Electronic Commerce Research (2021) 21:809–830
https://doi.org/10.1007/s10660-019-09344-9

A novel trust recommendation model for mobile social network based on user motivation

Gelan Yang[1] · Qin Yang[2] · Huixia Jin[3]

Published online: 17 April 2019

Abstract

Traditional collaborative filtering recommendation algorithm has the problems of sparse data and limited user preference information. To deal with data sparseness problem and the unreliability phenomenon on the traditional social network recommendation. This paper presents a novel algorithm based on trust relationship reconstruction and social network delivery. This paper introduces the method of eliminating falsehood and storing truth to avoid the unreliable phenomenon and improves the accuracy of falsehood according to the user similarity formula based on the scale of contact established by users. In this paper, the problem of attack caused by the misbehaving nodes is investigated when the recommended information is disseminated in the existing trust model. In addition, a recommendation-based trust model is proposed that includes a defensive plan. This scheme employs the clustering techniques on the basis of interaction count, information Compatibility and node intimacy, in a certain period of time dynamically filter dishonest recommendation related attacks. The model has been verified in different portable and detached topologies. The network knots undergo modifications regarding their neighbors as well as frequent routes. The experimental analysis indicates correctness and robustness of the reliance system in an active MANET setting. Compared with the most advanced recommender system, the proposed recommendation algorithm in accuracy and coverage measurements show a significant improvement.

Keywords Trust relationship · Mobile social network · Filtering algorithm · Recommendation attack · Recommendation management

✉ Qin Yang
190682355@qq.com

Extended author information available on the last page of the article

1 Introduction

Mobile Social Network, MSNs refers to the use of hand-held mobile terminal devices using E-mail, BBS, Weibo, WeChat and other applications formed by the social interaction groups. MSNs is a product of the continuous development and integration of social network services and the mobile Internet, which seamlessly combines social computing and mobile computing [1]. MSNs are becoming more and more important due to the rapid and widespread adoption of a variety of personal wireless devices used by people, such as cell phones and GPS. With the rapid development of MSNs, the network is becoming larger and more complex, and the research on MSNs has attracted more and more attention, which concerns the relationship between friends, selfish behavior, information dissemination, privacy and security [2, 3]. The management and mining of mobile social network data has become a research hot spot in academia.

In social networks, people can not only show their preference to other users, and can establish contact with initiative and similar ideas, user trust. Some recommendation algorithm founded on the relationship of trust in social nets, credible recommender system (TARS) is put forward accordingly.

Combined filtering recommendation (CF) is a broadly utilized method, effectively used in numerous uses. This method was founded on the supposition that alike customers have alike tastes and interests. Therefore, the use of CF is similar in taste to the views of users as the target users, to provide useful recommendations. Therefore, the user is given in the project on the history score was utilized to determine alike customers, and user preference forecast. Two major problems arise with CF: sparse information and cold beginning. The cold start problem that not enough previous rating history project (or user). In the cold start project (or user), the system usually can not provide good advice.

Trust-conscious RS was proposed as an operational method to surpass the sparse information and cold beginning problem [4–6]. This method is based on the trust network trust statement between users build target customers. A core role of trust nets is to solve the problem of nearby elements choice. Trust proved that users with similar statements are highly correlated. Trust declarations may be utilized as an efficient source of data unidentified rating prediction in RS. Furthermore, the use of trust declarations in CF method may be considered to avoid malevolent occurrences.

In this paper, a recommendation-based trust model is proposed that uses an effective defense method to filter out dishonest recommendation related attacks, such as malicious attacks, ballot paper padding and connivance of mobile ad hoc networks. The recommendation node chooses its honesty based on three factors: the interaction count with the network node being evaluated, the unification of opinions with the evaluation node, the issue of knowledge lacking, and the proximity to the evaluation node. The recommendation should be made over time to ensure that the recommendation node provides advice on the evaluated nodes. In this regard, clustering techniques are used to dynamically filter the recommendations over time based on (a) the interaction count (using confidence values); (b)

assessing node compatibility (by deviation testing); and (c) tightness of the nodes. Various nodes have been selected during the evaluation to check the performance of the filtering algorithms for different mobile topologies and neighborhoods.

The rest of this work is prepared as it proceeds here, The second section The associated investigation. The third section discuss the basic methods of description and use. The fourth section the proposed method, and the fifth section. We, through experimental evaluation to prove the validity of the recommended method on 2 real world data sequences. Finally, the sixth part puts forward some opinions and conclusions.

2 Related research

In social networks, people cannot only show their preferences to other users, but they also proactively connect with trusted users who have similar beliefs. Some recommended algorithms based on trust in social networks, Trusted Recommender System (TARS), have been suggested accordingly.

However, with the fast growth in the quantity of users and products, the rapid expansion of social networks, the social network recommendation faces the challenges of data sparseness, cold start-up and inter-user trust measurement, the researchers propose some new ways to improve the lack of recommendation of social networks. Literature [7, 8] considered the user's interests and hobbies, user friends, the similarity of interest, the impact of user friends, three factors, the use of probability matrix decomposition build personalized recommendation model, thus solving the problem of cold start and data sparse. Literature [9, 10] suggested a way to enhance the recommendation process of social network based on trust with explicit untrust worthiness in social network, which provides a new information resource for social network. Literature [11] uses a combination of social networks and collaborative filtering to develop the correctness and handling of predictions. Literature [12, 13] added contextual information to the model to construct trust networks on social networks and used random walk algorithm to collect the most relevant scores of trustworthy users in trust networks. Using the decomposition model to predict the absence of context, we solve the diversity and heterogeneity of friends in social networks.

Author in [14, 15] suggested a trust model called RFSTrust on the basis of fuzzy recommendation similarity. The proposed model is employed to measure and assess the trustworthiness of the nodes. The authors employed the similarity theory to assess the recommended association between network nodes. Such that, more relationship among the evaluation knot and the recommended knot indicates the additional constant assessment between them. The proposed model considers only one node for selfish node attack, and it does not test model's performance for other attacks concerned with the recommendation. Ziegler et al. [16] proposed a trust model that encourages cooperation among the nodes utilizing observation and recommendation directly. The proposed model takes the final view of the node alone being sent to a reputation management system after finish of every interval. Taking into consideration, the final view point is not sufficient to understand the fluctuations in behavior of the node, as in the case of

switch attack [17–19]. For purpose of improving the honesty of using recommendations, Subramani et al. [20] incorporated confidence values in the assessment by aggregating the values of confidence as well as trust into a single value known as confidence. The authors used the trustworthiness value to measure the recommended node weight of the recommended node with higher trust value. The provision of collusively recommended collusion attacks is not considered in this exercise and may result in a false assessment of the advice received [21, 22].

Zhijun et al. [23] has been suggested on the basis of a recommended trust model. It utilizes the additional parameters, which are mentioned as acceptability thresholds in comparison to a level of confidence The concept of acceptability is employed for recommended computations to assure that sufficient observations of behavior of active node have been achieved. But, the selection of acceptability is a agreement between achieve a more correct value of confidence and the time for convergence it takes to acquire it. Elahi et al. [24] suggested the Recommended Exchange Protocol (REP). The protocol allows the nodes to communicate recommendations between neighboring knots. It adds the aspect of association development, on the basis of the time during the time of node for knowing each other. The recommendations suggested using longstanding connections are more or less than those of temporary connections, and the development of the association is dependent on one factor, taking into account the period of the association only.

Zhang [25] proposed a technique on the basis of clustering algorithm to separate out untrustworthy suggestions, follow most rules, select the most recommended groups as trustworthy groups, test the model, and deal with some bad mouth and ballot-filling attacks. However, most rules may not be valid because some nodes may collude with attacks and can not provide honest judgment of other nodes. Although these improvements have effectively improved the accuracy of the prediction, they all utilize the complete social network information, and do not directly deal with the existing connections between users, which to a certain extent, affect the performance of the recommended system. Therefore, the reconstruction of trust relationship can improve the accuracy of recommendation. It can be deduced from the finding of the literature that mostly the models depend on a single parameter for calculating the credibility. In order to solve these limitations, this paper presents a defensive scheme that uses multiple parameters to calculate the credibility of a referrer. The model highlights the importance of social attributes in assessing trust and is used to investigate the relationship between node intimacy and behavioral similarity. The proposed technique considers the lack of usage of time and location evidence in the current literature. False negatives and false positives have been thoroughly examined in assessing the credibility of recommendations and their impact on network performance.

3 Problem description and basic methods

The social network recommendation system contains 2 data files, user's rating data of the project and trust data between users. The user item scoring data contains a set of m users $\{a_1, a_2, \ldots, a_m\}$ and a set of n items $\{i_1, i_2, \ldots, i_n\}$, where user m scores

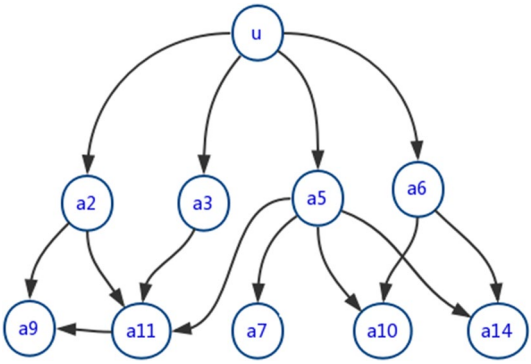


Fig. 1 User u social network attention

item n as rm, n. This article users rated the project for the five-point scale, the score is the user's level of love of the project performance. The trust relationship between users is binary data, trust is 1, no trust is 0.

Figure 1 shows the user u in the social nets, the spread of the trust map, the arrow indicates that the two users to establish contact. Among them, the circle is the user's number; the arrow points to which user represents the current user's attention to the pointed user. Find the set of friends T(u) for user u, the trust among customer u and friend v is trust of u and v Predict the user's rating on the item as follows:

$$Pu, i = \bar{R}u + \frac{\sum_{v \in T(u)} trust(u, v) \times \left(Rv, i - \bar{R}v\right)}{\sum_{v \in T(u)} trust(u, v)} \tag{1}$$

3.1 The trust relationship is challenged

Protecting your network from all kinds of attacks is indeed a challenge. Recent research in this area has focused on issues related to misconduct in packet forwarding environments such as black hole or wormhole attacks [26]. In order to ensure the quality, trust management framework is very important to resist the attacks [27]. In spite of some studies that have made significant efforts to shield the recommended transmission and aggregation in trust models, the research in this field is still in its infancy [28]. The attacks, namely Ballot Filler Attacks, Bad Mouth Attacks, Intelligent Behaviors Attacks, Time Dependent Attacks, Selective Misconduct Attacks, and Location-Relief Attacks (see Fig. 2 for attack classification) are recommended for propagation and aggregation [29–31]. This article for the first time uses location-based attacks.

The summary of the important attacks is presented in following text.

Bad mouth attack (BMA) It involves the nodes of collusion spread false positive comments of good nodes, deliberately damaging their reputation in the network. The effective routes in the net can be blocked by mixing trust and status managing mechanisms.

Ballot filling assault (BSA) Conjunction nodes on the network to some poor performance of the node spread unfair and positive assessment will contribute to

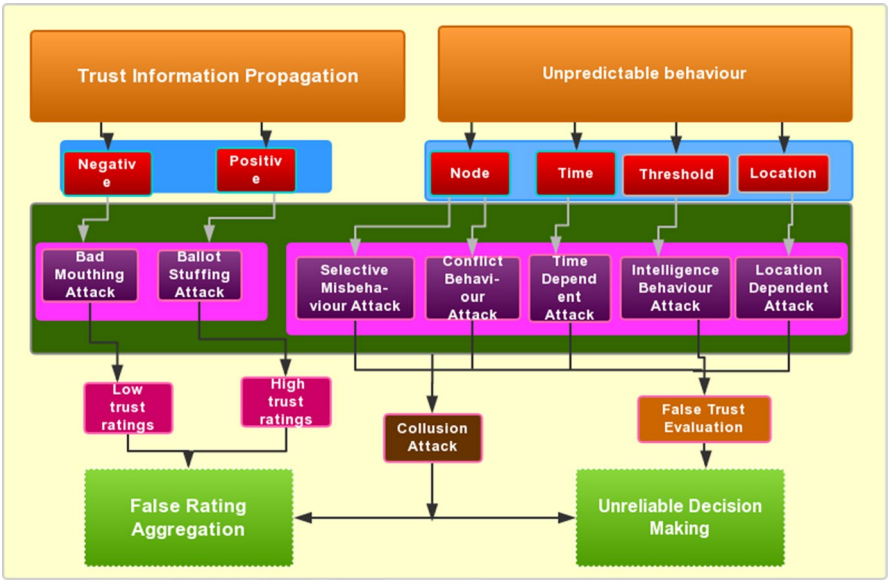


Fig. 2 Trust and reputation framework attacks related to misconduct issues in recommended management

ballot-filling attacks. The aim of a collusion node is to misguide the trust mechanism so that it fails while reporting the credibility of the node under consideration accurately.

Selective misconduct (SMA) Victims of such attacks are given some credible nodes by spreading the wrong rating, while acting normally on the other nodes. Such behavior can be a challenging task for detecting the trust mechanisms.

Intelligent behavior attack (IBA) Such attacks provide high or low ratings on the basis of the threshold of trust in a selective way. This type of attack can result in failure of the trust framework dynamically depending on the threshold value of trust and acting accordingly.

Time dependent attack (TDA) It causes active nodes to modify their behavior with passage of time. Nodes can be made active and running for certain period of time, and offering unfair ratings at some different point of times may be misbehaving. The subjective nature of trust also originate such attacks.

Location-related attack (LDA) Such attack exploits the mobility characteristics of MANET. In this case, the node behaves in a different way based upon its location. The subjective nature of trust leads to origination of such attacks. Here, the behavior at one location cannot impact the credibility of analyzing nodes at some other location.

The above cited assaults can be categorized into two different classes, namely, inconsistent ratings on the basis of trust edge, interval or position (IBA, TDA and LDA) and wrong ratings (BMA, BSA and SMA). The following text describes a few countermeasures for usage with these attack categories or specifically for attack category design. e.g., The authors of the study [32] suggest using only positive

advice, use only negative advice, which can deal with attacks such as voting pops and bad mouths. This defense can compromise trust information because the node can not report its complete experience. Statistical methods such as Bayesian theory can accurately calculate the correctness of the recommendation [33]. Full interactive proof [34] set a bar on the threshold of certain negative and positive suggestions, except for most of the opinions of technology [35], which may be used to reduce the impact of false and inconsistent ratings. An comparative analysis of time and place certification of recommended listings and recommended providers is a hopeful resolution to interval and position-related assaults as well. Initially, this algorithm considers the comparison of time and location.

It can be seen from the above discussion that the credibility of the recommended nodes can not be evaluated by only one scheme. This should be missed in the illustrated literature by utilizing various behavioral and social properties (e.g., the tightness of nodes and the proof of time and place). For the purpose of enhancing the correctness and robustness of trust models, the effect of untrustworthy suggestion must be decreased to address the issue of false positives as well as false negatives.

3.2 Recommended manager and cluster manager components

This paper provides a proposal of a recommended trust managing system that shields the directing protocols among the basis and end knots on the basis of the trust worth of every knot in the route. The suggested scheme takes attack issue debated prior into consideration for some kind of misbehavior in MANET. We suggested to employ a Bayesian numerical method on alike lines as employed by the authors of [36] for computing the trust value:

$$f(p|\alpha,\beta) = \frac{\tau(\alpha+\beta)}{\tau(\alpha)\tau(\beta)} p^{\alpha-1}(1-p)^{\beta-1} \tag{2}$$

On the basis of assumption of beta probability distribution. Beta distribution is approximated on the basis of parameters, namely, α, and β. These values can be computed by cumulative advancing and reducing observations. Thereat, the parameter α gives the increase of total explanations (advanced packages). β denotes the total of negative explanations (loss of packages). $p \in [0, 1]$; α and β are positive values when $\alpha < 1$, $p \neq 0$ and $\beta < 1$ and $p \neq 1$.

For the purpose of constructing a trust relationship, the nodes of the network analyze their behavior. Their analysis allows the nodes to determine for forwarding or holding the packets to their neighbors. The proposed model involves the relationship of initial trust between two nodes at time t as α_{ij} and β_{ij}. Here, α ij and β_{ij} give the observed positive interaction and negative iteration between knot i and knot j, respectively. At point of moment $t = 0$, we denote the initial value of the degree of trust between nodes from $\alpha_{ij} = 1$ and $\beta_{ij} = 1$, meaning that no evidence is collected or observed. The values f α_{ij} and β_{ij} can be computed as $\alpha_{ij} = \rho + 1$ and $\beta_{ij} = n + \rho$ and $n \geqq 0$, where n and ρ provides negative and positive interaction respectively. The trust metrics can be obtained from these arguments for each observation and updated to the expected value of β distribution.

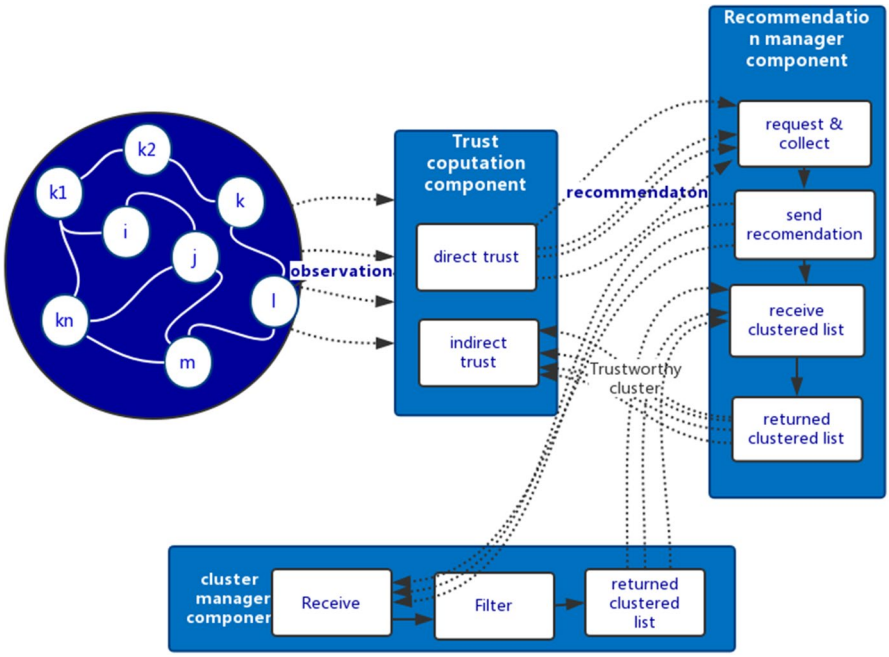


Fig. 3 Recommendations based trust model components

The suggested model employs techniques based upon clustering to maximize the level of consistency of the received suggestions. For an instance, a recommendation obtained by a mischievous network knot may possess a variety of ratings to analyze the network knot. The evaluated ratings can be inconsistent leading to confuse patterns of trust with malicious nodes, which are not similar to each other in a small span of time period. Dynamic clustering is recommended for a span of time period to find the bias ratings from the recommendations list, and hence decreasing the effect of false estimates in computing the trust values. The proposed model categorizes the recommendations on the basis of three criteria, namely, the interaction count by using confidence values, informational compatibility to the calculated knot using deviation tests and the nodes. Considering different criteria simultaneously for determining the dishonesty of a node can extenuate the impact of false negatives and false positives.

In order to compute trust, the proposed model considers three components namely, trust computing components using direct and indirect (secondhand) trust information, a recommendation manager component responsible for requesting and collecting recommendations for nodes from the set of recommended knots, and a cluster supervisor element designed for filtering the corrupt commendations using the set and sending a trusted message to the manager component suggested list. Figure 3 shows the components of the model and their interactions.

The suggested trust model employ the techniques based upon clustering to maximize the consistency level of the received suggestions. For an instance, a

recommendation from a misbehaving node may vary for different ratings to assess the node. The assessed ratings can be inconsistent, and may lead to confuse patterns of trust with malicious nodes, which are not similar to each other over a small span of time period.

The component designed for trust computations receives the value of trust directly from two network nodes having initialized the trust relationship. The two network nodes proceed to act upon each other for certain time. The value of direct trust is calculable, and calculations that are not honestly recommended are not reliable. Direct trust value T_{ij}^{d} node i and j direct trust value, calculated as shown in formula (3):

$$T_{ij}^{d} = \frac{\alpha_{ij}}{\alpha_{ij} + \beta_{ij}} \tag{3}$$

Experience changes over time, and trust models must account for the variation in effect. The suggested scheme contains a deterioration feature (μ) for the trust value. The trust value gets deceased by the impact of time before it is added with the new trust value. The past experience of forgetting is by confirming the time frame of the observation of record of positive or negative experiential experiences. But, the trust decay with passage of time in the process. During periods of inactivity, it is therefore significant for consideration of reducing the effect of trust on time. Firstly, on observation of new affirmative by the node, ρ and n will be updated, decreasing by the attenuation factor μ. Therefore, the trust value is updated according to Eq. (4) at time t_{i+1}.

$$\rho = \rho^{old} * \mu + \rho^{new}, n = n^{old} * \mu + n^{new} \tag{4}$$

In case of non establishment of prior trust relationship between two nodes through packet switching or any other method of communication, indirect trust must be considered. In this case, the evaluation experience is not sufficient to measure the reliability of the knot with the other knot. Unintended trust is as well computed by employing the beta function, same as that of the straight trust calculated in previous sections. In fact, indirect trust is a direct observation of a neighbor's neighbor. It can be utilized by the other knot as another evidence. It may be said that i's knot straight observation of knot j may be unintended or secondary evidence to the other knot with an assumption of non iteration of node i and node j.

$$\rho = \rho^{old} * \mu, n = n^{old} * \mu \tag{5}$$

It has a important effect on the chances of decreasing the credibility of the node's direct trust information and indirect trust information. Direct information is often given a higher weight by the existing models. Because, it is likely to a small extent for creating a dishonest recommendation. But, the properties like frequent variations in mobility and topology make it challenging for a node's self-assessment to fully trust the origin of information. The weights in the suggested model are dynamically computed on the basis of the number and quality of interactions assessed by the evaluation node. If the network node under evaluation has sufficient knowledge on the evaluation knot that the calculated knot is not damaged or susceptible to all terms of its surrounding (e.g., knot error or little energy degree), then the weight

Table 1 Cluster manager filtering algorithm

Algorithm 1: Recommendation Manager Algorithm
1. ***For*** each recommendation request ***Do***
2. ***Send*** request to neighbours
3. ***Collect*** received recommendations
4. ***Construct*** $L = \{k_1, k_2, k_3, \ldots, k_N\}$
5. ***Send*** L to the cluster manager for processing
6. ***Receive*** trustworthy cluster $C^{Trustworthy} = \{k_1^{Tr}, k_2^{Tr}, k_3^{Tr}, \ldots, k_N^{Tr}\}$
7. ***Send*** $C^{Trustworthy}$ to the requesting node
8. ***End*** For

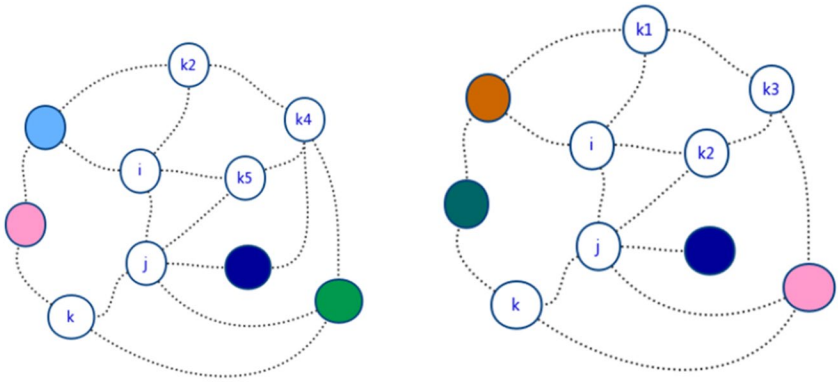
given to the evaluation node is equal to or greater than the weight of the indirect information. However, if the evaluation node can not estimate the reliability of the evaluation knot, the weight of indirect trust is given more.

Proposal Manager component in the suggested scheme behaves as an middle element among unintended trust calculation and cluster supervisor component. It allows the detection and elimination of false suggestions. The commendation supervisor plays 3 significant parts, namely, sending a recommendation request to the neighbor of the evaluation node, Collecting the established commendation message and sending this to the cluster manager running the filter program, and receiving the filtered recommendation. It is sent back to trust calculation element. The recommendation supervisor needs and collects evaluation nodes for nodes among moments t_i and t_{i+1} from the recommended node list $\{i_1, i_2, \ldots i_3$ The recommended list, and sent to the cluster supervisor to execute the filtering procedure, see Table 1. Afterward the filtering, it will receive a reliable cluster as a list of honest suggestions $\{i_{1tr}, i_{2tr}, \ldots, i_{3tr}, \ldots\}$.

3.3 Cluster-based recommendation filtering

This section examines the recommended features, the component called cluster manager and presents their interaction for filtering the untrusted recommendations. The suggested technique used for filtering process involves considering the dynamics of a MANET with passage of time. The section also presents the evaluation of the honesty of recommended nodes over a period of time for handling their adverse effects for that time span. A dynamic topology of MANET has been depicted in Fig. 4 by taking into consideration the node interested for assessing the other node through recommendation of the neighbor.

The above described algorithm involves clustering of the nodes on the basis of three parameters related to the confidence, bias, and proximity. The description of the parameters and clustering process and corresponding algorithm have been presented in the following sections.



(a) Recommending nodes at time t_i **(b)** Recommending nodes at time t_{i+1}

Fig. 4 Recommended by time

3.3.1 Confidence values

In the absence of observations between nodes, the confidence value begins at 0 and increments regularly corresponding to the recorded observations count. However, dependence on only trust values may results into observations of short-term and long-term. It has been observed that nodes may possess different observation levels in spite of similar trust level. Therefore, a false estimate can result in determining whether a node is honestly recommending a node's capabilities.

First, nodes with higher confidence values (nodes that have ample interaction with the evaluated node) are suitable due to ensuring the availability of sufficient information for selecting a good recommended node. Second, it is more likely that an attacker will be recommending nodes having more value for confidence in the initial phases of the network (during lack of sufficient interaction). As a result, dishonest nodes may be excluded from the recommendation list at an early stage. The value of confidence is computed in terms of alteration of the beta dispersal after specific alteration as suggested in [37]. The node uses the assessment of confidence to draw accurate decision regarding trustworthiness of the recommended node by considering accumulated observation count for individual node. Assuming that i is the recommended evaluation node received from the recommended node, the value of confidence v_{ikconf} is computed as per Eq. (6) (Table 2)

$$V_{ik}^{conf} = 1 - \sqrt{12}\sigma_{ik}$$
$$V_{ik}^{conf} = 1 - \sqrt{\frac{12\alpha_{ik}\beta_{ik}}{\left(\alpha_{ik}+\beta_{ik}\right)^2\left(\alpha_{ik}+\beta_{ik}+1\right)}} \tag{6}$$

We compare the proposed method using calculated confidence values with (TMUC in abbreviated form) that computes value of confidence by utilizing standard

Table 2 Confidence level the proposed model has the same level of trust as the TMUC model

α	s	β	F	Trust value	Confidence level (suggested model)	Confidence level (TMUC model)
1	0	1	0	0.5	0	0.907597979
5	4	2	1	0.721151242	0.439685556	0.968846932
10	9	4	3	0.721151242	0.589423531	0.979545894
15	14	6	5	0.721151242	0.659634426	0.989755378
20	19	8	7	0.721151242	0.711546747	0.993278793
25	24	10	9	0.721151242	0.724675898	0.993906432
30	29	12	11	0.721151242	0.758848582	0.995342157
35	34	14	13	0.721151242	0.763769324	0.995862773
40	39	16	15	0.721151242	0.784784222	0.996533772
45	44	18	17	0.721151242	0.793347842	0.996896432
50	49	20	19	0.721151242	0.806346784	0.997322674

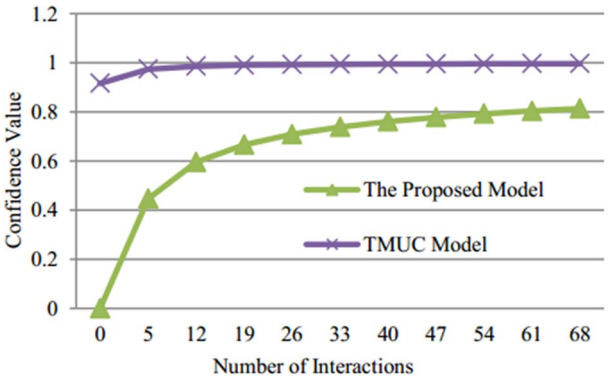


Fig. 5 The relationship between the recommended model and the TMUC model for interaction and confidence

deviation alone. The suggested approach for computing the value of confidence may present the knowledge possessed by the nodes on the basis of interaction count in an efficient manner in comparison to computation done by TMUC. For an instance, the values of $\alpha = \beta = 1$ implies lack of anterior interaction of the participating nodes. The suggested approach for computing the value of confidence as 0 and in TMUC, 0.92 that is observed closer to 1. Without interaction, start with a greater value of confidence may be ambiguous trust method and avoid it from drawing an accurate decision regarding the behavior of the node considered for evaluation purpose. Table 1 presents negative and positive interaction values for the suggested model, TMUC work and the confidence level for every level of interaction. Figure 5 illustrates the relationship between confidence and interaction for similar levels of trust.

As can be seen in Fig. 5, the suggested technique of calculating sureness provides a good confidence area in comparison to the TMUC. The change presents a good

cumulative interaction for similar values of trust (Refer Table 1). When there is no interaction, the value of confidence from the suggested model is zero, and interaction count grows. In case of TMUC, the value of confidence has been observed to be 0.92 during the absence of interaction, so when the number of interactions exceeds 19, close to the saturation level.

The deviation value represents the degree to which the received recommendation matches the personal experiment.

3.4 Evaluation node

The value of evaluation node is being utilized as a means of deviation testing in [18]. It confirms that the receiving knot POV. Every knot will receive the recommended information with their own first-hand information is compared to accept only those who do not deviate from the observation of self-information. In the suggested model, the value of bias is utilized as an extra argument for clustering algorithm that filters out the deviations above a predetermined threshold value of deviation. An issue get raised in this case of lack of lacks historical information in the node under evaluation. They acts with the node for evaluation and therefore does not offer a base comparative value. For addressing the issue, this text suggests the comparison of the confidence of nodes for evaluation and recommended nodes. The value of confidence is computed as per Eq. (7). We employed deviation tests for the nodes having similar level of confidence. With an assumption of 3 knots i, j, k, let it's knot tries to compute the amount of trust of knot in its neighborhood by utilizing the recommendation offered by node j. Here, node i initially performs an comparison of level of confidence with that of its recommended node to the conf_level, as per Eq. (7). If the difference in confidence is found to be less than the threshold conf_Threshold denoted as, then node i computes the value of deviation as the deviation of the received commendation and the straight observation of the assessed knot as per Eq. (8). Associating the resulting amount with a predetermined amount of deviation onset, we omit any advice that changes significantly from the information of the node for evaluation itself.

$$Conf\_Level = |CV_{ij} - CV_{kj}| \leq Conf\_Threshold \tag{7}$$

where CV_{ij} is the value of confidence for knot i and knot j. Where CV_{kj} is the amount of confidence for node k and node j. The deviation value V_{ij}^{dev} is computed as per Eq. (8) upon satisfaction of Eq. (7).

$$V_{ij}^{dev} = |T_{ij}^{d} - T_{kj}^{r}| \leq d^{dew} \tag{8}$$

3.4.1 Intimacy center value

Trust is a kind of social factor, so it may be applied to the perception of social life trust calculation and communication. In MANETs, an interesting research direction is to evaluate the trust between the node group environment of trust in the use of social relations, the aspect of social structure [5]. The given scheme utilizes the

aspect of an intimacy center among the evaluation node and the social trust recommendation node. Intimate centrality measures the remoteness among the assessed knot and the recommended knot based on the actual distance, hop count or delay. The closeness of the model to the model in the proposal is a amount of the remoteness among the assessment knot and the recommended knot. The usage of near-centrality enhances the filtering algorithm because proximity nodes may have the same properties and the same environmental and value network health and work over a period of time. Moreover, close friends may have more interaction when they are in friendship. Therefore, the trust values of the neighbors converge to almost the same level. This may help to identify untrusted referral nodes whose recommendations differ greatly from similar referral nodes. The intimacy value refers to the degree of closeness of the node at the recommended node close at time close, by Eq. (9).

$$v_{ik}^{close} = \sqrt{(x_i^{loc} - x_k^{loc})^2 + (y_i^{loc} - y_k^{loc})^2} \leq d^{dis} \tag{9}$$

The X^{place} and Y^{place} I and K in the node moment t position, D^{early} is a preset remoteness among knot threshold and knot threshold needs to be smaller than the communication range.

3.5 Cluster process

The cluster supervisor in the suggested scheme inputs as recommendation set using the commendation supervisor. Further, it uses the cluster method to perform operations on it. The clustering algorithm operates all the recommendations in the list by the evaluation node splitting the vectors from the recommended knots to a preset amount of clusters expressed as K. In the beginning, individual vector is assumed as a cluster. Afterwards, the clusters having minimum value of Euclidean distance are combined to form a novel cluster. Thus, the clustering procedure is applied again and again by merging the two clusters received from preceding processing till preset amount of clusters K are obtained. The clustering process initially involves merging of the vectors having closest similarity. Secondly, we can choose a trusted cluster provided recommended knots in a particular cluster meets the next conditions. It is followed by applying the majority rule to choose the cluster having highest member count. Finally, the trusted cluster get refunded to the commendation supervisor and node under evaluation to apprise its secondary trust to the knot being evaluated. The suggested cluster manager's working is presented in Algorithm 2 (Table 3).

4 Simulations and results

NS2 emulator is an freely available DES program being developed to provide sustenance for investigation pertaining to PC networks. It consists of a variety of subroutines for perform testing of many network elements like network packets, network nodes, network routing, and protocols at transport layer. Its characteristics provides capability to enhance protocol for DSR routing of MANETs architecture. The

Table 3 Cluster manager processing

Algorithm 2: Cluster Manager Algorithm
1. ***For*** each recommendation list L ***Do***
2. ***For*** each rating vector in the list (α^r, β^r) ***Do***
3. ***Calculate*** confidence value V_{ij}^{conf} as in Equ. 7
4. ***Calculate*** deviation value V_{ij}^{dev} as in Equ. 8, 9
5. ***Calculate*** closeness value V_{ij}^{close} as in Equ. 10
6. ***Construct*** data vector as $(V_{ij}^{conf}, V_{ij}^{dev}, V_{ij}^{close})$
7. ***End*** For
8. ***Initialize*** each vector as a unique cluster
9. ***Repeat***
10. ***For*** each vector ***Do***
11. ***Merge*** two clusters with the shortest Euclidean distance
12. ***End*** For
13. ***Until*** number of clusters = K
14. ***For*** each cluster that appeared in the previous iteration ***Do***
15. ***If*** $(V_{ij}^{conf} \geq d_{min}^{conf})$ and $(V_{ij}^{conf} \leq d_{max}^{conf})$ ***Then***
16. ***If*** $(V_{ij}^{dev} \leq d^{dev})$ and $(V_{ij}^{close} \leq d^{dis})$ ***Then***
17. ***Select*** trustworthy cluster
18. ***End*** If
19. ***End*** If
20. ***End*** For
21. ***For*** each chosen trustworthy cluster ***Do***
22. ***Apply*** the majority rule
23. ***Return*** trustworthy cluster $C^{Trustworthy}$
24. ***End*** For
25. ***End*** For

component of the suggested trust model is integrated to the simulator for testing the legitimacy of the suggested scheme. In a net of fifty moveable knots random simulation in the area of 700×700 square meters to move. The description of process used in simulations is as below. The enactment of the whole net performance for the 2 arguments: quantity of network and rate of packet loss, voting and selfish node packet loss rate. Evaluate the trust value (rather than bad behavior) of a good node to prevent the impact of such an attack, with and without a proposed defensive plan. The bad node (bad behavior) trust value is also assessed versus a ballot paper pop-up attack to view distortion of trust value of the node by the attacker. A similar experiment was conducted on ballot papers by studying the performance of the suggested model under generally accepted dishonest advice, as well as false negatives and false positives in the occurrence of corrupt information assaults with and without defensive schemes. Finally, a comparative study, development scheme is suggested.

4.1 The performance of evolution

The simulation process is now given. The effectiveness of the whole net into 2 arguments: net amount and package loss rate, packet loss rate of filling and selfish

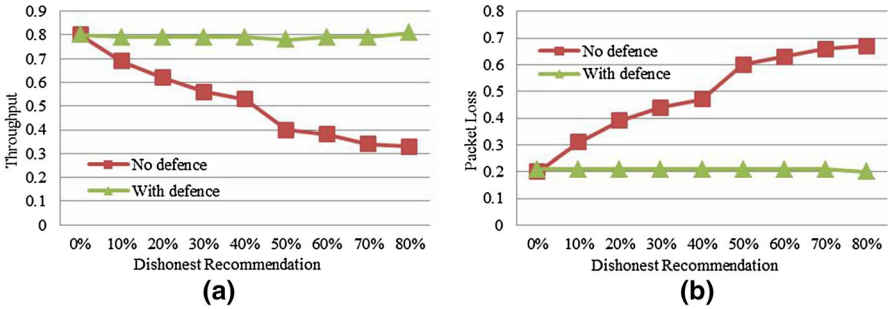


Fig. 6 Net effectiveness in the occurrence of a false recommended node **a** throughput; **b** package loss

nodes vote. For a good peer's trust value (not bad) were evaluated, in order to prevent the impact of this attack, and this attack has no merger proposed defense scheme. Bad nodes (wrong) the trust value is to evaluate votes filled assault to check this, how invaders falsify the knot's trust worth. Study on the effectiveness of the introduced recognized dishonest suggestion, and with and without defense scheme in case of false negative bad news attack and false positive. Similar experiments were carried out on the ballot. Finally, a comparative study of maturity model 24 presented in the existing research.

Figure 6 indicates the result of false suggestion on both of the effectiveness measures, namely, throughput and package loss of the net. The ordinate in Fig. 6a indicates the percentage of amount with and without defensive mechanism for a dishonest node in the presence of a 0–80% change in the entire count of knots. It has been noticed that non-defensive amount of the network deceases from nearly 80% in the absence of a dishonest node to nearly 30%, with its population increasing to 80%. When the proportion of dishonestly recommending nodes increases from 40 to 80%, the defense network throughput (Fig. 6a) decreases slightly and then increases. This may be because throughput depends on the misbehaving node count as well as degree of connectivity such that neighbor count, the capability of nodes to divide their neighbors, and the time required to obtain classification (because of network topology and mobility Sex, which is different in each simulation). However, even in the case of a dishonest node with a large population, the defense mechanism proposed maintains the value of nearly 80% of throughput. This can be explained as the ability of defensive schemes to address the negative effect of dishonest suggestion on throughput performance. Figure 6b presents the effect of dishonest nodes upon packet loss. When there is no defense in network, the rate of packet loss increases proportional to dishonest nodes increasing in range of 20–60%. Although only 20% of the packets are lost utilizing the suggested defense arrangement in the availability of a false recommended knot that range from 0 to 80% of the knots in the net. On similar lines, as percent of false recommended knots get enhanced from 70 to 80%, the percentage of packet losses get reduced to a small extent, the same as discussed in the analysis of Fig. 6a. From the above analysis, it can be seen that dishonest suggestions may confuse the trust model, thereby significantly affecting the metrics

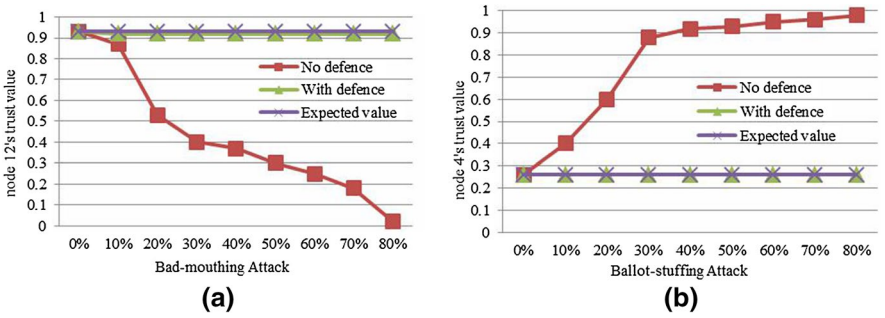


Fig. 7 Credit rating **a** trust value of good node 12 under malicious attack; **b** trust value of bad node 4 in case of voting attack

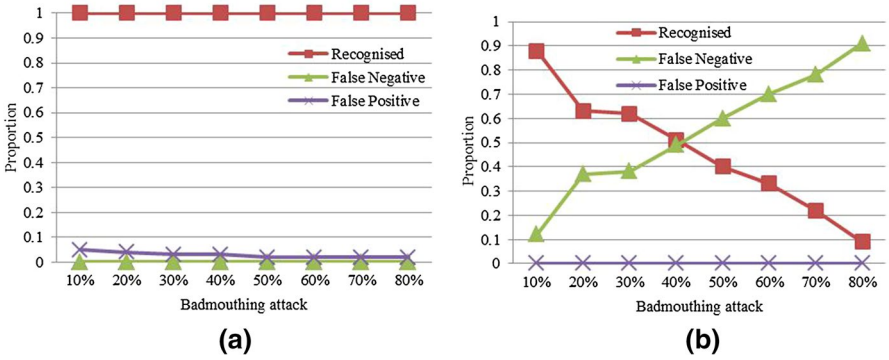


Fig. 8 **a** Recognition of defensive malware attacks, false negative and false positive ratio; **b** without defense

of throughput as well as packet loss. The suggested technique can maintain these metrics to an desirable level for high number of dishonest nodes.

Figure 7 indicates the mean of the unintended trust possessed by additional knots in the net for a respectable knot (here, knot 12) and a corrupt knot (here, knot 4). The x-axis in Fig. 7a indicates malicious node populations in range of 0–80%. The ordinate indicates the mean of unintended trust values for a respectable knot (here, node 12) possessed by all nodes with previous interactions. The following is a comparative analysis of three different arguments. Firstly, it is the indirect value of trust for no dishonest node, called the expected value. Secondly, it indirectly depends on the value of defense for dishonest nodes and the defense plan is operational. Thirdly, the dishonest node exists, the indirect value of trust that defense technology does not work, no defense. It can be observed that as the malicious attacker count get increased, the value of average trust of node 12 get decreased without any defense, while the trust value stays the same as hoped in the case of defense (Fig. 8).

Figure 10a shows the results of votes filled attack. The proposed defense plan is considered to be the recognition of dishonest recommendations, and effectively

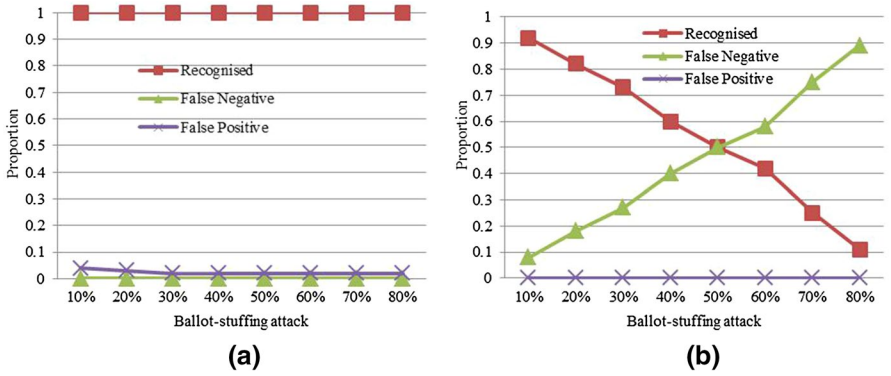


Fig. 9 **a** The percentage of false negative and false positive identified in the case of defensive ability in the case of a vote attack; **b** without defense

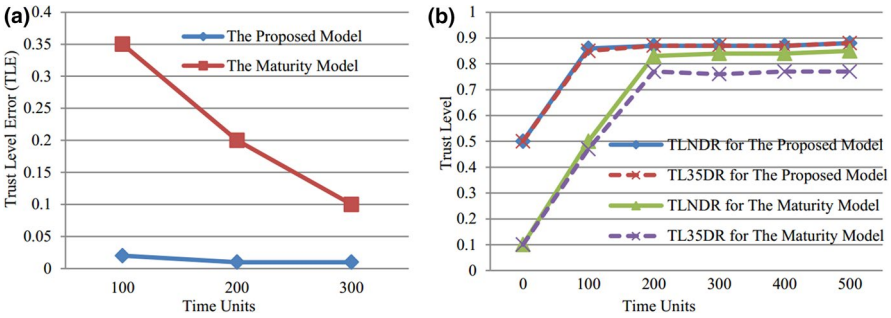


Fig. 10 **a** Trustlevel Error with time units by other nodes to evaluate node 8 trust level, **b** good nodes from the network (node 1)

eliminate the false negative. Untrue positive ratio is preserved at a sensible degree. Figure 10b in effect is obviously the honest recommendation. If there is no defensive measures, then recognition ratio decreased from about 0.9 to nearly 0.1 votes, and filling the attacker's ratio increased from 0.1 to 0.8. The proportion of false negative with the increase of the percentage of dishonest recommenders increased to nearly 0.9.

Lastly, the effectiveness of the scheme and 24 In relations of 2 metrics: a trust degree error (TDE), indicating the wrong ratio of assessing a node's trust degree (in this case, node 8); and a good node for the trust level to evaluate another node in the net for decent (here it is knot 1). We take after a similar system setup and hub choice gave in the development display (see to direct this trial. With this setup, rapid systems display high hub versatility, which is not the same as our first arrangement. This arrangement of the test organize enables us to exhibit the adequacy of the proposed arrangement. Figure 9 demonstrates the consequences of this test. Figure 10a demonstrates the trust level mistake amid the recreation time. It can be seen that the proposed model can keep the TLE not as much as

the blunder announced by the development show. On account of the proposed show, the TLE is steady all through the assessment and focalizes towards the little esteem near 0.01 later. For the development show, the underlying estimation of the TLE esteem (0.35) is higher than the estimation of the proposed model and joins to 0.1 just toward the end (time unit of 3000). Figure 10b demonstrates the adequacy assessment of the given defense plot.

Good nodes from the network (node 1). It takes into account the following: no honest recommendation (TLNDR) expected trust value, and when the given scheme and the development scheme has 35% dishonest recommendation (TL35DR) when. The outcomes display that the given defense scheme may be used to evade dishonest recommendation, the node trust value close to the anticipated amount of 1, somewhat larger than the maturity model outcomes.

4.2 Defense plan cost

The characteristics of mobile Ad hoc network is in announcement, storage use and computation difficulty requirements of limited resources. All given models or defense scheme need to possess the trade-off among the correctness and reliability of the net performance. Due to the collection and dissemination of information trust will consume more energy and resources in a distributed time between nodes, so it can improve the efficiency of decision making. From the dynamic multiple fault point and highly mobile network technology to enhance the credibility of decision nodes. Nonetheless, the given defense scheme is insubstantial in many ways. In communications, the given system is appropriate for MANET, since just the recommended demand and reply packages to submit and receive a set of recommended. The recommended packet represents a single source of information exchange between the node and the node from the assessment recommended in recommendation manager. The size of the data and the span is pretty minor, because each recommendation knot gives only 3 cumulative arguments of positive and undesirable explanations and its present location. Message is thereby strengthening. On the proposal, request recommended when needed. Therefore, defense schemes are led with no net overflowing and acquisition delays. The characteristics of the defense scheme is has the advantages of management scheme based on the role of filtering, dishonesty is recommended for three different components, which are interoperable in order to complete the job. The use of clustering in the distributed network can promote the aggregation of data, the computing capability of every knot to other nodes to reduce the credibility of the. A cost of defense is the complexity in the maintenance of clusters and choose the most reliable cluster can deal with. Another is the cost of memory consumption, the defense model takes additional storage to store the commendation for a time interval, in order to perform filtering algorithm by evaluating node operation recommendation and cluster management, but the evaluation side did not consume memory node. The additional cost is more time-consuming than the traditional defense consumption, the use of a single recommendation data to update the credibility of the knot is calculated. In the defense scheme proposed,

the cost can be reduced by using only the cluster filter last calculation to include recommendations. The number of time dynamic selection can be based on advice has several benefits, (1) decrease the difficulty and storage use, (2) to eliminate all suggestions from the previous evaluation, (3) to decrease the selection of trustworthy cluster.

5 Conclusion

Developed and analyzed a defense scheme on the basis of recommendation trust model that separates out dishonest recommendation consented with attacks exchanged by nodes in MANETs. Recommended use can effectively reduce nodes familiar with one another, without past interactions, but it discloses dishonest node and unjust recommendations. So, the suggested defense scheme employs clustering techniques to separate unjust recommendations for node shifting in the network on the basis of three arguments, namely, the level of confidence that the node has in keeping with other nodes; (b) the gap between the assurance evaluation node and the evaluation node (c) close to the center value to confirm that the recommended node is intimate with the evaluation node over time. The proposed model performs a wide range of simulation tests on throughput and packet loss, as well as against malicious attacks and vote-filling attacks, in comparison to the other scenarios. The simulative results indicates that the suggested defense approach can safely integrate the accurate evidence of indirect trust received and remove the evidence of untrust worthiness. Moreover, the impact of false negatives and false positives when selecting recommended nodes is reduced. The suggested model can be enhanced by adding the weights to the recommendations on the basis of time and position to address the effect of position and time-reliant assaults.

Funding Funding was provided by Natural Science Foundation of Hunan Province (CN) (Grant No. 2018JJ2023) and Scientific Research Fund of Hunan Provincial Education Department (Grant No. 17C0295).

References

1. Walter, F. E., Battiston, S., & Schweitzer, F. (2008). A model of a trust-based recommendation system on a social network. *Autonomous Agents and Multi-Agent Systems, 16*(1), 57–74.
2. Zhang, J., Tang, J., Liang, B., Yang, Z., Wang, S., & Zuo, J., et al. (2008). Recommendation over a heterogeneous social network. In *Ninth international conference on web-age information management*. IEEE Computer Society.
3. Jamali, M., & Ester, M. (2009). Using a trust network to improve top-N recommendation. In *ACM conference on recommender systems*. ACM.
4. Hu, J., Gao, Z., & Pan, W. (2013). Multiangle social network recommendation algorithms and similarity network evaluation. *Journal of Applied Mathematics, 2013,* 1–8.
5. Sohn, J. S., Bae, U. B., & Chung, I. J. (2013). Contents recommendation method using social network analysis. *Wireless Personal Communications, 73*(4), 1529–1546.

6. Golbeck, J. (2009). Trust and nuanced profile similarity in online social networks. *ACM Transactions on the Web, 3*(4), 1–33.
7. Yu, S. J. (2012). The dynamic competitive recommendation algorithm in social network services. *Information Sciences, 187,* 1–14.
8. Jiang, W., Wu, J., Wang, G., & Zheng, H. (2014). FluidRating: A time-evolving rating scheme in trust-based recommendation systems using fluid dynamics. In *IEEE INFOCOM 2014—IEEE conference on computer communications*. IEEE.
9. Deng, S., Huang, L., & Xu, G. (2014). Social network-based service recommendation with trust enhancement. *Expert Systems with Applications, 41*(18), 8075–8084.
10. Chen, K. H., Han, P. P., & Wu, J. (2013). User clustering based social network recommendation. *Chinese Journal of Computers, 36*(2), 349–359.
11. Cao, B., Liu, J., Tang, M., Zheng, Z., & Wang, G. (2013). Mashup service recommendation based on user interest and social network. In *2013 IEEE 20th international conference on web services (ICWS)*. IEEE.
12. Zhang, W. Y., Zhang, S., Chen, Y. G., & Pan, X. W. (2013). Combining social network and collaborative filtering for personalised manufacturing service recommendation. *International Journal of Production Research, 51*(22), 6702–6719.
13. Jamali, M., & Ester, M. (2009). Using a trust network to improve top-N recommendation. In *ACM conference on recommender systems*. ACM.
14. Dziczkowski, G., Bougueroua, L., & Wegrzynwolska, K. (2009). Social network—An autonomous system designed for radio recommendation. In *International conference on computational aspects of social networks*. IEEE.
15. Liu, S., Pan, Z., & Cheng, X. (2017). A novel fast fractal image compression method based on distance clustering in high dimensional sphere surface. *Fractals, 25*(04), 10.
16. Ziegler, C. N., & Lausen, G. (2005). Propagation models for trust and distrust in social networks. *Information Systems Frontiers, 7*(4–5), 337–358.
17. Xie, X. (2010). Potential friend recommendation in online social network. In *IEEE/ACM international conference on green computing and communications and international conference on cyber*. IEEE Computer Society.
18. Wang, Z., Sun, L., Zhu, W., Yang, S., & Li, H. (2013). Joint social and content recommendation for user-generated videos in online social network. *IEEE Transactions on Multimedia, 15*(3), 698–709.
19. Koohborfardhaghighi, S., & Kim, J. (2013). Using structural information for distributed recommendation in a social network. *Applied Intelligence, 38*(2), 255–266.
20. Subramani, M. R., & Rajagopalan, B. (2003). Knowledge-sharing and influence in online social networks via viral marketing. *Communications of the ACM, 46*(12), 300–307.
21. Davoodi, E., Afsharchi, M., & Kianmehr, K. (2012). A social network-based approach to expert recommendation system. In *International conference on hybrid artificial intelligent systems*. Berlin: Springer.
22. Jiang, W., Wu, J., Wang, G., & Zheng, H. (2014). FluidRating: A time-evolving rating scheme in trust-based recommendation systems using fluid dynamics. In *IEEE INFOCOM 2014—IEEE conference on computer communications*. IEEE.
23. Ding, Z., Li, X., Jiang, C., & Zhou, M. (2018). Objectives and state-of-the-art of location-based social network recommender systems. *ACM Computing Surveys, 51*(1), 1–28.
24. Elahi, N., Karlsen, R., & Holsbø, Einar J. (2013). Personalized photo recommendation by leveraging user modeling on social network. In *International conference on information integration and web-based applications and services*. ACM.
25. Fu-Guo, Z. (2014). Survey of online social network based personalized recommendation. *Journal of Chinese Computer Systems, 35*(7), 1470–1476.
26. Li, Y. S., Song, M. N., Hai-Hong, E., & Song, J. D. (2014). Social recommendation algorithm fusing user interest social network. *The Journal of China Universities of Posts and Telecommunications, 21,* 26–33.
27. Chen, S., Owusu, S., & Zhou, L. (2013). Social network based recommendation systems: A short survey. In *2013 international conference on social computing*. IEEE Computer Society.
28. Xia, F., Wang, W., Bekele, T. M., & Liu, H. (2017). Big scholarly data: A survey. *IEEE Transactions on Big Data, 3*(1), 18–35.
29. Sohn, J. S., Bae, U. B., & Chung, I. J. (2013). Contents recommendation method using social network analysis. *Wireless Personal Communications, 73*(4), 1529–1546.

30. Atzori, L., Iera, A., Morabito, G., & Nitti, M. (2012). The social internet of things (siot)—When social networks meet the internet of things: Concept, architecture and network characterization. *Computer Networks, 56*(16), 3594.
31. Zheng, X., Zeng, Z., Chen, Z., Yu, Y., & Rong, C. (2015). Detecting spammers on social networks. *Neurocomputing, 159,* 27–34.
32. Komiak, S. Y. X., & Benbasat, I. (2006). The effects of personalization and familiarity on trust and adoption of recommendation agents. *MIS Quarterly, 30*(4), 941–960.
33. Walter, F. E., Battiston, S., & Schweitzer, F. (2008). A model of a trust-based recommendation system on a social network. *Autonomous Agents and Multi-Agent Systems, 16*(1), 57–74.
34. Andersen, R., Borgs, C., Chayes, J., Feige, U., Flaxman, A., & Kalai, A., et al. (2008). Trust-based recommendation systems: An axiomatic approach. In *International conference on world wide web*. ACM.
35. Baofeng, S., Bin, M., Hufeng, Y., Jing, W., & Wenli, S. (2018). A novel approach for reducing attributes and its application to small enterprise financing ability evaluation. *Complexity, 2018,* 1–17.
36. Kumar, S., Singh, S. K., Abidi, A. I., Datta, D., & Sangaiah, A. K. (2017). Group sparse representation approach for recognition of cattle on muzzle point images. *International Journal of Parallel Programming, 46*(12), 1–26.
37. Liu, S., Fu, W., He, L., Zhou, J., & Ma, M. (2017). Distribution of primary additional errors in fractal encoding method. *Multimedia Tools and Applications, 76*(4), 5787–5802.

Affiliations

Gelan Yang[1] · Qin Yang[2] · Huixia Jin[3]

Gelan Yang
glyang@mail.ustc.edu.cn

Huixia Jin
14972097@qq.com

[1] Department of Computer, Hunan City University, Yiyang 413000, China

[2] School of Business, Sichuan Agricultural University, Dujiangyan 611830, China

[3] Department of Information Science and Engineering, Hunan City University, Yiyang 413000, China