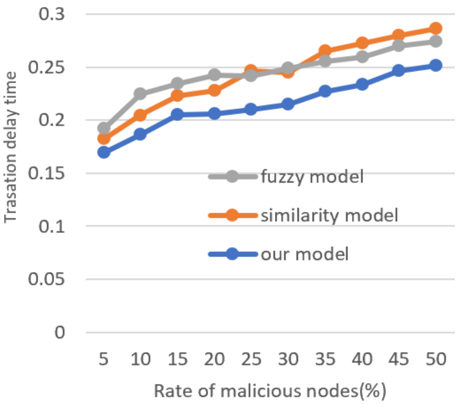


FIGURE 8. Transaction delay time comparison.

of Fig. 8, we can see that the node transaction time of our model is smaller than the other two models because our model with a high degree of trust for transactions nodes is much higher than that of a trust model with only a fuzzy model or a similarity model. After evaluating similar processing, the trust value obtained is more accurate, and the transaction delay times selected nodes is bad than the trust model of fuzzy model and similar model.

G. SYSTEM OVERHEAD OF OUR MODEL

This experiment measures the system overhead during the process that trust mechanism system is running by using the network flow, including the total query message request, response message and closing message. In the networks with different scales, the network flow is shown in Fig. 9 if the successful file service provided by goodwill node is more than 95%. In case of small networks, it appears that networks flow is a little bit different. However, as the scale of networks increases, the flow of networks will rise quickly.

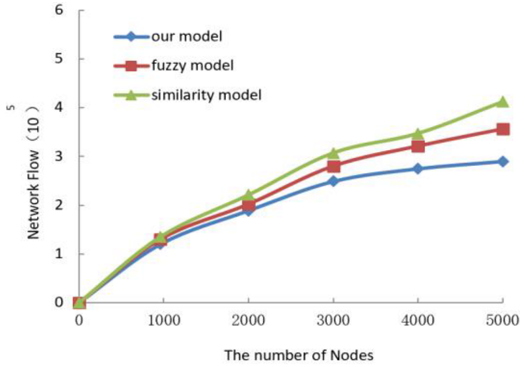


FIGURE 9. Transaction delay time comparison.

Our model is more optimal than the other two because Kalman Filter mechanisms and evaluation rank are adopted to calculate the trust value of nodes, so that trust value reflect the actual situation of nodes in our model system, and the node that has a higher trust value will be selected if nodes require request service. Therefore, in our model, nodes possess a higher successful transaction ratio and decreases the flow of networks effectively.

VIII. CONCLUSION

As the network environment changes quickly, issues related to network security have been a problem of public concern. Because the selection of a trust transaction node is one of the factors people must consider, trust model is proposed on basis of node trust evaluation. In case of evaluating the trust of a node, evaluation message given by every node must be got through processing the theory of fuzzy similar, so as to obtain the trust value of the node. In the calculation of the trust value, the paper pays attention to make a similar calculation of the fuzzy domain of trust evaluation message, besides, for the security of the model, a feedback algorithm is proposed to withstand the actions of malicious nodes and prevent wrong, fraudulent, slanderous and bad behaviors of online nodes, so as to guarantee a safe network environment. At the end, by applying simulation analysis, our trust model based on fuzzy theory and similar theories is more scientific and safer than common trust model. In the future, we will further study the influence of node behavior on the trust model and the evolution of the model.

REFERENCES

[1] S. Moalla, B. Defude, and S. Hamdi, "A new trust management model in P2P systems," in *Proc. 6th Int. Conf. Signal-Image Technol. Internet Based Syst.*, Oct. 2010, vol. 51, no. 10, pp. 2529–2553.

[2] D. Wei and Q. J. Jiao, "A novel core-peer based trust model for peer-to-peer networks," *J. Comput. Theor. NanoSci.*, vol. 23, no. 11, pp. 45–58, 2017.

[3] L. Ma and Z. Wei-Ming, "Survey of research on dynamic trust mechanism in grid environment," *J. Chin. Comput. Syst.*, vol. 29, no. 2, pp. 825–830, 2018.

[4] W. Li-Juan, Z. Guang-Hui, and C. Shan, "A trust model under grid computing environment," in *Message Engineering and Applications* (Lecture Notes in Electrical Engineering). 2012, pp. 420–428.

[5] K. Ren, T. Li, Z. Wan, F. Bao, R. Deng, and K. Kim, "Highly reliable trust establishment scheme in ad hoc networks," pp. 354–367, 2012.

[6] S. A. Marsh, "Formalizing trust as a computational concept," Ph.D. dissertation, Dept. Math. Comput. Sci., Univ. Stirling, Stirling, U.K., 1994.

[7] R. Andersen, C. Borgs, J. Chayes, U. Feige, A. Flaxman, A. Kalai, V. Mirrokni, and M. Tennenholtz, "Trust-based recommendation systems: An axiomatic approach," in *Proc. 17th Int. Conf. World Wide Web (WWW)*, Beijing, China, 2008, pp. 199–208.

[8] S. Chakraborty, J. Adams, M. Nassiri, and G. H. Vance, "Therapy-related myeloid neoplasm with bone marrow involvement, myelosarcoma, and a t(8;16)(p11.2;p13.3)—A case report," *Cancer Genet.*, vol. 207, nos. 10–12, pp. 511–515, Oct. 2014.

[9] D. Jiang, Z. Zheng, G. Li, Y. Sun, J. Kong, G. Jiang, H. Xiong, B. Tao, S. Xu, H. Liu, and Z. Ju, "Gesture recognition based on binocular vision," *Cluster Comput.*, vol. 22, no. 6, pp. 13261–13271, 2019.

[10] L. Dong, W. Wu, Q. Guo, M. N. Satpute, T. Znati, and D. Z. Du, "Reliability-aware offloading and allocation in multilevel edge computing system," *IEEE Trans. Rel.*, early access, May 15, 2019, doi: 10.1109/TR.2019.2909279.

[11] Y. Jake *et al.*, "Advancing the strategic messages affecting robot trust effect: The dynamic of user- and robot-generated content on human-robot trust and interaction outcomes," *Cyberpsychol., Behav. Social Netw.*, pp. 3465–3478, Jan. 2016.

[12] M. H. Nguyen and D. Q. Tran, "A computational trust model with trustworthiness against liars in multiagent systems," in *Computational Collective Intelligence. Technologies and Applications*. Berlin, Germany: Springer-Verlag, 2012, pp. 446–455.

[13] Z. Chen, D. Chen, Y. Zhang, X. Cheng, M. Zhang, and C. Wu, "Deep learning for autonomous ship-oriented small ship detection," *Saf. Sci.*, vol. 130, Oct. 2020, Art. no. 104812.

[14] Y. Zhang, S. Chen, and G. Yang, "SFTrust: A double trust metric based trust model in unstructured P2P system," in *Proc. IEEE Int. Symp. Parallel Distrib. Process.*, May 2009, pp. 1–7.

[15] L. Zhao, T. Hua, C.-T. Lu, and I.-R. Chen, "A topic-focused trust model for Twitter," *Comput. Commun.*, vol. 76, pp. 1–11, Feb. 2016.

[16] R. Deepa and S. Swamynathan, "A trust model for directory-based service discovery in mobile ad hoc networks," in *Recent Trends in Computer Networks and Distributed Systems Security* (Communications in Computer and Information Science), vol. 420. New York, NY, USA: Springer-Verlag, 2014, pp. 115–126.

[17] O. Fachrunnisa, A. Adhiatma, and H. K. Tjahjono, "Collective engagement and spiritual wellbeing in knowledge based community: A conceptual model," in *Proc. Conf. Complex, Intell., Softw. Intensive Syst.* Cham, Switzerland: Springer, 2019, pp. 899–906.

[18] A. Das and M. M. Islam, "SecuredTrust: A dynamic trust computation model for secured communication in multiagent systems," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 2, pp. 261–274, Mar. 2012.

[19] L. Mekouar, Y. Iraqi, and R. Boutaba, "A reputation management and selection advisor schemes for peer-to-peer systems," in *Proc. 15th IFIP/IEEE Int. Workshop Distrib. Syst., Oper. Manage.*, 2009, pp. 534–541.

[20] S. Moalla and M. Rahmouni, "Trust path: A distributed model of search paths of trust in a peer-to-peer system," *Secur. Commun. Netw.*, vol. 8, no. 3, pp. 360–367, 2015.

[21] P. S. Pawar, M. Rajarajan, T. Dimitrakos, and A. Zisman, "Trust model for cloud based on cloud characteristics," in *Proc. IFIP Int. Conf. Trust Manage.*, vol. 401, 2013, pp. 239–246.

[22] E. Bergamini, H. Meyerhenke, and C. L. Staudt, "Approximating betweenness centrality in large evolving networks," *Comput. Sci.*, vol. 9, no. 6, pp. 155–166, 2015.

[23] Q. Guo, Y. Guo, and C. Guo, "Alternative ranking based on fuzzy similarity in group decision-making," *J. Southwest Jiaotong Univ.*, vol. 45, no. 2, pp. 307–311, 2010.

[24] W. W. X. Xia, M. Wozniak, X. Fan, R. Damasevicius, and Y. Li, "Multi-sink distributed power control algorithm for cyber-physical-systems in coal mine tunnels," *Comput. Netw.*, vol. 161, pp. 210–219, Oct. 2019.

[25] S. Wang, K. Lu, M. Li, Q. Zhen, and X. Che, "Fighting pollution attack in peer-to-peer streaming systems: A dynamic reputation management approach," in *Proc. 3rd Int. Conf. Trustworthy Syst. Appl. (TSA)*, Sep. 2016, pp. 23–28.

[26] S. Maity and S. K. Ghosh, "A cognitive trust model for access control framework in MANET," in *Information Systems Security*. Springer, 2012, pp. 75–88.

[27] Z. Chen, L. Li, and J. Gui, "Fuzzy theory for the P2P subject trust evaluation model," *Int. J. Advancements Comput. Technol.*, vol. 8, no. 9, pp. 76–79, 2012.

[28] X. Kui, Y. Sun, S. Zhang, and Y. Li, "Characterizing the capability of vehicular fog computing in large-scale urban environment," *Mobile Netw. Appl.*, vol. 23, no. 4, pp. 1050–1067, Aug. 2018.

[29] L.-M. Li, Z.-G. Chen, J.-S. Gui, and X.-H. Deng, "P2P network trust model based on priority," *Comput. Eng.*, vol. 39, no. 5, pp. 148–151, 2013.

[30] T. Li, W. Liu, T. Wang, Z. Ming, X. Li, and M. Ma, "Trust data collections via vehicles joint with unmanned aerial vehicles in the smart Internet of Things," *Trans. Emerg. Telecommun. Technol.*, p. e3956, Apr. 2020.

[31] Y. Zhao, T. Wang, S. Zhang, and Y. Wang, "Towards minimum code dissemination delay through UAV joint vehicles for smart city," *IET Commun.*, vol. 14, no. 15, pp. 2442–2452, 2020, doi: 10.1049/iet-com.2019.1205.

[32] Y. Ren, Z. Zeng, T. Wang, S. Zhang, and G. Zhi, "A trust-based minimum cost and quality aware data collection scheme in P2P network," *Peer-Peer Netw. Appl.*, vol. 13, no. 6, pp. 2300–2323, Nov. 2020, doi: 10.1007/s12083-020-00898-2.

[33] X. Kui, A. Samanta, X. Zhu, S. Zhang, Y. Li, and P. Hui, "Energy-aware temporal reachability graphs for time-varying mobile opportunistic networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 10, pp. 9831–9844, Oct. 2018.

LIMIAO LI received the B.S. degree in computer science and technology from the Changsha University of Science and Technology, Hunan, China, in 2003, the M.S. degree from the Guilin University of Science and Technology, Guangxi, China, in 2008, and the Ph.D. degree in computer science and technology from Central South University, Changsha, China, in 2013.

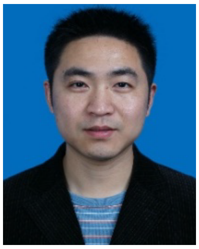
Since 2013, she has been a Lecturer with the School of Computer Engineering and Applied Mathematics, Changsha University. Her research interests include network security, algorithm optimization, and the Internet of Things.

Dr. Li is a member of China Computer Federation (CCF).

JIAYIN FENG received the B.S. degree in computer science and the M.S. degree in computer application science from Yanshan University Hebei, China, in 2005 and 2008, respectively. She has more than ten years of teaching experience in the Computer Science Department, Hebei Normal University of Science and Technology. Her research interests include information security, mobile application security, machine learning, and deep learning.

HUI YE received the B.S. degree in computer science and technology from Changsha University, Hunan, China, in 2000, the M.S. degree from Hunan University, Changsha, China, in 2005, and the Ph.D. degree in computer science and technology from Central South University, Changsha, in 2010.

From 2011 to 2016, he was a Lecturer with the School of Computer Engineering and Applied Mathematics, Changsha University, where he has been an Assistant Professor with the School of Computer Engineering and Applied Mathematics, since 2017. His research interests include wireless sensor networks, algorithm optimization, and the Internet of Things.



XIN LIU received the Ph.D. degree in computer science from NUDT, in 2009. He is currently a Vice Professor with the College of Computer Engineering and Applied Math, Changsha University (CCSU). His research interests include social networks, network routing, and software engineering. He is currently a member of CCF.