Hindawi Publishing Corporation
Mobile Information Systems
Volume 2016, Article ID 5185170, 16 pages
http://dx.doi.org/10.1155/2016/5185170

Research Article

A Fuzzy Collusive Attack Detection Mechanism for Reputation Aggregation in Mobile Social Networks: A Trust Relationship Based Perspective

Bo Zhang,[1] Qianqian Song,[1] Tao Yang,[2] Zhonghua Zheng,[3] and Huan Zhang[1]

[1]*College of Information, Mechanical and Electrical Engineering, Shanghai Normal University, Shanghai 200234, China*
[2]*The Third Research Institute of Ministry of Public Security, Shanghai 201204, China*
[3]*Anhui Boryou Information Technology Co., Ltd., Hefei, Anhui 230000, China*

Correspondence should be addressed to Tao Yang; yangtao@stars.org.cn

Received 21 November 2015; Revised 25 February 2016; Accepted 6 March 2016

Academic Editor: Claudio Agostino Ardagna

While the mechanism of reputation aggregation proves to be an effective scheme for indicating an individual's trustworthiness and further identifying malicious ones in mobile social networks, it is vulnerable to collusive attacks from malicious nodes of collaborative frauds. To conquer the challenge of detecting collusive attacks and then identifying colluders for the reputation system in mobile social networks, a fuzzy collusive attack detection mechanism (FCADM) is proposed based on nodes' social relationships, which comprises three parts: trust schedule, malicious node selection, and detection traversing strategy. In the first part, the trust schedule provides the calculation method of interval valued fuzzy social relationships and reputation aggregation for nodes in mobile social networks; further, a set of fuzzy valued factors, that is, item judgment factor, node malicious factor, and node similar factor, is given for evaluating the probability of collusive fraud happening and identifying single malicious nodes in the second part; and moreover, a detection traversing strategy is given based on random walk algorithm under the perspectives of fuzzy valued nodes' trust schedules and proposed malicious factors. Finally, our empirical results and analysis show that the proposed mechanism in this paper is feasible and effective.

1. Introduction

The nature of free communication and information acquiring of mobile social networks has made them one of the most popular platforms for people's daily interactions [1]. There are massive amounts of entities which are shared among nodes on these mobile platforms. However, the open network environment has also made it unavoidable that dishonest individuals (called nodes in this work) and their malicious behaviors exist in the networks and honest nodes are vulnerable to frauds or attacks under such environment [2]. Therefore, how to counter the frauds and prevent nodes from malicious attacks has now gained much attention in network security researches.

For identifying the historical trustworthiness and predicting future likelihood of remaining reliable, a reputation system has been seen as a feasible and indispensable solution to ensuring the security of mobile social networks [3]. Commonly, a healthy reputation system can reflect a node's trustworthy degree authentically through an indicator, named reputation, by aggregating comprehensive trustable opinions from other members. A higher reputation level of a node in the reputation system implies more benefits, such as more opportunities of attracting potential followers, more forwarding, higher approving rate, and even more chances of selling products. Naturally, frauds often take place in reputation systems for acquiring more benefits. Therefore, it is essential that the reputation systems be able to recognize whether the reputation of an individual is trustworthy or not.

For most reputation systems which utilize summary/average methods based on past experiences [4], there are unavoidable threats which can endanger the reputation aggregation mechanism because all judgments are given equally for aggregating reputation [5]. Those mass dishonest

judgments, as a result, would damage the reliability of reputation systems; that is, reputation systems might show wrong trustworthiness of individuals once malicious ones attack the reputation aggregation mechanism through inflating or slandering. And worse still, the collusive attacks would bring more damage than single attacks because the scale of attack is larger and there are more attackers in collusive attacks [6, 7]. Therefore, detecting collusive attacks in reputation systems and further finding the malicious nodes in the attack in mobile social networks are a significant challenge for ensuring reputation aggregation security.

Over the course of the past decades, many efforts have been made to evaluate, recognize, predict, and prevent attacks or frauds in reputation systems [8–10]. There are three main kinds of techniques for detecting fraud in reputation aggregation: majority rule [11], signal modeling, and trust management [12]. However, most of these studies focused only on individual malicious behavior detection while an important factor, social relationship, has not been paid sufficient attentions in collusive cooperation. Another essential problem is that the collusive attack detection should be evaluated based on a fuzzy interval number rather than an exact crisp numerical value due to the uncertain nature of detection. In addition, even if malicious nodes can be recognized, it is also very difficult to recognize and verify their collusive partners, named colluders, in mobile social networks since the pairwise comparison method for detecting colluders often causes increased complexity and computation burden. Therefore, how to detect colluders with lower workload is another challenge tackled in this study. To do that, we notice that the trustworthiness relationships among nodes reflect a relative high probability of being partners in their collaborations, which also can be taken into account in collusive attack and colluder detection. That is, if a single node is recognized and verified as a malicious one, we can select the malicious one as a start point and then traverse through its trustworthy relationships to evaluate and detect colluders. From this consideration, the underlying principle of our work is that if a node maintains a higher trustworthy relationship with a verified malicious node, there would be more likelihood of being a colluder of the verified malicious one. Therefore, the main motivation of this paper includes two aspects: the need of representing the uncertainty or fuzziness of trust relationship and reputation and further the ultimate goal of evaluating and recognizing the collusions with lower workload.

To achieve that, the rationales of our proposed work are as follows: (1) social relationship is introduced to measure the closeness of nodes in mobile social networks since we assume that the malicious colluders in collusions have relatively close ties, which is denoted as high trust relationships in this work; (2) collusive frauds can be detected through evaluating the malicious probabilities of nodes based on their mutual past collaborations and behaviors; and (3) the detection can be employed by traversing the trust relationship network of nodes from a verified colluder with lower workload.

In this study, we propose a fuzzy collusive attack detection mechanism for detection of reputation systems oriented collusive attack in mobile social networks. Our main proposals in this paper are as follows: (1) the formal model of FCADM, which comprises three parts, namely, trust schedule, malicious node selection, and detection traversing strategy, and its related definitions; (2) a fuzzy trust schedule node of FCADM, which comprises trust and reputation calculation methods; (3) malicious factors, including item judgment factor, node malicious factor, and node similar factor based on fuzzy interval value for colluder evaluation and malicious node selection; and (4) a traversing strategy based on random walk algorithm for FCADM to detect colluders according to nodes' trust relationships in mobile social networks.

2. Related Work

2.1. Reputation System. In general, reputation denotes a public and authoritative view of trust obtained from an impartial community [3, 13]. Thus, we consider that reputation should be established based on all the impressions. However, to ensure fairness, reputation aggregation must prevent malicious nodes from obtaining high scores by cheating or by reducing the reputation of honest nodes. All attacks on reputation aggregation must be detected and punished.

Many studies have addressed trust and reputation in recent decades [3, 4, 14–17]. Methods have been proposed to optimize one or more aspects of trust computation, such as the summation/average/iteration of past trust ratings [18], Bayesian systems [14], and weighted average of ratings [19]. Traditionally, reputation systems have two main types of architecture: centralized [3] and distributed [18]. The former is a feasible method for a small-scale network, such as a single website, where a central authority can collect all the ratings and publish reputation scores for each participant. However, in a large-scale environment, centralized reputation system is not a reasonable method due to high costs, including high computational overheads, large storage space requirements, and time-consuming retrieval operations. By contrast, in distributed reputation systems, each member submits reputation assessments after being requested to do so by reliable members. However, the distributed nature of this scheme may lead to inconsistent opinions among nodes and malicious reputation attacks are more likely to succeed. Therefore, methods for measuring attacks on reputation aggregation are indispensable in distributed schemes.

Previous studies have also considered trust computing in social networks. For example, Ortega and colleagues [20] proposed a method for computing the rankings of nodes in social networks based on the positive and negative opinions of nodes. The opinions of others obtained from each node could then influence their global trust scores. Qureshi and colleagues [21] proposed a decentralized framework and related algorithms for trusted information exchange and social interactions among nodes based on a dynamicity-aware graph relabeling system.

2.2. Collusive Attack Detection. By observing the actions of surrounding nodes, reputation-based methods can be quite effective in combating internal active attacks or selfish behaviors. However, attacks pose great threats to reputation systems in mobile social networks [22], and even more collusive

Table 1: Main scheme feature of reputation attack detection.

Scheme	Methodology	Reference
Majority rule	Marking ratings that are far away from the majority's opinion	[11, 26–28]
Signal modeling	Detecting the rating values changing rapidly with time changing	[25]
Trust management	Calculating node's trust information to identify the honest one or malicious one	[8, 12]

attacks bring more damage to reputation aggregation system [23]. A collusion attack [24] occurs when two or more selfish or malicious nodes collaborate to make an attack without being detected. In such cases, malicious peers perform attacks with their partners in collusion and cause more damage than any single malicious peer. Many efforts have been made to evaluate, recognize, detect, and prevent collusion in reputation systems, such as majority rule [11], signal modeling [25], and trust management [8, 12]. All abovementioned methods are a kind of nonanonymous attack detection based on explicit evidences which are accessible data in network. Our proposed work in this paper, too, belongs to this kind. The main features of abovementioned method are listed in Table 1.

As shown in Table 1, in the majority rule, the ratings that are far from the opinion of the majority are marked as suspicious ratings. Representative majority-rule based techniques include statistical filtering [11, 26], an endorsement-based method [12, 27], and an entropy-based method [12, 28]. However, if the colluders comprise the majority providing ratings, collusion will be difficult to detect. Signal modeling techniques are used to detect sudden temporal changes in the features of rating values to identify collaborative attacks [25]. Trust management aims to calculate the trustworthiness of raters to evaluate how much the raters are trusted to provide honest ratings [8]. These three techniques are used widely to detect attacks both independently and jointly, and however, the main defect is that they focus on examining the rating values for individual products [12]. That is, the above schemes cannot identify whether or not an attack is collusion.

Other methods have also been proposed for collusion detection. Rossi and Pierre proposed a method for detecting generic collusion attacks, as well as preventing them by extending the path rater component of reputation-based IDS [29]. Silaghi and colleagues [30] proposed a mechanism for detecting collusion, which successfully detects malicious clients that return incorrect results with a certain probability. In our previous work, we also proposed a relationship based collusive attack detection method for social network platforms [31]. We presented a set of factors by evaluating inauthentic judgment and attack behavior similarity to detect colluders through their close relationships in social networks. By contrast, there are following newly parts as: (1) the fuzzy interval view for reputation aggregation, (2) the model of FCADM with its detail workflow, (3) a fuzzy evaluation for malicious factors, and (4) random walk based traversing strategy given in this work, which are also not included in our previous work.

However, these methods are all based on the details of malicious behaviors and evaluating all nodes in such large network environment is also a huge cost work. In our consideration, we can find colluders by checking a detected attacker's connected nodes since they would have close relationships if they cooperated for their collusion in past. Different from existing works, we have the following concerns in our scenario of collusive fraud detection: (1) the main fundamental criterion, trust and reputation measurement, of our proposed is based on a fuzzy-interval perspective, while most other methods are based on exact numerical criteria in malicious fraud detection; (2) to ensure the accuracy of malicious colluder detection, we propose a series of factors for calculating and identifying the honest individual or malicious one based on nodes' behaviors; (3) trust relationship is seen as a significant factor for detecting colluders in traversing strategy by finding colluders according to nodes' mutual trust levels. That is, if a malicious node is detected, those that have high mutual trust levels with the detected malicious one would be more likely to be colluders; and (4) the detecting strategy is designed based on *random walk* algorithm rather than a flooding searching method, which aims to decrease the complexity of our proposed method.

3. Overview of Proposed Model

Here, we address the model of collusive attractive detection and then proposed related definitions in this section.

3.1. Model of FCADM. Most collusive attacks are lunched simultaneously by a large number of *colluders* in mobile social networks through giving mass inauthentic judgments to the target individual for attacking its reputation degree. In our consideration, there are following features of reputation oriented collusions in mobile social networks as (1) inauthentic judgments are dramatically different between malicious rates and honest rates, (2) most colluders remain consistent behaviors in past if they are in a same collusive team; (3) most colluders keep similar reputation degrees because they execute almost similar behaviors, and (4) there must be close social relationships, which can be described as a trust relationship, among colluders due to necessity of communication and cooperation for collusions. Based on such features, our proposed FCADM detects collusive attack through evaluating the four above aspects among suspicious nodes. The detail workflow of FCADM model is shown as in Figure 1.

Accordingly, our proposed model of FCADM includes the following parts.

(1) Part 1: Trust Schedule. In FCADM, we define a distributed formal list for each node in mobile social networks to record its local trust information, including trust relationships with others that have interactions with it, and reputation degree

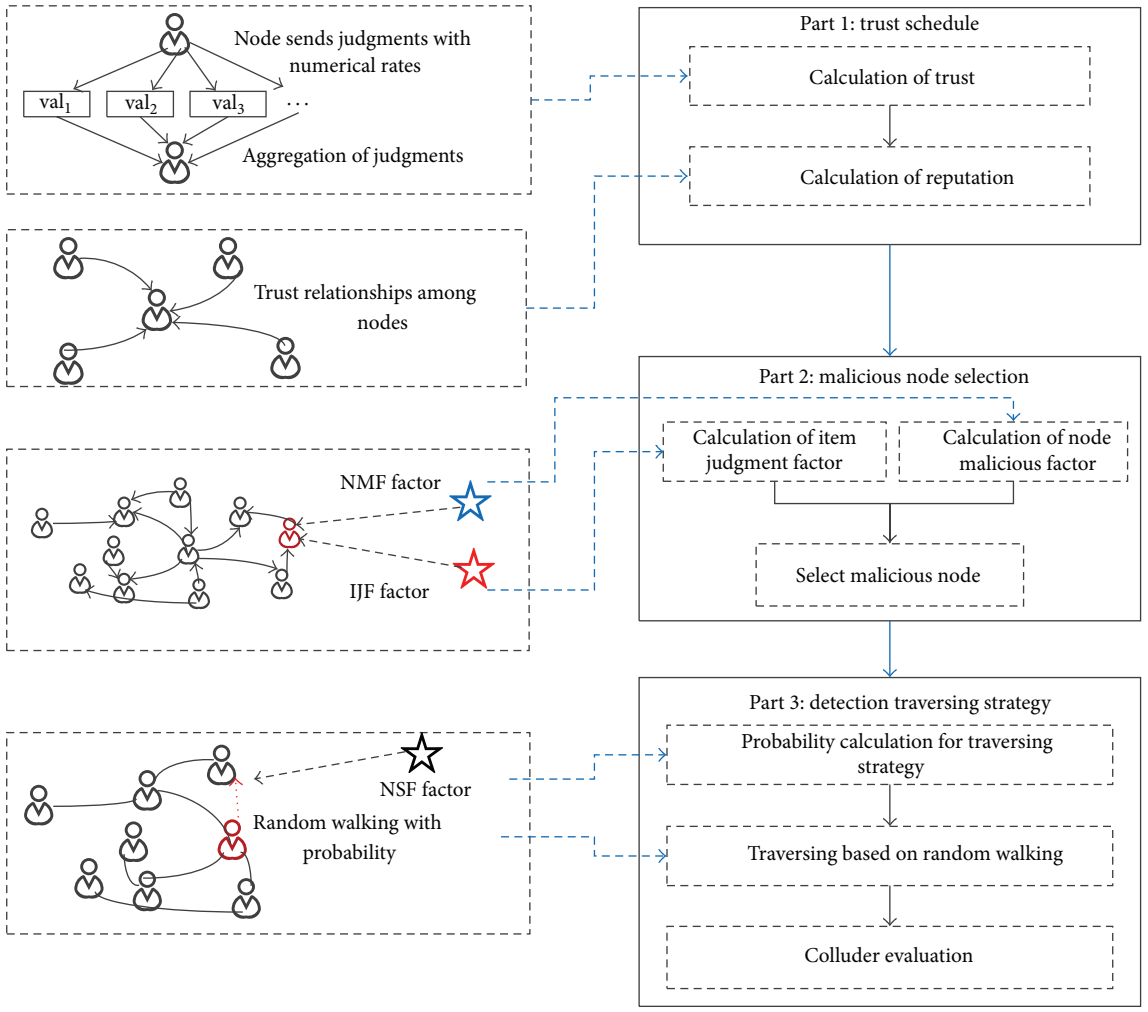

Figure 1: The framework of FCADM.

of nodes. As shown in Figure 1, a node can send judgments with numerical rates to another node and then aggregate trust relationship between nodes, while a node's reputation is aggregated according to other nodes' direct trust relationships (in blue dotted line with arrows pointing towards Part 1 in Figure 1). Trust schedule provides the trustworthiness information of nodes in mobile social networks, which enables FCADM to evaluate the malicious likelihood of a node being colluder and further offers traversing rules in node trust relationship network.

(2) Part 2: Malicious Node Selection. In FCADM, we give a set of malicious factors and related calculation methods for selecting a malicious colluder. As shown in Figure 1, two factors of item judgment factor (IJF) and node malicious factor (NMF) are evaluated for identifying the malicious degree of a node through fuzzy interval value (in blue dotted line with arrows pointing towards Part 2 in Figure 1). The factors are calculated based on node's behaviors and records. Then, the results of factor calculation are combined to select single malicious node. Therefore, we can make decision to recognize whether a node is malicious node or not and the recognized malicious node is seen as the source node for further colluder detection.

(3) Part 3: Detection Traversing Strategy. In this part, we give a traversing strategy in node trust relationship network based on random walking algorithm [32]. FCADM selects a recognized malicious node as the source node in mobile social networks (given according to the result of Part 2) and then traverses the whole network along the relationships among nodes (in red dotted line in Figure 1) according to the probabilities calculated by node similar factor and trust degree (in blue dotted line pointing towards Part 3 in Figure 1). Our main rational of proposed traversing strategy is that if a node has both higher degree of trust relationship and larger value of NSF factor with a malicious one, it would have more possibility of being colluder with the malicious one. Then, the traversing strategy can calculate the probability of selecting traversing objects according to trust relationships among nodes.

Moreover, we here give our assumption for our work here. In this work, we aim to detect malicious colluders by retrieving them through users' relationships. Then, the reasons of

our assumption are as follows: (1) a single malicious node is easy to detect because of its explicit malicious behaviors, while it is difficult to verify that several malicious nodes which are detected separately are colluders in collusion without taking their relationships into account and (2) of cause, some malicious nodes want to hide their relations and show less evident relationship in social network. On contrary, in our consideration, the collusive attacks must be organized based on mobile social networks more or less by colluders. Therefore, our work focuses on nonanonymous attack detection based on explicit evidences (e.g., witness behaviors and accessible data in social network), because if colluders communicate without any explicit evidence (e.g., through an offline method), it is definitely hard to find their relationships only depending on social network. It can be seen as anonymous collusive attacks and it is not included in this work.

Therefore, our work is based on the following assumptions regarding organized collusion:

(1) Malicious nodes always exhibit consistent behaviors during organized collusion. In particular, any node (honest node/colluder) will not change its identification and attitude (honest/malicious) while it appears in the mobile social networks, according to the theoretical analysis. In addition, all nodes will keep their certifications and they will not leave the network after they enter the mobile social networks and their investigation begins.

(2) There are major differences between the malicious ones and honest ones. Thus, malicious behaviors are very different from factual behaviors. That is, malicious evidences of colluders are accessible more or less in mobile social networks.

(3) Due to the necessity for communication and cooperation, there must be at least one social relationship between the organizing colluder and other colluders. Thus, colluders cannot attack collusively without possessing relationships in mobile social networks.

3.2. Related Definitions. First, we clarify the role of fuzzy view in our work. Commonly, the trust and reputation degrees are calculated based on past records or experiences from users. And also, we can see that trust or reputation is essentially a dynamic degree with the past records changing. Therefore, the uncertain nature of trust or reputation leads to unreasonable results if the degree is expressed as crisp numbers. Many efforts have been made to prove the fact that crisp numerical concepts are not sufficient for expressing the uncertainty of concepts [33]. For example, three nodes u_1, u_2, and u_3 are given such that u_1 has trust degrees to u_2 and u_3, respectively. In traditional method, the trust degrees are expressed as crisp numbers, and then, it is hard to measure whether the trust degree of u_1 to u_2 exceeds, equals, or is less than the trust degree of u_1 to u_3 if the two crisp numbers are approximate. That is because the trust degrees will keep updating timely with the changing of interaction data among users. Such uncertainty of trust relationship leads to unreasonable comparison by using crisp numbers. In fact, we can find that the value of trust degree between nodes is in an interval and such fuzzy interval reflects the reasonable measurement for user's uncertain trustworthy opinion to others. Similarly, the role of fuzzy applies to reputation aggregation and malicious factor evaluation as well, and the fuzzy interval expression is a reasonable method for our work.

Then, we address a set of related definitions for FCADM as follows.

Definition 1 (graph model of mobile social networks). Mobile social networks can be described as a directed graph w which is a two-tuple as $\mathrm{SG} = \langle U, E\rangle$, where $U = \{u_1, u_2, \ldots\}$ and $E = \{e_1, e_2, \ldots\}$ denote the sets of nodes and their relationships, respectively.

Definition 2 (trust schedule). Trust schedule of a node is described as $\mathrm{TS}(u_i) = \langle \mathrm{rep}(u_i), \mathrm{Trust}(u_i)\rangle$, where $\mathrm{rep}(u_i)$ is the reputation degree of node u_i and $\mathrm{Trust}(u_i)$ is the set of trust relationship values from u_i to nodes that have direct trust relationships with u_i.

From Definition 2, we can see that trust schedule records two kinds of trustworthiness information of each node, that is, reputation and trust relationship. To represent the fuzziness of trust, the value of $\mathrm{TS}(u_i)$ is described as an uncertain value. That is, we here use an interval fuzzy value to describe trust schedule information as $\mathrm{rep}(u_i) = (\mathrm{rep}(u_i)^-, \mathrm{rep}(u_i)^+)$, $\mathrm{Trust}(u_i) = (\mathrm{Trust}(u_i)^-, \mathrm{Trust}(u_i)^+)$, where $\mathrm{rep}(u_i)^-$ and $\mathrm{Trust}(u_i)^-$ are the minimum values of them in past time and $\mathrm{rep}(u_i)^+$ and $\mathrm{Trust}(u_i)^+$ are the maximum values of them in past. We also have $\mathrm{Trust}(u_i)^- = (\mathrm{Trust}(u_i, u_j)^-, \mathrm{Trust}(u_i, u_k)^-, \mathrm{Trust}(u_i, u_m)^-, \ldots)$ and $\mathrm{Trust}(u_i)^+ = (\mathrm{Trust}(u_i, u_j)^+, \mathrm{Trust}(u_i, u_k)^+, \mathrm{Trust}(u_i, u_m)^+, \ldots)$, where u_j, u_k, and u_m are the nodes that get direct trust relationships by u_i; namely, u_j is the out-degree node of u_i. Hence, $\mathrm{Trust}(u_i, u_j)^-$ is the minimum value of the trust from u_i to u_j, while $\mathrm{Trust}(u_i, u_j)^+$ is the maximum value of the trust relationship from u_i to u_j. In other words, we have $\mathrm{Trust}(u_i, u_j) = (\mathrm{Trust}(u_i, u_j)^-, \mathrm{Trust}(u_i, u_j)^+)$.

Additionally, we propose the factors for collusive attack evaluation in FCADM: malicious factor and item attack probabilities.

Definition 3 (malicious factor). Malicious factor evaluates a single node's malicious possibility through two aspects: items and nodes which are judged by it. Malicious factor comprises three factors, that is, item attack probability, item judgment factor, and node malicious factor, which are utilized to evaluate the likelihood of a single node's malicious attack.

(1) Item Attack Probability (IAP). This factor is to describe the probability of an item being attacked in its reputation aggregation. The factor IAP can be denoted as $\mathrm{IAP} = (\mathrm{IAP}^-, \mathrm{IAP}^+)$, and the item attack probability is in this range.

(2) Item Judgment Factor (IJF). Item judgment factor aims to evaluate the probability of malicious judgment occurrence given by a node's judgments to items. IJF can be denoted

as IJF $= (\mathrm{IJF}^{-}, \mathrm{IJF}^{+})$, which signifies that the probability of malicious judgment occurrence is in this range.

(3) Node Malicious Factor (NMF). Node malicious factor aims to evaluate the likelihood of a single node being a colluder. In this study, we consider that if a node sends more judgments which are far different with reputation of targets, the likelihood of the node being a colluder, measuring through NMF, would be larger.

With respect to malicious factor, item judgment factor is given to evaluate the difference between node's judgment and the obtained judgment of an item, while the item attack probability is to evaluate the likelihood of attack happening for an item. Meanwhile, NMF factor is given based on node's past rates through evaluating whether it often sends inconsistent judgments to others for their reputation aggregation.

Definition 4 (node similar factor (NSF)). Node similar factor is presented to describe the behavior similarity of nodes, which can be used to evaluate likelihood of node being colluder in collusive attack.

The factor NSF is proposed to improve the performance of traversing in colluder detection, concerning the fact that colluders in collusive attacks might have similar behaviors. In part of detection traversing strategy, we combine the trust relationship and NSF factor to get the node selection criterion for traversing strategy.

Details of proposed related definitions will be discussed with calculation methods and examples in later sections.

4. Calculation Method of Trust Schedule

In this section, we give the calculation method of trust schedule in FCADM, which includes two aspects as reputation and trust relationship.

(1) Trust Relationship Calculation. Firstly, we discuss the trust relationship and its calculation method. Trust relationship demonstrates one's subjective trustworthy willingness with respect to others, which can be measured based on a node's past experience or interaction. For instance, a node completes interactions and then is able to send judgment concerning its experience from interaction with other nodes. From this perspective, trust relationship is an aggregation concerning the historical feelings between nodes. In this work, we use a fuzzy interval value to represent the trust relationship between nodes. Assume that u_j gets direct trust relationship from u_i; $O(u_i)$ is the set of directly linked nodes from u_i and $|O(u_i)|$ denotes the total number of set $O(u_i)$; then $\mathrm{Trust}(u_i, u_j) \in [0, 1]$ can be calculated as follows:

$$\mathrm{Trust}\left(u_i, u_j\right)^{(t)} = \begin{cases} \widetilde{\mathrm{val}}\left(u_i, u_j\right), & \text{if } \left|\widetilde{\mathrm{val}}\left(u_i, u_j\right) - \overline{\mathrm{val}}\left(u_i\right)\right| \le \vartheta, \\ \widetilde{\mathrm{val}}\left(u_i, u_j\right) + \dfrac{\widetilde{\mathrm{val}}\left(u_i, u_j\right) - \overline{\mathrm{val}}\left(u_i\right)}{\sum_{u_k \in O(u_i)} \left|\widetilde{\mathrm{val}}\left(u_i, u_k\right) - \overline{\mathrm{val}}\left(u_i\right)\right|}, & \text{else}, \end{cases} \tag{1}$$

$$\vartheta = \sqrt{\frac{\sum_{u_j \in O(u_i)} \left[\widetilde{\mathrm{val}}\left(u_i, u_j\right) - \overline{\mathrm{val}}\left(u_i\right)\right]^2}{\left|O\left(u_i\right)\right|}},$$

where $\mathrm{Trust}(u_i, u_j)^{(t)}$ denotes the trust degree at time point t, $\widetilde{\mathrm{val}}(u_i, u_j)$ is the impartial average judgment value from u_i to u_j, and $\overline{\mathrm{val}}(u_i)$ is the average value from u_i to its all directly linked nodes. According to (1), we can see that if the difference between $\widetilde{\mathrm{val}}(u_i, u_j)$ and $\overline{\mathrm{val}}(u_i)$ is in a reasonable range ($\le \vartheta$), the value of $\mathrm{Trust}(u_i, u_j)$ is seen as reasonable; if such difference is out of the range, we give an adjusting mechanism for trust calculation as follows: if $\widetilde{\mathrm{val}}(u_i, u_j) < \overline{\mathrm{val}}(u_i)$, the greater difference of $\widetilde{\mathrm{val}}(u_i, u_j) - \overline{\mathrm{val}}(u_i)$ denotes that u_i does not trust u_j more; if $\widetilde{\mathrm{val}}(u_i, u_j) > \overline{\mathrm{val}}(u_i)$, the greater difference of $\widetilde{\mathrm{val}}(u_i, u_j) - \overline{\mathrm{val}}(u_i)$ denotes that u_i trusts u_j more. Then, we address the value calculation methods of $\widetilde{\mathrm{val}}(u_i, u_j)$ and $\overline{\mathrm{val}}(u_i)$ as follows.

Assume that $\mathrm{val}(u_i, u_j)_k \in [0, 1]$ is the kth judgment from u_i to u_j and $\mathrm{val}(u_i, u_j)_{\max}$ is the maximum value of judgment from u_i to u_j in the past, while $\mathrm{val}(u_i, u_j)_{\min}$ is the minimum value of judgment from u_i to u_j in the past. The calculations of $\widetilde{\mathrm{val}}(u_i, u_j)$ and $\overline{\mathrm{val}}(u_i)$ are as follows:

$$\widetilde{\mathrm{val}}\left(u_i, u_j\right) = \frac{\sum_{k=1}^{m} \mathrm{val}\left(u_i, u_j\right)_k - \mathrm{val}\left(u_i, u_j\right)_{\max} - \mathrm{val}\left(u_i, u_j\right)_{\min}}{m - 2}, \tag{2}$$

$$\overline{\mathrm{val}}\left(u_i\right) = \frac{\sum_{u_j \in O(u_i)} \widetilde{\mathrm{val}}\left(u_i, u_j\right)}{\left|O\left(u_i\right)\right|},$$

where $\mathrm{val}(u_i, u_j)_k$ denotes the kth judgment from u_i to u_j. Further, we assume that, at time point g, the value of $\mathrm{Trust}(u_i, u_j)$ is minimum and we denote $\mathrm{Trust}(u_i, u_j)^{-} = \mathrm{Trust}(u_i, u_j)^{(g)}$, while at time point h, the value of $\mathrm{Trust}(u_i, u_j)$

Table 2: The judgment value from u_1 to others.

val	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$
u_1, u_2	0.3	0.4	0.5	0.7	0.4	0.3
u_1, u_3	0.8	0.7	0.3	0.9	0.8	Null
u_1, u_6	0.3	0.2	0.1	0.3	Null	Null

Table 3: The trust value from u_1 to others.

Trust	t_1	t_2	t_3
u_1, u_2	0.3	0.35	0.7
u_1, u_3	0.2	0.3	0.1
u_1, u_6	0.4	0.5	0.6

$\text{Trust}(u_1, u_2) = (0.3, 0.7)$, $\text{Trust}(u_1, u_3) = (0.1, 0.3)$, and $\text{Trust}(u_1, u_6) = (0.4, 0.6)$.

is maximum and we denote $\text{Trust}(u_i, u_j)^+ = \text{Trust}(u_i, u_j)^{(h)}$. Then, the equation of trust degree can be as follows:

$$\begin{aligned}\text{Trust}\left(u_i, u_j\right) &= \left(\text{Trust}\left(u_i, u_j\right)^-, \text{Trust}\left(u_i, u_j\right)^+\right) \\ &= \left(\text{Trust}\left(u_i, u_j\right)^{(g)}, \text{Trust}\left(u_i, u_j\right)^{(h)}\right).\end{aligned} \tag{3}$$

Here, we give an example as follows: assume that the out-degree collection of u_1 is $O(u_1) = \{u_2, u_3, u_6\}$. At time t, we assume $\overline{\text{val}}(u_1) = 0.4$ and the judgment values from u_1 to u_2, u_3, u_6 are listed in Table 2.

Then, we can calculate $\text{Trust}(u_1, u_2)$ as follows:

$$\begin{aligned}&\widetilde{\text{val}}\left(u_1, u_2\right) \\ &\quad= \frac{0.3 + 0.4 + 0.5 + 0.7 + 0.4 + 0.3 - 0.3 - 0.7}{6 - 2} \\ &\quad= 0.4, \\ &\widetilde{\text{val}}\left(u_1, u_3\right) = 0.77, \\ &\widetilde{\text{val}}\left(u_1, u_6\right) = 0.43, \\ &\frac{\widetilde{\text{val}}\left(u_i, u_j\right) - \overline{\text{val}}\left(u_i\right)}{\sum_{u_k \in O(u_i)} \left|\widetilde{\text{val}}\left(u_i, u_k\right) - \overline{\text{val}}\left(u_i\right)\right|} \\ &\quad= \frac{0.4 - 0.43}{|0.4 - 0.43| + |0.77 - 0.43| + |0.17 - 0.43|} \\ &\quad= -0.05, \\ &\text{Trust}\left(u_1, u_2\right)^{(t)} = -0.05 + 0.4 = 0.35.\end{aligned} \tag{4}$$

Further, we list the trust values from node u_1 to others at different time points as shown in Table 3, we can therefore get the trust fuzzy interval values as in Table 3.

(2) Reputation Calculation. Reputation objectively denotes a shareable and authoritative trustworthy perspective from others that have direct interactions with it. In this work, the calculation of reputation is based on abovementioned trust relationship; that is, a node's reputation is an integrated view based on trust relationships from other directly linked nodes to it. The higher the trust relationship values from other nodes to a node are, the higher its reputation would be. Then, fuzzy interval valued reputation $\text{rep}(u_i)$ can be calculated as follows:

$$\begin{aligned}\text{rep}\left(u_i\right)^- &= \frac{\sum_{u_k \in I(u_i)} \text{Trust}\left(u_k, u_i\right)^-}{\left|I\left(u_i\right)\right|}, \\ \text{rep}\left(u_i\right)^+ &= \frac{\sum_{u_k \in I(u_i)} \text{Trust}\left(u_k, u_i\right)^+}{\left|I\left(u_i\right)\right|},\end{aligned} \tag{5}$$

where $I(u_i)$ is the node set which includes nodes directly linked to u_i. Then, we can get the fuzzy interval valued reputation as follows:

$$\text{rep}\left(u_i\right) = \left(\text{rep}\left(u_i\right)^-, \text{rep}\left(u_i\right)^+\right). \tag{6}$$

Here, we give an example as follows: we assume that the node set which includes nodes directly linked to u_1 is $I(u_1) = \{u_3, u_5\}$ and $\text{Trust}(u_3, u_1) = (0.2, 0.6)$, $\text{Trust}(u_5, u_1) = (0.4, 0.5)$. So, we can get reputation interval of $\text{rep}(u_1)^- = (0.2 + 0.4)/2 = 0.3$ and $\text{rep}(u_1)^+ = (0.6 + 0.5)/2 = 0.55$. Then, reputation of u_1 is as $\text{rep}(u_1) = (0.3, 0.55)$.

Since the reputation aggregation as listed in (5) and (6) is based on trust relationship calculation. Such aggregation mechanism will cause a vital problem that reputation is vulnerable if malicious ones establish inauthentic trust relationships to a node by sending malicious judgments to it. More seriously, collusive attacks from collaborative inauthentic judgments can do huge harm to reputation aggregation.

5. The Evaluation for Malicious Node Selection

In this section, we propose the evaluation method of selecting malicious nodes, which are verified to be malicious ones and further could be colluders in mobile social networks. Here, our criteria of evaluating colluders are as mentioned in Section 3, that is, malicious judgments dramatically different with honest rates and node malicious behaviors occurrence, which are calculated through two factors of IJF and NMF.

(1) Calculation of Item Attack Probability (IAP). In reputation systems, reputation of a node u_j is aggregated according to the collected judgments of all items which belong to u_j. Consequently, any attacks of item item_k belonging to node u_j would also damage the reputation aggregation of u_j. From this point, we use the factor of IAP to measure the likelihood of attack happening for items. That is, if a node's item $u_j.\text{item}_k$ received the average judgment value from other nodes with greater difference from reputation of node u_j, there would be more probability of item attack happening to item $u_j.\text{item}_k$. Therefore, we denote the given average judgment value of item $u_j.\text{item}_k$ as $\text{ave}(u_j.\text{item}_k)$. The factor of IAP can be calculated through the difference between $\text{ave}(u_j.\text{item}_k)$ and $\text{rep}(u_j)$. In addition, with respect to node's uncertain or occasional quality of item which might earn trustworthiness or distrust extremely, we introduce a smooth coefficient as

0.5. Then, the item attack probability can be calculated as follows:

$$\begin{aligned}
&\mathrm{IAP}\left(u_j.\mathrm{item}_k\right)^{-} \\
&\quad = \frac{\left|\mathrm{ave}\left(u_j.\mathrm{item}_k\right) - \mathrm{rep}\left(u_j\right)^{-}\right|}{\sum_{\mathrm{item}_l \in u_j}\left|\mathrm{ave}\left(u_j.\mathrm{item}_l\right) - \mathrm{rep}\left(u_j\right)^{-}\right|} \times 0.5, \\
&\mathrm{IAP}\left(u_j.\mathrm{item}_k\right)^{+} \\
&\quad = \frac{\left|\mathrm{ave}\left(u_j.\mathrm{item}_k\right) - \mathrm{rep}\left(u_i\right)^{+}\right|}{\sum_{\mathrm{item}_l \in u_j}\left|\mathrm{ave}\left(u_j.\mathrm{item}_l\right) - \mathrm{rep}\left(u_j\right)^{+}\right|} \times 0.5.
\end{aligned} \tag{7}$$

For instance, from Table 4 we get that $\mathrm{ave}(u_1.\mathrm{item}_1) = (0.3+0.4+0.3)/3 = 1/3$, $\mathrm{ave}(u_1.\mathrm{item}_2) = (0.6+0.7+0.8)/3 = 0.7$, and $\mathrm{ave}(u_1.\mathrm{item}_3) = (0.4+0.5+0.4+0.5)/4 = 0.45$. Based on above example, we have reputation of u_1 as $\mathrm{rep}(u_1) = (0.3, 0.55)$. Then, we can calculate IAP factor as follows:

$$\begin{aligned}
&\mathrm{IAP}\left(u_1.\mathrm{item}_1\right)^{-} \\
&\quad = \frac{|1/3 - 0.3|}{|1/3 - 0.3| + |0.7 - 0.3| + |0.45 - 0.3|} \times 0.5 \\
&\quad = 0.03, \\
&\mathrm{IAP}\left(u_1.\mathrm{item}_1\right)^{+} \\
&\quad = \frac{|1/3 - 0.55|}{|1/3 - 0.55| + |0.7 - 0.55| + |0.45 - 0.55|} \times 0.5 \\
&\quad = 0.23, \\
&\mathrm{IAP}\left(u_1.\mathrm{item}_2\right)^{-} \\
&\quad = \frac{|0.7 - 0.55|}{|1/3 - 0.55| + |0.7 - 0.55| + |0.45 - 0.55|} \times 0.5 \\
&\quad = 0.16, \\
&\mathrm{IAP}\left(u_1.\mathrm{item}_2\right)^{+} \\
&\quad = \frac{|0.7 - 0.3|}{|1/3 - 0.3| + |0.7 - 0.3| + |0.45 - 0.3|} \times 0.5 \\
&\quad = 0.34, \\
&\mathrm{IAP}\left(u_1.\mathrm{item}_3\right)^{-} \\
&\quad = \frac{|0.45 - 0.3|}{|1/3 - 0.3| + |0.7 - 0.3| + |0.45 - 0.3|} \times 0.5 \\
&\quad = 0.05, \\
&\mathrm{IAP}\left(u_1.\mathrm{item}_3\right)^{+} \\
&\quad = \frac{|0.45 - 0.55|}{|1/3 - 0.55| + |0.7 - 0.55| + |0.45 - 0.55|} \times 0.5 \\
&\quad = 0.11.
\end{aligned} \tag{8}$$

Table 4: The judgment values of items belonging to node u_1.

Item	$m = 1$	$m = 2$	$m = 3$	$m = 4$
item_1	0.3	0.4	0.3	Null
item_2	0.6	0.7	0.8	Null
item_3	0.4	0.5	0.4	0.5

(2) Calculation of Item Judgment Factor (IJF). Factor of IAP signifies the probability of a node attacking another node's item. As for factor of item judgment factor, it describes the possibility of a node attacking all the items that it sends judgment to. Let there be a set of items, noted as $\mathrm{Item}(u_i)$, which includes all the items judged by u_i. For $\mathrm{item}_k \in \mathrm{Item}(u_i)$, we denote that the overall average judgment value of the item_k is as $\overline{\mathrm{val}}(\mathrm{item}_k)$, and the mth judgment value from u_i to item_k is denoted as $\mathrm{val}(u_i, \mathrm{item}_k)_m$. Then, the item judgment factor of u_i can be calculated as follows:

$$\begin{aligned}
&\mathrm{IJF}\left(u_i, \mathrm{item}_k\right) \\
&\quad = \sqrt{\frac{\left(\sum_{m=1}^{n}\left[\mathrm{val}\left(u_i, \mathrm{item}_k\right)_m - \overline{\mathrm{val}}\left(\mathrm{item}_k\right)\right]^2\right)}{n}},
\end{aligned} \tag{9}$$

where n denotes the total number of judgments from u_i to item_k.

Further, we use the factor of IAP to improve the calculation of IJF. Our underlying meaning is that if an item has a high probability of being attacked (with high value of IAP of the item) and meanwhile a node has a large overall judgment difference of the same item (with a high value of IJF), the node would have high possibility of attacking the item as a malicious one. For a node u_i and its judged item set $\mathrm{Item}(u_i)$, the total item judgment factor of it can be calculated as follows:

$$\begin{aligned}
&\mathrm{IJF}\left(u_i\right)^{-} \\
&\quad = \frac{\sum_{\mathrm{item}_k \in \mathrm{Item}(u_i)}\left[\mathrm{IJF}\left(u_i.\mathrm{item}_k\right) \times \mathrm{IAP}\left(\mathrm{item}_k\right)^{-}\right]}{\sum_{\mathrm{item}_k \in \mathrm{Item}(u_i)} \mathrm{IJF}\left(u_i.\mathrm{item}_k\right)}, \\
&\mathrm{IJF}\left(u_i\right)^{+} \\
&\quad = \frac{\sum_{\mathrm{item}_k \in \mathrm{Item}(u_i)}\left[\mathrm{IJF}\left(u_i.\mathrm{item}_k\right) \times \mathrm{IAP}\left(\mathrm{item}_k\right)^{+}\right]}{\sum_{\mathrm{item}_k \in \mathrm{Item}(u_i)} \mathrm{IJF}\left(u_i.\mathrm{item}_k\right)}.
\end{aligned} \tag{10}$$

(3) Calculation of Node Malicious Factor (NMF). Factor of NMF is given based on node's rates to other nodes' reputation aggregation. In general, a significant variation between a malicious and an honest node's fraud is behavior. Thus, we can evaluate whether a single node is malicious or not by comparing its judgments with reputation values of the other nodes. For a node u_i, assume that it rates n times of reputation judgments to other nodes in past. And for each node u_j that received rates voting by u_i, it has reputation value of $\mathrm{rep}(u_j)$ and the kth judgment from u_i to u_j is denoted as

$\mathrm{val}(u_i, u_j)_k \in [0, 1]$. Then, the node malicious factor can be calculated as follows:

$$\mathrm{NMF}\left(u_i^{-}\right) = \sqrt{\frac{\sum_{u_j \in \mathrm{Vote}(u_i)} \sum_{k=1}^{n} \left[\left(\mathrm{val}\left(u_i, u_j\right)_k - \mathrm{rep}\left(u_j\right)^{-}\right)\right]^2}{n}},$$
$$\mathrm{NMF}\left(u_i^{+}\right) = \sqrt{\frac{\sum_{u_j \in \mathrm{Vote}(u_i)} \sum_{k=1}^{n} \left[\left(\mathrm{val}\left(u_i, u_j\right)_k - \mathrm{rep}\left(u_j\right)^{+}\right)\right]^2}{n}}, \tag{11}$$

where $\mathrm{Vote}(u_i)$ is the set of nodes that received judgments from u_i in the past for reputation aggregation. The lower the value of the NMF factor, the more honest the node.

(4) Selection of Malicious Nodes. Here, we set the interval of IJF factor as $\alpha = (\alpha^{-}, \alpha^{+})$, and the interval of NMF factor is $\beta = (\beta^{-}, \beta^{+})$. Therefore, for a node u_i, if both of its range overlap rates of α and β are greater than a given threshold, we define u_i as a malicious node. The range overlap rates are calculated as follows:

$$\mathrm{range}(\alpha) = \left|\mathrm{IJF}\left(u_i\right)^{+} - \alpha^{+}\right| - \left|\mathrm{IJF}\left(u_i\right)^{-} - \alpha^{-}\right|,$$
$$\mathrm{range}(\beta) = \left|\mathrm{NMF}\left(u_i\right)^{+} - \beta^{+}\right| - \left|\mathrm{NMF}\left(u_i\right)^{-} - \beta^{-}\right|. \tag{12}$$

By our empirical analysis, threshold of range overlap rates of α and β can be set as 0.3. And also, we will discuss the impacts of α and β setting in later examination section.

6. Traversing Strategy of Colluder Detection Based on Random Walk

6.1. Traversing Strategy of FCADM. In our traversing strategy of colluder detection in FCADM, we use the trust relationship as a factor for making decision of path detection in social graph model. Here, we first address the probability evaluation in traversing strategy for finding colluders by using trust relationships among nodes.

Firstly, we give a set of symbols in our traversing strategy in FCADM as follows:

(i) mau: the malicious node which is selected through method proposed in Section 5 and used as start point in traversing.

(ii) cur_u: the current node in each step of traversing.

(iii) next_u: the node selected for next traversing step from current node.

(iv) Neighbor(cur_u): the set of direct neighbors that have direct current node trust relationships from cur_u.

(v) COL(mau): the set of colluders that are selected from start point mau in traversing.

(vi) TRA(mau): the set of nodes that are traversed from mau in a single time of traversing.

We can select a malicious node mau from the set obtained by previous section. Starting from mau, we perform our traversing strategy through nodes' trust relationships with a probability of selecting the next node for traversing. Our proposed traversing strategy is based on *random walk* algorithm under a certain probability condition. At each step of traversing, we are at a current node cur_u and need to make decision of whether the traversing should keep going on and which node would be selected as the next one. If the node cur_u is evaluated to be another colluder, then we mark it as colluder of mau; if cur_u is an honest one, we skip it and continue our traversing until termination of traversing. For each cur_u, we have following options:

(1) With probability χ_{forward}, we continue our traversing and select next_u. We evaluate the probability of selected node to be a colluder.

(2) With probability $1 - \chi_{\mathrm{forward}}$, we do not continue the traversing strategy. That means that the current node is the end and we can restart another round of traversing.

(3) If the out-degree of node cur_u is 0, we need to backtrack our traversing to the previous node (noted as pre_u) and then restart the trust traversing according to option (1) or (2).

Next, we discuss the former two options, respectively, as follows.

(1) Firstly, we need to decide the probability of continuing traversing. We consider that the probability of χ_{forward} can be calculated based on number of neighbors set of current node and the shortest distance between the current node and start point node as follows:

$$\chi_{\mathrm{forward}} = \begin{cases} \left(1 - \dfrac{1}{\left|\mathrm{Neighbor}\left(\mathrm{cur}\_u\right)\right| + 1}\right)^{1 - 1/\mathrm{dis}(\mathrm{cur}\_u, \mathrm{mau})}, & \mathrm{cur}\_u \neq \mathrm{mau}, \\ 1, & \mathrm{cur}\_u = \mathrm{mau}, \end{cases} \tag{13}$$

where $\mathrm{dis}(\mathrm{cur}\_u, \mathrm{mau})$ is the shortest length from current node to start point node. Obviously, with more nodes in neighbor set and shorter length from current node to start point node, the probability of χ_{forward} would be larger.

Then, we need to decide the probability of the traversing and selecting the next node. That means that we need to select a directly trust related neighbor of current node cur_u under a certain probability. We have two rules for

defining the probability calculation here: trust relationship and node similar factor. That means that a higher valued trust relationship to neighbor and meanwhile a higher node similar factor imply a higher probability of being selected as the next traversing node. We denote next_u as the next node for selecting a node v from current node's direct trust related nodes. Then, the probability of selecting node v is as

$$p(v) = \frac{(1-\eta)}{|\text{Neighbor}(\text{cur\_}u)|} + \eta \frac{\overline{\text{Trust}}(\text{cur\_}u, v) \times \overline{\text{rep}}(v)}{\sum_{w \in \text{Neighbor}(\text{cur\_}u)} \overline{\text{Trust}}(\text{cur\_}u, w) \times \overline{\text{rep}}(w)}, \quad (14)$$

where $|\text{Neighbor}(\text{cur\_}u)|$ is the total number of $\text{Neighbor}(\text{cur\_}u)$, $\overline{\text{Trust}}(\text{cur\_}u, v)$ denotes the average value of interval fuzzy value $\text{Trust}(\text{cur\_}u, v) = (\text{Trust}(\text{cur\_}u, v)^-, \text{Trust}(\text{cur\_}u, v)^+)$, and $\overline{\text{rep}}(v)$ denotes the average value of $\text{rep}(v) = (\text{rep}(v)^-, \text{rep}(v)^+)$. In addition, we define a damping factor $\eta \in [0, 1]$ to denote the probability of randomly being selected as the next node for a node. That means that each node has a probability if it is the direct neighbor of current node. It can be used for selecting a new connected neighbor as the next node in traversing under a certain probability even if it has a relative low trust with current node.

In addition, since we aim to find a malicious colluder in our traversing, the node similarity is another essential factor for our strategy. Then, we here propose a factor τ(v) for evaluating the weight of node v with its node similar factor. In our study, factor $\tau(v)$ is calculated as

$$\tau(v) = \text{NSF}(\text{mau}, v) = \frac{1}{2} \times \left| \frac{\text{Vote}(\text{mau}) \cap \text{Vote}(v)}{\text{Vote}(\text{mau}) \cup \text{Vote}(v)} \right| + \frac{1}{2} \times \left| \frac{\text{Item}(\text{mau}) \cap \text{Item}(v)}{\text{Item}(\text{mau}) \cup \text{Item}(v)} \right|, \quad (15)$$

where Vote(mau) is the set of nodes that mau has voted to in the past; Item(mau) is the set of items which mau has sent judgments to in the past.

Correspondingly, we have the final probability of selecting next node as

$$p(\text{next\_}u = v) = p(v)\,\tau(v). \quad (16)$$

(2) With probability $1 - \chi_{\text{forward}}$, we stay at current node and then evaluate current node whether it would be a colluder. The idea is that we define an evaluation method of cur_u to recognize the colluder. We will discuss the details of the evaluation method later.

6.2. Evaluation of Colluder in Traversing Strategy. In each step of traversing strategy, we should evaluate whether the selected current node is a colluder of malicious node (start point) or not. Here, we propose an evaluation method for recognizing the colluder based on malicious factors and node's reputation. The evaluation method comprises the following steps.

Step 1. For each current node cur_u, we evaluate its malicious factors of IJF and NMF based on (3), (5), and (6) and then measure whether it is a malicious one as in Section 5.

Step 2. If cur_u is evaluated as a malicious one in Step 1, we calculate its reputation difference with average reputation value of selected colluders as follows:

$$\text{Diff}(\text{cur\_}u) = \frac{\left(\left(\text{rep}(\text{cur\_}u)^- + \text{rep}(\text{cur\_}u)^+\right)/2 - \overline{\text{rep}}\right)^2}{\sum_{u_k \in \text{COL(mau)}} \left(\left(\text{rep}(u_k)^- + \text{rep}(u_k)^+\right)/2 - \overline{\text{rep}}\right)^2}, \quad (17)$$

$$\overline{\text{rep}} = \frac{\sum_{u_k \in \text{COL(mau)}} \left(\text{rep}(u_k)^- + \text{rep}(u_k)^+\right)}{|\text{COL}(\text{mau})| \times 2}.$$

If we get $\text{Diff}(\text{cur\_}u) \geq \varepsilon$, $\varepsilon \in [0, 1]$, we exclude the current node from colluder set.

6.3. Termination of Traversing Strategy in FCADM. Under above traversing strategy, we can detect colluders by traversing along node trust relationships. Such traversing can be repeated iteratively for discovering all possible colluders with the selected start point (a malicious node). In each step, we have two possible alternatives as follows:

(1) Current node is a colluder, and then, we should definitely continue our traversing.

(2) Current node is an honest node, and we skip the node and continue our traversing. However, we consider that an honest node would have a relatively low probability of connecting to a malicious one.

Based on above consideration, we here propose a termination factor for a single time traversing to decide whether a traversing should be terminated or not. Firstly, if the current node is a colluder one, we consider that it would have high probability of connecting to another colluder, and then the termination factor should be low. By contrast, if the current node is an honest one, we should increase the termination factor. Therefore, the termination factor of traversing strategy can be calculated as follows:

$$\text{ter} = \begin{cases} 1, & \text{if } \text{cur\_}u = \text{mau or } \text{cur\_}u \in \text{COL}(\text{mau}), \\ 1 - \left[\prod_{u_i \in \text{TRA(mau)}} \left(\text{IJF}(u_i) \times \text{NMF}(u_i)\right) \right] & \text{else.} \end{cases} \quad (18)$$

Here, we define that the single traversing would be terminated if factor ter is larger than a threshold (set as 0.8 in this study). In addition, to prevent a long depth traversing, we set the max step of traversing in a single traversing strategy as $n = 6$ based on the idea of "*six degrees of separation,*" which is mentioned widely [32].

Moreover, we here address the termination of overall traversing strategy in FCADM. With the increasing times of traversing, we can obtain colluders with their trust malicious factors. Then, we can terminate the traversing if there is no new detected colluder in numerous times of traversing continuously. It is also noted that we set a minimum number of traversing thresholds as 100 for ensuring that the strategy is working well in cold start state. And meanwhile, if no colluder can be detected after a maximum number of traversing thresholds (set as 500 in this study) from starting point, we consider that there is no colluder with it.

7. Experiment and Analysis

Extensive simulation experiments have been conducted to evaluate the performance of our proposed FCADM in this section. We perform simulations using our prototype system. The simulation environment is as follows.

(1) Simulation Platform. To test the performance of our proposed method, we developed a prototype that can simulate the nodes and their interaction behaviors based on prototype configurations. In the prototype, nodes are controlled automatically by the system and interact with others according to certain set behaviors, such as propagating information, sending comments of items or nodes, forwarding posts, and approving posts.

(2) Dataset. In our experimental scenarios, the initial dataset was collected manually from mobile social based systems. Our data included about 1,560 IDs and more than 170,000 records (including posts, comments, and other behaviors). The collected nodes were inserted as initial nodes into the prototype with their real personal data. We then added about 900 additional nodes whose roles were set manually. There were two node roles in the prototype: honest node and malicious node. In the initial settings, all nodes with real data were seen as honest ones, while malicious nodes were set from the additional nodes. In our prototype, once a node was set as an honest node or a malicious one, it could not change its role. The reputation values for each ID were initially set according to a normal distribution with mean 0.7 and variance 0.1 in our prototype.

(3) Interaction Behavior of Node. Honest nodes executed no malicious behaviors toward others, while malicious nodes sent malicious comments to honest nodes and sent fake comments to malicious ones to inflate their reputations.

(4) Topology of Prototype. For the nodes collected from real data, there was a one-way direct link from one node towards another one if it had a relationship with the node, and all direct links were generated from the initial data set and were fixed and invariable in the prototype. The initial dataset was used to calculate the initial trust according to the reliability, and then a network topology was formed based on this real-world source. For our collected real nodes and their relations, the average out-degree of real nodes is around 6.8 and the in-degree is around 3.7. Therefore, we set that additional nodes are connected with an average out-degree 7 and an average in-degree 4.

Table 5: Parameter setting in examinations.

Parameter	Value
Real node number	1560
Additional node number	900
Average out-degree	7
Average initial trust of real nodes	[0.58–0.75]
Average initial reputation of real nodes	[0.6–0.8]

Detailed characteristics of simulation in the prototype are shown in Table 5.

7.1. Performance Evaluation of Trust Schedule Calculation. In this test, we aim to evaluate the performance of trust schedule calculation based on fuzzy interval valued perspective. Firstly, we compare the calculation methods of trust relationship proposed in this work. We set four groups for the performance comparison of trust relationship: average of trust aggregation (AG), EigenTrust method (ET), ultimate trust rating (UT), and the proposed trust based on fuzzy interval value in FCADM (FT). In the test, we conduct two tests with 20% and 30% malicious additional nodes with 10,000 times of interactions among nodes and then record the accuracies of trust relationship calculation. As shown in Figures 2(a) and 2(b), we can see that the accuracies of proposed method (FT) are higher than methods of AG and ET, while the method of UT gets the best performance in all methods. In our consideration, the reasons are as follows: (1) the ultimate trust method provides trust by its dynamic adjusting of factor by large computational costs, which results in the best performance due to all nodes maintaining trustworthy knowledge about others for detecting malicious interactions; (2) the proposed method in this work can reflect a fuzzy scale based on judgments, which results in a reasonable numerical interval including maximum and minimum values rather than a single value. Such interval valued trust gives higher accuracy than exact crisp numeric value in other methods; and (3) the effect of time dimension is taken into account in our proposed method, while it is not considered in the other two methods.

Then, we examine the performance of reputation proposed in FCADM. Similar with above test, we conduct two tests with 20% and 30% additional nodes with 10,000 times of interactions among nodes and then record the accuracies of reputation of nodes. For comparison, we set three groups for reputation calculation: EigenRep method (ER), average aggregation method for reputation (AR), and proposed reputation based on fuzzy interval valued reputation in FCADM (FR). As shown in Figures 3(a) and 3(b), our proposed

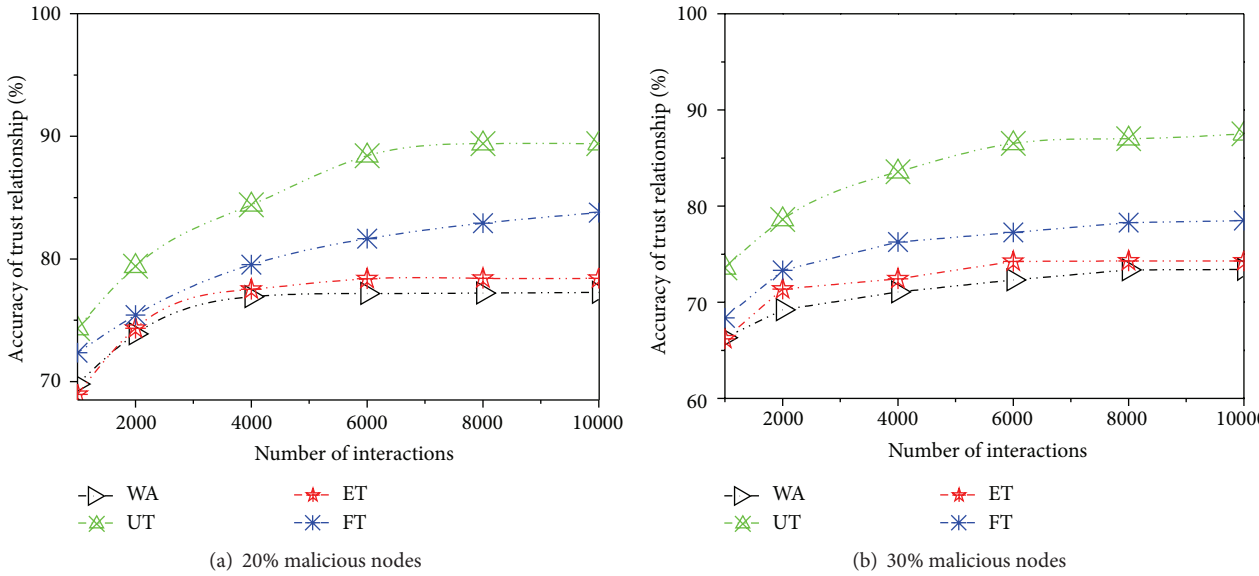

Figure 2: Performance of trust relationship comparison.

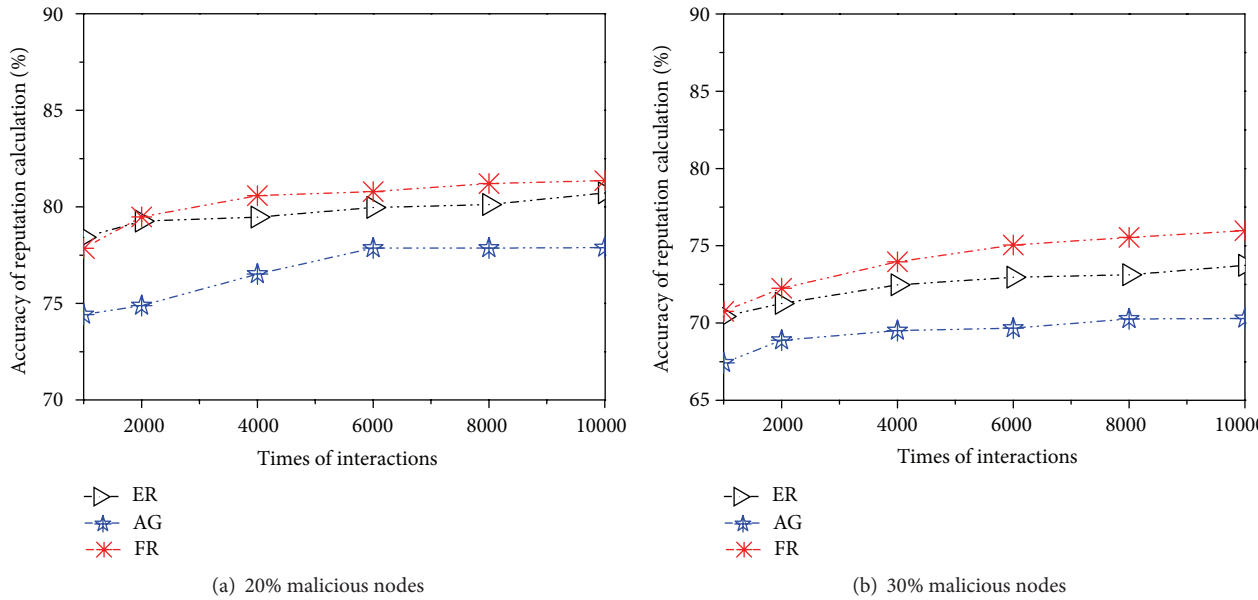

Figure 3: Performance of reputation comparison.

method gets a little better performance in all methods. In our analysis, the reasons are as follows: (1) the proposed method (FR) in this work can reflect a fuzzy scale based on reputation, which results in a reasonable numerical interval including maximum and minimum values rather than a single value. Similar with trust relationship, the interval valued reputation gives higher accuracy of meeting the requirement of accurate reputation aggregation than exact crisp numeric value in other methods; and (2) the consideration of time dimension also contributes to higher accuracies of reputation aggregation.

7.2. Performance Evaluation for Proposed Malicious Node Selection. In this examination, we firstly examine the impacts of the value setting for parameters α and β which are given to select malicious nodes. The parameters of α and β play important roles in the later selection of malicious nodes. For different combinations of α and β, the accuracies are different as shown in Figure 4(a). From the results, we can see that if the parameters are set as $\alpha = (0.55, 1.0)$ and $\beta = (0.6, 1.0)$, the performance of detecting malicious nodes is the best. Moreover, we conduct experiments to reveal the sensitivity of parameters of α and β. From Figures 4(b)-4(c),

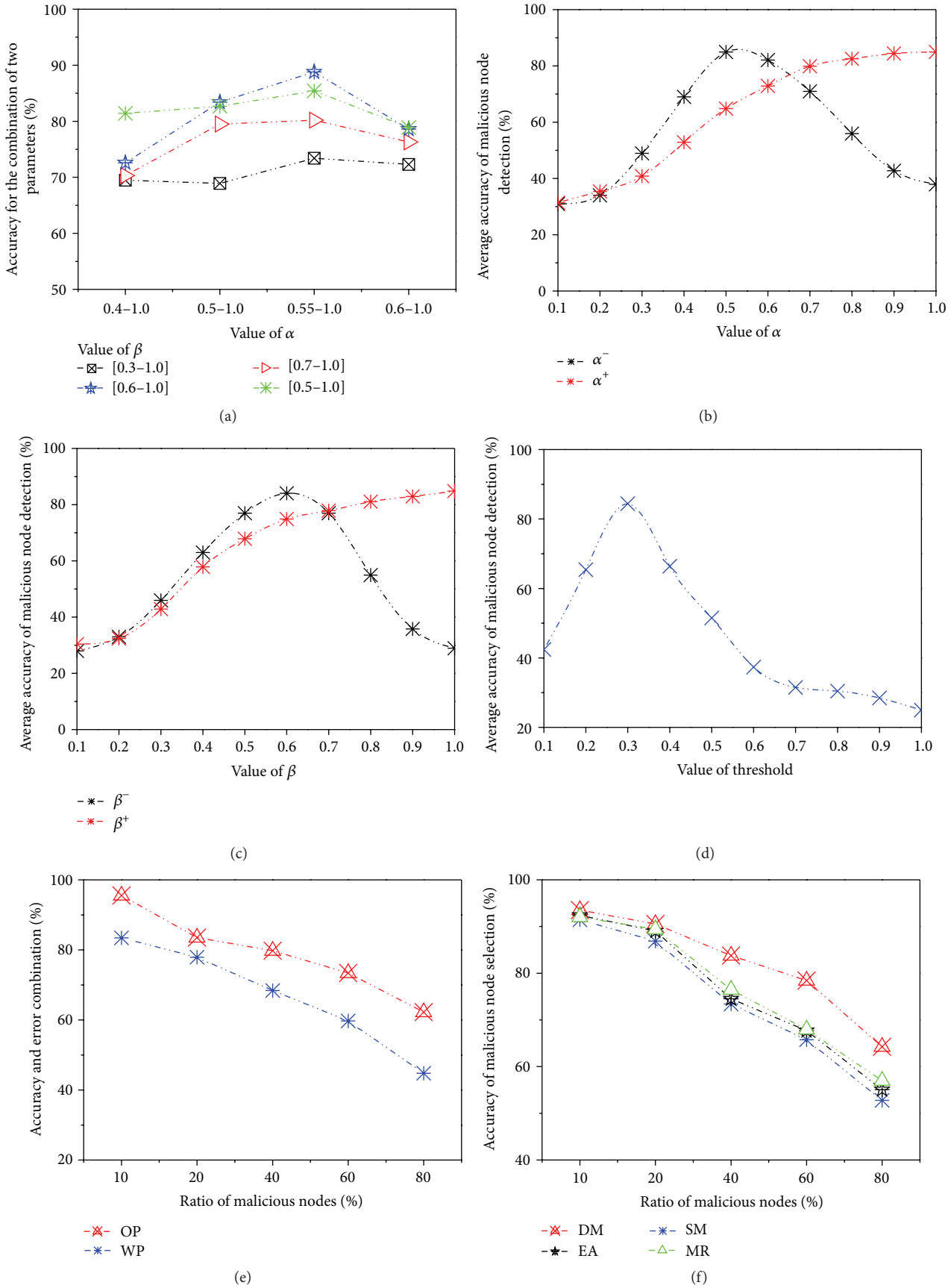

Figure 4: Performance evaluation for proposed malicious node selection.

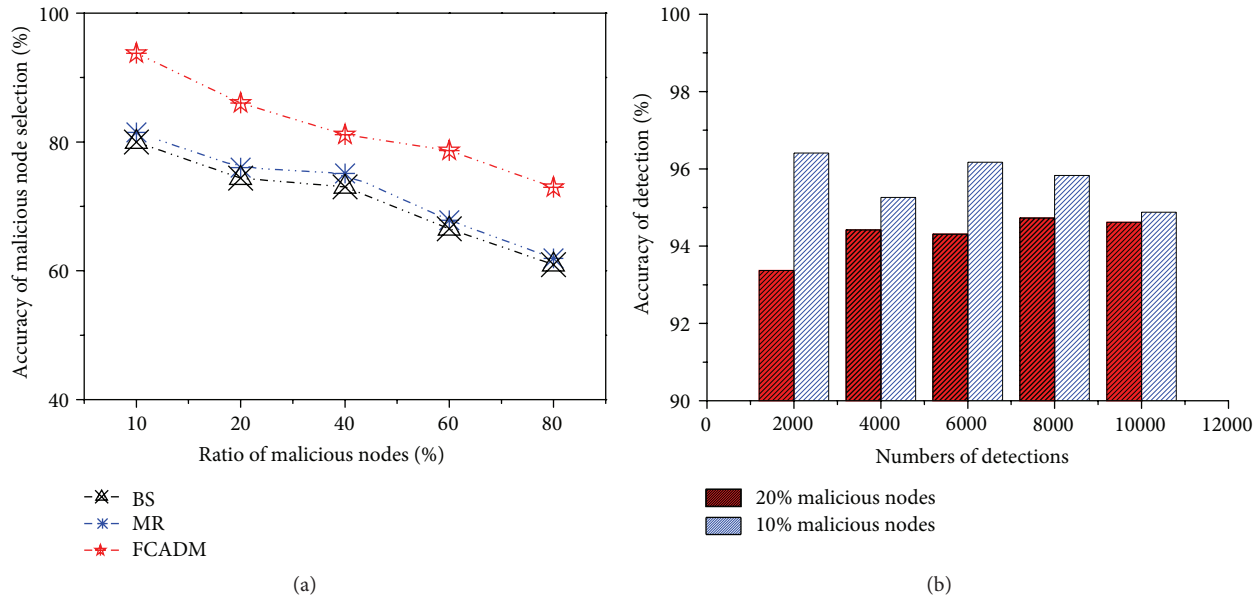

Figure 5: Comparison of different methods and scale.

we can see that the accuracies of detecting malicious nodes are changing, while the results are in agreement with the result in Figure 4(a). Further, we analyze the impact of threshold of range overlap rates of α and β in (12). As shown in Figure 4(d), the accuracy of malicious node detecting is lower while the value of threshold is set too low or too high. We consider that a too high value of threshold leads to malicious nodes being excluded in detection while a too low value of threshold leads to honest node being included in detection mistakenly. This test validates that the thresholds around 0.3 are often a reasonable compromise.

Then, we examine the performance of proposed malicious node selection based on (1), (2), (3), (5), (6), and (9) for selecting malicious nodes. The results are shown in Figures 4(e)-4(f). In Figure 4(e), we give the performance comparison under optimal value combination and the worst value combination of parameters α and β. By comparing the accuracies as shown in Figure 4(e), we can see that the performance difference between OP and WP has become larger with the ratio of malicious node increasing. That means that an appropriate value combination of parameters is a significant factor for malicious node selection.

Further, we compare performances of four methods as follows: our proposed method (DM), the majority rule (MR), the entropy-based approach (EA), and the signal modeling-based method (SM). We record the average accuracy of each method after 10,000 transactions. In this examination, we set parameters as $\alpha = (0.55, 1.0)$ and $\beta = (0.6, 1.0)$. As shown in Figure 4(f), we can see that, with the changing of ratio of malicious nodes in mobile social networks, the overall accuracies of all methods are decreasing. However, our proposed method has the best performance in all methods.

7.3. Performance Evaluation for Detection Traversing Strategy. In this examination, we verify the performance of our proposed detection traversing strategy for detecting collusive attack nodes. For comparison, we set three groups as follows: our proposed FCADM with majority rule (MR) and behavior similarity (BS). The results are shown in Figures 5(a)-5(b). As shown in Figure 5(a), we can see that the collusive attack nodes detection based on proposed FCADM has the best performance in all methods, with an approximately average improvement of 12.3% and 15.5%, respectively. Furthermore, we set that there are 20% or 10% malicious nodes in mobile social networks and then detect collusive attacks. We notice that, under different numbers of nodes in mobile social networks, the accuracies of collusive attack detection based on FCADM maintain stability as shown in Figure 5(b). The results show that FCADM is feasible and effective for detecting collusive attack in mobile social networks.

8. Conclusion

For users in mobile social networks, receiving judgments for establishing personal reputation by interacting with strangers is very common and inevitable. However, due to the lack of knowledge of the other ends they are dealing with and the magnitude of the network, most receivers might face potential risks because of the existence of malicious users. Preventing honest users from frauds, especially collusive attacks, for their reputation aggregation has its practical significance. First, our work provides a valuable guideline for constructing a collusive attack detection framework with fuzzy view. The monitoring systems in mobile social networks can be easily built according to our proposed framework and its related calculation methods. Meanwhile, the given formal definitions and conceptions in this work are quite appropriate for machines that read and understand the calculation methods so that a machine driven mechanism can achieve higher efficiency than manual methods to reduce

the workload of fuzzy intervals calculating and collusive attack detecting. Likewise, monitoring centers can inquire about details about attack detection, including information of nodes, reputation voting, and their reputations for the further purpose of fuzzy trust evaluation and malicious factor calculation. Secondly, application of the malicious factors helps monitoring centers to recognize many aspects as possible to get a more comprehensive evaluation about nodes. This is because the proposed IAP factor reflects whether an attack has happened, while IJP factor reflects whether a node has launched attacks. Further, UMF factor reveals whether a node is a malicious one in a comprehensive way. Thereby, our proposed method can provide sound usability for single malicious node discovering. Thirdly, the proposed traversing strategy helps to trace potential colluders connected to the recognized single malicious node according to the trust relationships among users. By traversing trustworthy relationships, we select nodes based on random walk algorithm in different probabilities corresponding to the trustworthy manners among people in real life; for example, a trustworthy node has more probability of being an associate. In fact, our proposed method can be used for reputation system monitoring and security enhancement in mobile social network based e-commerce platforms.

In our view, robustness and reliability are essential for reputation aggregation in mobile social networks. Therefore, our proposed study aims to detect collusive attacks by considering reputation from a fuzzy aspect based on node's relationship. In this study, we propose a collusive attack nodes detection mechanism (FCADM) in mobile social networks comprising the following aspects: (1) formal definitions for FCADM; (2) fuzzy trust schedule for trust relationship and reputation calculation; (3) selection method of malicious nodes based on proposed factors; and (4) traversing strategy for detecting collusive attack nodes based on random walk.

The results have justified the performances of our proposed scheme and have shown accuracy under our dataset. To conclude, the experimental results have been analyzed, showing that the results based on our proposed scheme are in line with the actual statement. The proposed FCADM can make objective judgment of nodes of collusive attacks, which can enhance the security of mobile social networks.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This work is funded by National Natural Science Foundation of China (61572326, 61103069, and 71171148), Key Lab of Information Network Security, Ministry of Public Security (C14602), and Program of Shanghai Normal University (DCL201302).

References

[1] S. P. Borgatti, D. J. Brass, and D. S. Halgin, "Social network research: Confusions, criticisms, and controversies," *Research in the Sociology of Organizations*, vol. 40, pp. 1–29, 2014.

[2] Z. Huang, S. Ruj, M. A. Cavenaghi, M. Stojmenovic, and A. Nayak, "A social network approach to trust management in VANETs," *Peer-to-Peer Networking and Applications*, vol. 7, no. 3, pp. 229–242, 2014.

[3] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems*, vol. 43, no. 2, pp. 618–644, 2007.

[4] S. D. Kamvar, M. Schlosser, and H. Garcia-Molina, "EigenRep: reputation management in peer-to-peer networks," in *Proceedings of the 12th International World Wide Web Conference (WWW '03)*, pp. 123–134, Budapest, Hungary, 2003.

[5] A. Kumar, S. K. Gupta, A. K. Rai, and S. Sinha, "Social networking sites and their security issues," *International Journal of Scientific and Research Publications*, vol. 3, no. 4, pp. 1–5, 2013.

[6] Y. Wang, S. Yao, J. Li, Z. Xia, H. Yan, and J. Xu, "ReSpam: a novel reputation based mechanism of defending against tag spam in social computing," in *Proceedings of the 8th IEEE International Symposium on Service Oriented System Engineering (SOSE '14)*, pp. 338–343, IEEE, Oxford, UK, April 2014.

[7] B.-H. Cha and S.-I. Choi, "Continuous media fingerprinting against time-varying collusion attacks," *Information Sciences*, vol. 298, pp. 66–79, 2015.

[8] M. G. Pérez, J. E. Tapiador, J. A. Clark, G. M. Pérez, and A. F. S. Gómez, "Trustworthy placements: improving quality and resilience in collaborative attack detection," *Computer Networks*, vol. 58, no. 1, pp. 70–86, 2014.

[9] C. S. Hyder, B. Grebur, L. Xiao, and M. Ellison, "ARC: adaptive reputation based clustering against spectrum sensing data falsification attacks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 8, pp. 1707–1719, 2014.

[10] G. Wang, F. Musau, S. Guo, and M. B. Abdullahi, "Neighbor similarity trust against Sybil attack in P2P E-commerce," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 3, pp. 824–833, 2015.

[11] E. Staab and T. Engel, "Collusion detection for grid computing," in *Proceedings of the 9th IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID '09)*, pp. 412–419, IEEE, Shanghai, China, May 2009.

[12] Y. Liu, Y. Yang, and Y. L. Sun, "Detection of collusion behaviors in online reputation systems," in *Proceedings of the 42nd Asilomar Conference on Signals, Systems and Computers (ASILOMAR '08)*, pp. 1368–1372, IEEE, Pacific Grove, Calif, USA, October 2008.

[13] J. Wu, F. Chiclana, and E. Herrera-Viedma, "Trust based consensus model for social network in an incomplete linguistic information context," *Applied Soft Computing Journal*, vol. 35, pp. 827–839, 2015.

[14] M.-R. Motallebi, F. Ishikawa, and S. Honiden, "Trust computation in web service compositions using Bayesian networks," in *Proceedings of the IEEE 19th International Conference on Web Services (ICWS '12)*, pp. 623–625, Honolulu, Hawaii, USA, June 2012.

[15] B. Qureshi, G. Min, and D. Kouvatsos, "A distributed reputation and trust management scheme for mobile peer-to-peer networks," *Computer Communications*, vol. 35, no. 5, pp. 608–618, 2012.

[16] F. G. Marmol, M. G. Perez, and G. M. Perez, "Reporting offensive content in social networks: toward a reputation-based assessment approach," *IEEE Internet Computing*, vol. 18, no. 2, pp. 32–40, 2014.

[17] K. Chen, H. Shen, K. Sapra, and G. Liu, "A social network based reputation system for cooperative P2P file sharing," *IEEE Transactions on Parallel & Distributed Systems*, vol. 26, no. 8, pp. 2140–2153, 2015.

[18] F. Hendrikx, K. Bubendorfer, and R. Chard, "Reputation systems: a survey and taxonomy," *Journal of Parallel & Distributed Computing*, vol. 75, pp. 184–197, 2015.

[19] A. A. Selçuk, E. Uzun, and M. R. Pariente, "A reputation-based trust management system for P2P networks," *International Journal of Network Security*, vol. 6, no. 3, pp. 235–245, 2008.

[20] F. J. Ortega, J. A. Troyano, F. L. Cruz, C. G. Vallejo, and F. Enríquez, "Propagation of trust and distrust for the detection of trolls in a social network," *Computer Networks*, vol. 56, no. 12, pp. 2884–2895, 2012.

[21] B. Qureshi, G. Min, and D. Kouvatsos, "Trusted information exchange in peer-to-peer mobile social networks," *Concurrency Computation Practice & Experience*, vol. 24, no. 17, pp. 2055–2068, 2012.

[22] B.-Z. He, C.-M. Chen, Y.-P. Su, and H.-M. Sun, "A defence scheme against Identity Theft Attack based on multiple social networks," *Expert Systems with Applications*, vol. 41, no. 5, pp. 2345–2352, 2014.

[23] S. Liu, J. Zhang, C. Miao, Y.-L. Theng, and A. C. Kot, "An integrated clustering-based approach to filtering unfair multinominal testimonies," *Computational Intelligence*, vol. 30, no. 2, pp. 316–341, 2014.

[24] J. Marshall, V. Thakur, and A. Yasinsac, "Identifying flaws in the secure routing protocol," in *Proceedings of the 22nd IEEE International Performance, Computing, and Communications Conference*, pp. 167–174, IEEE, April 2003.

[25] Y. Yang, Y. L. Sun, S. Kay, and Q. Yang, "Defending online reputation systems against collaborative unfair raters through signal modeling and trust," in *Proceedings of the ASM Symposium on Applied Computing (SAC '09)*, pp. 1308–1315, Honolulu, Hawaii, USA, March 2009.

[26] K. Thirunarayan, P. Anantharam, C. Henson, and A. Sheth, "Comparative trust management with applications: bayesian approaches emphasis," *Future Generation Computer Systems*, vol. 31, no. 1, pp. 182–199, 2014.

[27] F. Liu, L. Wang, L. Gao, H. Li, H. Zhao, and S. K. Men, "A web service trust evaluation model based on small-world networks," *Knowledge-Based Systems*, vol. 57, no. 2, pp. 161–167, 2014.

[28] J. S. Weng, C. Y. Miao, and A. Goh, "An entropy-based approach to protecting rating systems from unfair testimonies," *IEICE Transactions on Information & Systems*, vol. 89, no. 9, pp. 2502–2511, 2006.

[29] A. Rossi and S. Pierre, "Collusion-resistant reputation-based intrusion detection system for MANETs," *International Journal of Computer Science and Network Security*, vol. 9, no. 11, pp. 8–14, 2009.

[30] G. C. Silaghi, F. Araujo, L. M. Silva, P. Domingues, and A. E. Arenas, "Defeating colluding nodes in desktop grid computing platforms," *Journal of Grid Computing*, vol. 7, no. 4, pp. 555–573, 2009.

[31] B. Zhang, H. Yuan, F. Song, and H. Li, "A relationship based collusive attack detection mechanism for reputation aggregation in social network," in *Proceedings of the International Conference on Mechatronics, Electronic, Industrial and Control Engineering*, 2014.

[32] M. Jamali and M. Ester, "TrustWalker: a random walk model for combining trust-based and item-based recommendation," in *Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '09)*, pp. 397–406, ACM, July 2009.

[33] J. Wu and F. Chiclana, "A social network analysis trust–consensus based approach to group decision-making problems with interval-valued fuzzy reciprocal preference relations," *Knowledge-Based Systems*, vol. 59, pp. 97–107, 2014.