Hindawi
Complexity
Volume 2022, Article ID 5317738, 18 pages
https://doi.org/10.1155/2022/5317738

Research Article

Reputation Detection for Information Diffusion in Social Network Systems

Yifeng Zhou [1,2] **and Fang Yu** [3]

[1]*School of Information Engineering, Nanjing Audit University, Nanjing 211815, China*
[2]*School of Computer Science and Engineering, Southeast University, Nanjing 211189, China*
[3]*China Electric Power Research Institute, Nanjing 210003, China*

Correspondence should be addressed to Yifeng Zhou; yfzhouseu@gmail.com

Received 15 December 2021; Revised 30 March 2022; Accepted 14 May 2022; Published 7 July 2022

Academic Editor: Yu Zhou

Reputation detection in traditional distributed systems (e.g., electronic commerce systems and peer-to-peer systems) relies heavily on the factor of interaction reputation, which can be derived from direct interactions between agents through bidirectional relationships. However, in the current information diffusion in social network systems (SNS) (e.g., Twitter), the characteristic of the unidirectional relationship between agents and the decay property of diffusion will result in lacking direct interactions; therefore, interaction reputations will be difficult to be obtained by agents in a distributed manner. To solve this problem, a novel distributed reputation detection model following the pattern "*from path to individual*" (*FPTI*) is proposed, which can provide a new reputation factor as an alternative to interaction reputation in such environments. The main idea is that the positive (or negative) observation of an information diffusion process increases (or decreases) the belief of the corresponding diffusion path, which further increases (or decreases) the reputation of each involved agent. Thus, the reputation of a target agent can be assessed by the superimposition of reputations of multiple paths on which this agent has participated in past information diffusion processes. Furthermore, being aware of agent's limited capacity for reputation detection in SNS, we then propose the *enhanced FPTI model* (*eFPTI*), which simplifies the detection source to reduce detection costs and achieve the approximate performance as FPTI. Theoretical analyses and experimental evaluations validate the efficiency and effectiveness of our models and also show several properties of the models, for example, the robustness for dynamic environments.

1. Introduction

Social network systems (SNS) (e.g., Twitter [1, 2] and LinkedIn [3]) provide platforms for online information sharing. Due to the open nature of SNS, some malicious agents may be involved and engage in malicious behavior that will influence the performance of these systems [4–8]. An efficient way to address this problem makes use of the reputation mechanism, which can provide agents with credits for reference that help them make decisions about whom to trust and encourage agents to engage in trustworthy behavior [5, 7, 9–23].

Generally, the reputation of an agent (an agent in a social network system is an autonomous entity that can have interactions with other entities following some interaction rules; for example, an agent in Twitter can interaction with other agents following the rules defined by the Twitter client. It is worth noting that the agent in social network systems can be either a real user or a software bot) is often regarded as the assessment of the behaviors of this agent [15]. Some representative reputation models, for example, Regret (Regret is named by Sabater and Sierra representing "a reputation model for gregarious societies") [16] and FIRE (FIRE, which is from "fides" and "reputation," is named by Huynh et al.) [17], evaluate agents' reputations by integrating reputation factors from various sources, for example, direct interaction experiences, exchange of reputation information, and intrinsic features of agents. Among these

reputation factors, the *interaction reputation* of agents, which is based on direct interactions, is the most crucial because it not only reflects the trustworthiness of agents based on direct interaction experiences, but also can be treated as the basis for reputation information exchange (e.g., neighborhood reputation [16], witness reputation [17]). These reputation models can perform well in traditional distributed systems, for example, electronic commerce systems [13, 15] and P2P systems [24], in which agents have *direct interactions* through bidirectional relationships (the relationship between agents in SNS is the network connection, which is one necessary condition for the behavior transfer; a bidirectional relationship between a pair of agents allows bidirectional behavior transfer, which is often considered as the direct interactions).

However, due to the unidirectional relationship between agents [1, 25], for example, the follower-following topology of Twitter [1], and the decay property of diffusion [26] in the information diffusion scenarios in SNS, direct interactions between agents may be rare. This scarcity of direct interactions makes it difficult to determine the interaction reputations of agents. Traditional reputation models that rely heavily on interaction reputation, for example, Regret [16], FIRE [17], and P2PRep [24], may be of limited use in such environments. This situation will lead to inappropriate formation of trust between agents and may naturally result in the increase of malicious behaviors due to the absence of the effective supervision of agents' behaviors.

To address this problem, we propose a novel reputation detection idea to generate a new reputation factor as an alternative for interaction reputation: a positive observation of an information diffusion process increases the belief of the corresponding diffusion path (a path in this paper represents a queue of agents comprising the information diffusion pathway), which increases the reputation of each involved agent, and conversely, a negative observation decreases the belief of the corresponding diffusion path, which decreases the reputation of each involved agent. This method determines the reputations of agents by following the pattern "*from path to individual*" [27]: the reputation of an agent is evaluated by superimposing the reputations of multiple paths on which this agent participated in previous information diffusion processes. The key contributions of this paper are summarized as follows:

(i) This paper introduces the reputation detection problem considering the unidirectional relationship between agents in information diffusion scenarios in SNS and proposes the detection pattern "*from path to individual*" that employs the path reputation as the intermediate for reputation assessment of agents.

(ii) To detect path reputations in information diffusion processes, *feedback* and *feed-forward* approaches are proposed, which utilize *crossing situations* in information diffusion to check whether malicious behavior has occurred or not and then generate the path reputations.

(iii) To assess the reputations of individual agents from the obtained path reputations, an aggregation approach is proposed on the basis of evidence–belief transformation [28–32], and it especially considers the *suspicion probability* for agents in negative evidences of path reputations.

(iv) With the consideration of agents' limited capacity in SNS, a filtering method is presented, which can simplify the detection source to reduce the detection costs with reputation detection performance guarantee.

The remainder of this paper is organized as follows. In Section 2, we introduce some related research on reputation detection. In Section 3, we present the problem description and the novel reputation detection pattern. In Sections 4 and 5, we introduce the FPTI and eFPTI reputation detection models and conduct theoretical analyses, respectively. Then, in Section 6, we present experimental results that validate our models. Finally, we conclude our paper and discuss the future work in Section 7.

2. Related Work

The eBay model [18] and the Sporas model [19] are two typical reputation models in SNS. The reputation model on eBay [18] estimates the reputations of agents (buyer or seller) by the ratings provided by their partners after transactions. The rating can be −1 (negative rating), 0 (neural rating), or +1 (positive rating). The reputation of an agent (buyer or seller), which is the value of the sum of all the ratings on this agent, is provided on the transaction page attached to the users' screen names. It can indicate the reliability of a buyer or a seller in transactions and can be used as the reference for whether to trade or not. Similar with the eBay model, Sporas [19] also evaluates the reputation of an agent by aggregating the ratings about the agent from others. But by considering that agents may change their behavior patterns over time, which is ignored by the eBay model, Sporas assigned more weight to more recent ratings in the aggregation of reputation evaluation.

Using the eBay [18] and Sporas [19] models, the ratings for reputation evaluation provided by agents (which can be also considered as one kind of interaction reputation) can be generated based on the past experiences of direct interactions between the agents; thus bidirectional relationships between agents are required. Hence, if direct interaction is lacking because of unidirectional relationships between agents [1, 25] and the decay property of diffusion [26], it may be infeasible for reputation evaluation by using these models.

The eBay model [18] and the Sporas [19] model can be classified as single reputation models that assess agents' reputations by a single source. The single reputation model is designed for a specific application scenario and cannot make full use of various information sources in the system. Thus, with the proposal of the integrated reputation model, the single reputation models are often used as key components

to support the reputation aggregation. There are many representative reputation models, such as Regret [16], FIRE [17], FIRE+ (FIRE+ is an extension of FIRE model proposed by Qureshi et al., which can avoid collusion attacks) [20], DISARM (DISARM is a social, distributed, hybrid, rule-based reputation model named by Kravari and Bassiliades, which uses defeasible logic) [21], and AFRAS (AFRAS is from "a fuzzy reputation agent system" named by Carbo et al.) [22], can be classified as integrated reputation models that generate agents' reputations by integrating many reputation factors.

In the Regret model [16], which is implemented in transaction scenarios, the reputations of agents are computed from three dimensions: the individual dimension, the social dimension, and the ontological dimension. The individual dimension component of Regret presents the solution for obtaining the interaction reputation of agents, the social dimension component presents the solutions for producing the indirect reputation factors, and the ontological dimension component can combine different types of reputation factors into a new factor. The FIRE model [17] integrates four types of reputation factors that are derived from direct interaction experiences, witness information, role-based relationships, and certified information. It has been tested in provider and consumer games. The FIRE-+model [20] is devised to avoid collusion attacks that cannot be avoided by the Fire model; it also mainly focuses on the sources of direct and witness-based interaction experiences, but through a graph construction of witness ratings and various interaction policies (direct interaction policy, witness interaction policy, and connection decision policy), collusion among agents can be effectively detected. DISARM [21] introduces a distributed reputation system considering the relationships among agents as a network; DISARM proposes the use of defeasible logic combining the direct and witness information to support accurate reputation assessment. Wu et al. [23] introduce an artificial neural network-based reputation bootstrapping approach, which establishes the reputation of an agent by explicit evidences (direct interaction experiences) and implicit evidences (information that may be relevant with performance) in order to solve the reputation detection problem of newly deployed agents. The AFRAS model [22] introduces the fuzzy logic to represent the agent's reputation; the evaluation of the reputation value of an agent depends on not only the direct interactions, but also the recommendations from other agents of the society.

In these integrated reputation models, the interaction reputation derived from direct interactions can be the most important factor in reputation evaluation. It could be possible to produce some of the indirect reputation factors in these models (e.g., the social dimension reputation in Regret [16] and the witness and certified reputation in FIRE [17], FIRE+ [20], etc.) on the basis of the interaction reputation. However, the studies on these models did not consider the situation that direct interactions were lacking. This situation will not only cause a problem of infeasible interaction reputation generation, but may also make it impossible to determine some indirect reputation factors. In contrast, our models proposed in this paper provide solutions for solving this crucial problem.

3. Problem Description and Our Solutions

Diffusion is a common phenomenon in agents' collective behavior in SNS [33–40]. In previous studies, interaction reputations have often been generated from agents' observations and evaluations of other agents' behaviors [16, 18, 24]. In information diffusion processes (the spread of messages through agents in the network), the diffused *messages* can serve as the measure of the behaviors of agents. Moreover, in current SNS, for example, Twitter [1], messages spreading through agents (users) contain not only the message texts, but also the information of the spreading paths (e.g., the @ behavior in Twitter [1, 25]). This characteristic coincides with the characteristic of the diffusion process of chain letter messages [41]. In information diffusion process, there are two types of agent behaviors when diffusing messages: (a) *malicious behavior*: the agent tampers with the idea or content of some messages it received and diffuses them intentionally or unintentionally [42]; (b) *proper behavior*: the agent diffuses some messages it received with no tampering. To benefit the readers with a quick reference, the major notations of this paper are listed in Table 1.

3.1. Problem Description. Given a SNS, $N = <A, E>$, where A is the set of agents, $\forall <a_i, a_j> \in E$ indicates the existence of an edge directed from agent a_i to a_j. The distributed reputation detection problem in information diffusion scenarios can be described as follows:

$$M_i \longrightarrow \{r_i(j)\}, \tag{1}$$

where M_i represents the local message storage of agent a_i in the information diffusion process, and $r_i(j)$ represents the reputation of a_j produced by a_i. M_i consists of the messages sent by a_i and the messages a_i received from others. (Note that the messages sent by a_i include not only the messages wrote by a_i but also the messages a_i received from others and diffused by itself.)

Based on (1), the process of generating interaction reputations can be simply represented by the following (for brevity, messages with the same ID are labelled by their diffusion paths in the remainder of this paper.):

$$\left[m_{ij}, m_{iji}\right] \in M_i \longrightarrow r_i(j), \tag{2}$$

where m_{ij} indicates one message diffused from a_i to a_j and m_{iji} is the response of m_{ij} from a_j. By observing the response from a_j, a_i can evaluate or update the reputation of a_j.

However, $[m_{ij}, m_{iji}]$, which actually represents the direct interaction in information diffusion, must rely on a bidirectional relationship between a_i and a_j, i.e., $\exists <a_i, a_j>$, $<a_j, a_i> \in E$. Thus, due to the unidirectional relationship between agents in information diffusion, $[m_{ij}, m_{iji}]$ cannot be obtained. Moreover, even if a bidirectional relationship exists, because of the decay property of information diffusion, $[m_{ij}, m_{iji}]$ may also be missing due to the absence of m_{iji}.

Table 1: Major notations.

Notation	Description
A	The set of agents in the system
E	The set of edges in the system; $<a_i, a_j> \in E$ indicates the existence of an edge directed from agent a_i to a_j
$r_i(j)$	The reputation of a_j assessed by a_i
M_i	The local message storage of agent a_i
$m_{o\#i}$	The message with diffusion path $o\#i$, where o indicates the origin agent of this message, i indicates the agent a_i, and "#" represents the upstream path of a_i
$m_{o\#i^*i}$	The message with diffusion path $o\#i^*i$, where o indicates the origin agent of this message, i indicates the agent a_i at the crossing position, and "#" and "*" represent the upstream and downstream paths of a_i, respectively
PR	The path reputation PR = <path, (p, n)>, (p, n) is the corresponding evidence space
$\mathrm{PRF}_j^{\mathrm{PR}_k}$	The path reputation factor of PR_k for agent a_j
$\varepsilon_j^{PR_k}$	The suspicion probability of agent a_j for the negative evidence of PR_k

To solve this problem, a natural approach is to introduce some intermediates for producing the reputations of agents from the message storage. This approach is described as follows:

$$M_i \longrightarrow \{\text{Intermediates}\}_i \longrightarrow \{r_i(j)\}. \quad (3)$$

The intermediates introduced should meet the following requirements: (1) the intermediate can effectively reflect the agents' behaviors in information diffusion processes; and (2) the intermediate can be simply achieved by agents from their local message storage.

Then, the reputation detection problem in information diffusion scenarios in SNS can be divided into three subproblems:

(i) An appropriate intermediate should first be introduced.

(ii) Approaches for obtaining the intermediates should be proposed.

(iii) A mechanism for transforming the intermediates into the reputations of agents should be devised.

3.2. Our Solutions. To solve the above problems, we propose the reputation detection pattern "*from path to individual*." The main idea is that the reputations of agents can be detected according to the observations of their behaviors through the information diffusion paths; hence, the positive (or negative) observation of an information diffusion process increases (or decreases) the belief of the corresponding diffusion path, which further increases (or decreases) the reputation of each involved agent.

(i) To solve the first subproblem, we introduce the concept of *path reputation* (PR) as an intermediate for reputation detection that can meet the requirements for a detection intermediate. (1) Path reputations represent the evidence space for the information diffusion paths, which are past observations of the concatenations of agents' behaviors along the paths. For this reason, each path reputation can partially represent the behavior feature of each agent along the path. (2) Path reputations can be simply detected by agents from their local message storages using path reputation detection approaches described below.

(ii) To solve the second subproblem, *feedback* and *feed-forward* approaches (see Section 4.1) are proposed for path reputation detection. The central idea of these approaches is to find $\{[m]\}_i \subseteq M_i$ that can be used to produce path reputations. Here, $\{[m]\}_i$ represents the message subsets of M_i. The feedback and feed-forward approaches utilize the *crossing situations* in message spreading processes to find appropriate $\{[m]\}_i$, which can provide opportunities for checking whether malicious behaviors exist in the diffusion processes.

(iii) To solve the third subproblem, the *aggregation* approach (see Section 4.2) that can transform the path reputations into reputations of agents is devised. Negative evidence in path reputation can only partially reflect the disbelief of each involved agent because the evidence is the observation of the concatenation of agents' behaviors along the path; that is, the negative evidence may only be caused by the malicious behaviors of partially involved agents. Thus, in the transformation, the *suspicion probability* that can revise the weight of negative evidence for each agent involved is considered.

Figure 1 shows the reputation detection pattern of "*from path to individual*." The reputation detection can be operated synchronously with the operations of information diffusion. When some information diffusion actions result in an update of the local message storage of an agent, the agent can use the path reputation detection component (feedback and feed-forward) to update local path reputations and then update reputations of agents using the aggregation component. In Figure 1, the two dashed boxes represent the reputation detection process and the information diffusion process, respectively, and the arrow between them indicates their synchronous relationship.

4. Reputation Detection Model: *From Path to Individual* (FPTI)

4.1. Path Reputation Detection. Path reputation is composed of two essential parts: (1) the path information, which indicates the track of message spreading from one agent to another (which is actually created based on the information diffusion pathway), and (2) the evidence space, which

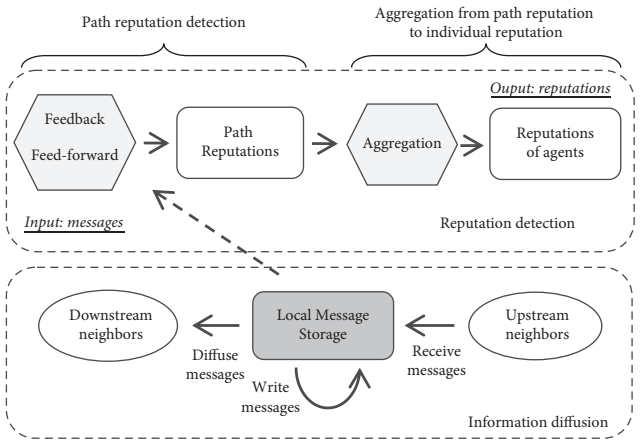

Figure 1: Reputation detection pattern "from path to individual."

contains both positive and negative evidences for the observations of information diffusion along the path. (Positive evidence is derived from the positive observation, which indicates that it is observed that no malicious behavior has been involved during the information diffusion process, and vice versa.) The path reputation is defined as follows:

$$\mathrm{PR} = \langle \mathrm{path}, (p, n) \rangle, \tag{4}$$

where path indicates the path information, and (p, n) is the corresponding evidence space, defined by the number of pieces of positive evidence (p) and negative evidence (n).

For the malicious behavior of tampering in information diffusion, we find that the key factor in detecting the path reputation is to find an appropriate subset of messages to check the correctness of messages that can further generate evidences for their information diffusion paths. In this paper, we utilize the subset of messages whose diffusion paths form a crossing situation, because some messages in such a subset can be treated as a standard for checking the correctness of the other messages. Based on the checking results, the path reputations of their diffusion paths can be generated. For this reason, the messages to be compared in a given subset should have the same ID.

In summary, two types of crossing situations in information diffusion can be utilized:

(1) The *feedback* cross, which is created by a single diffusion path that forms a loop (Figure 2). The corresponding message subset is represented by $[m_{o\#i}, m_{o\#i^*i}]$, where o indicates the origin agent of this message, i indicates the agent a_i at the crossing position, and # and * represent the upstream and downstream paths of a_i, respectively.

(2) The *feed-forward* cross, which is created by multiple diffusion paths joining up (Figure 3). The corresponding message subset is represented by $[m_{o\#i}, m_{o\#'i}, \ldots, m_{o\#''i}]$, in which the messages all have the same ID but have different diffusion paths.

The feedback and feed-forward detection approaches are described in the following sections, with an emphasis on how to provide the checking standard for the feedback and feed-forward crosses.

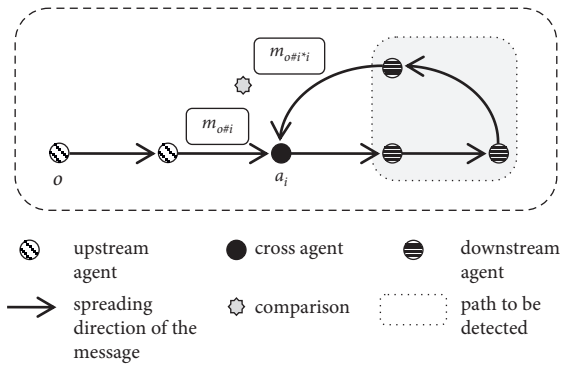

Figure 2: Example for feedback path reputation detection.

4.1.1. Feedback Detection. The feedback detection approach utilizes the feedback crossing situation to generate path reputations. Figure 2 gives an example of a feedback cross. A feedback cross is formed by a single diffusion path of a message having being diffused to cross agent a_i at some time in the past ($m_{o\#i}$) and diffused to a_i again after several diffusion steps ($m_{o\#i^*i}$). The message $m_{o\#i}$ is a previous copy of $m_{o\#i^*i}$; thus, it is used as the standard to check the relative correctness of $m_{o\#i^*i}$, that is, to check whether this message has been tampered with or not along the downstream path after $m_{o\#i}$.

In feedback detection, agents first seek feedback message subsets in their local message storages; then, they check the correctness of the message texts in each message subset; and finally, they generate path reputations of the *downstream paths* based on the checking results.

Figure 2 is an example for feedback detection. To find the feedback message subset, the agents need to find the message whose diffusion path already contains itself twice in its local message storage, i.e., $\exists m_{o\#i^*i} \in M_i$. If $m_{o\#i^*i}$ can be found, the previous version of message $m_{o\#i^*i}$ must also be contained in M_i, i.e., $\exists m_{o\#i} \in M_i$ (See Figure 2). Thus, the feedback message subset $[m_{o\#i}, m_{o\#i^*i}]$ is built. By comparing the texts of the two messages $m_{o\#i}$ and $m_{o\#i^*i}$, evidence for the downstream path "*" can be generated. If there is no difference, a piece of positive evidence is added to the downstream path, i.e., $p = p + 1$, and the number of pieces of negative evidence, n, remains unchanged; otherwise, a piece of negative evidence should be added, i.e., $n = n + 1$, and the number of pieces of positive evidence, p, remains unchanged.

4.1.2. Feed-Forward Detection. The feed-forward detection approach can generate path reputations by utilizing feed-forward crossing situations. A feed-forward crossing situation is formed by multiple diffusion paths joining up. The corresponding messages have the same ID but different diffusion paths.

Thus, the feed-forward message subset is represented by $[m_{o\#i}, m_{o\#'i}, \ldots, m_{o\#''i}]$. To simplify the analysis, the feed-forward message subset is divided into paired messages. For instance, the feed-forward message subset $[m_{o\#i}, m_{o\#'i}, m_{o\#''i}]$ can be divided into $[m_{o\#i}, m_{o\#'i}]$, $[m_{o\#'i}, m_{o\#''i}]$, and $[m_{o\#i},$

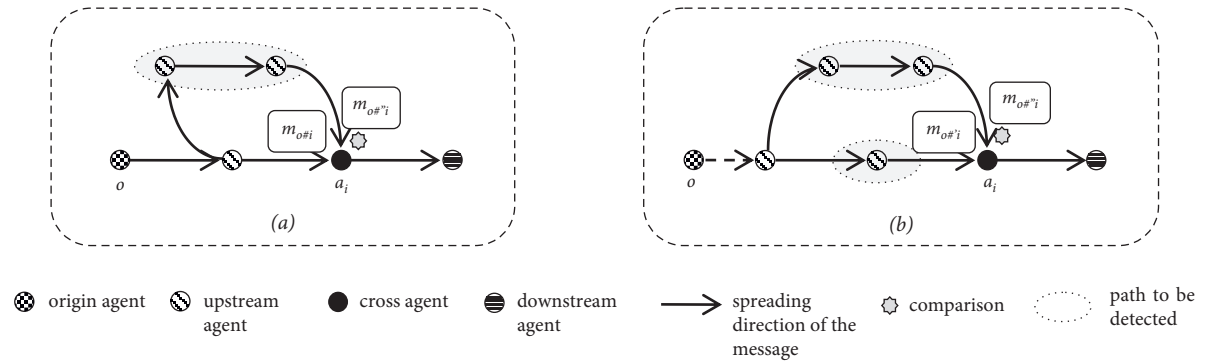

Figure 3: Example for feed-forward path reputation detection.

$m_{o\#''i}$]. Based on the different path relationships, the feed-forward detection approach is studied for two types of paired messages:

(i) The entire diffusion path of one message overlaps with part of the path of another message, as shown in Figure 3(a);

(ii) The diffusion paths of the two messages both have a nonoverlapped part with each other, as shown in Figure 3(b);

Crossing situation (a) can be used to produce the path reputation of the nonoverlapped part of the longer diffusion path. This use is reliable within feed-forward detection because the message with the shorter diffusion path can be treated as the local standard for comparison to check the relative correctness of the other message. Figure 3(a) is an example for crossing situation (a). If there is no difference between the texts of the two messages $m_{o\#i}$ and $m_{o\#''i}$, a piece of positive evidence is added to the path to be detected, i.e., $p = p + 1$, and the number of pieces of negative evidence, n, remains unchanged; otherwise, a piece of negative evidence should be added, i.e., $n = n + 1$, and the number of pieces of positive evidence, p, remains unchanged.

Crossing situation (b) can produce the path reputations of the nonoverlapped part of the message diffusion paths under the condition that the two messages have the same texts. Here, we assume that if a message has been tampered with by different agents, the texts will not be the same; that is, collusion between agents is not considered in this paper. Thus, if the two messages have the same texts, it is presumed that neither message has been tampered with through the nonoverlapping part of the diffusion paths. However, if the texts are different, the crossing situation (b) cannot take effect. Figure 3(b) is an example for crossing situation (b). If there is no difference between the texts of the two messages $m_{o\#'i}$ and $m_{o\#''i}$, a piece of positive evidence is added to each path to be detected, i.e., $p = p + 1$, and the number of pieces of negative evidence, n, remains unchanged; otherwise, the numbers of pieces of positive evidence and negative evidence, p and n, both remain unchanged.

The procedures for executing feed-forward detection are similar to those for feedback detection. For brevity, the procedures are not presented here. Unlike feedback detection, feed-forward detection can detect the *upstream paths* of cross agents.

4.2. Aggregation from Path Reputation to Individual Reputation. After path reputation detections are executed, agents need to transform the path reputations obtained into individual reputations of agents. First, the belief of the path reputation for each agent involved should be calculated. Then, the reputation of a target agent can be evaluated by superimposing the belief values of the multiple paths on which this agent has participated in past information diffusion processes.

4.2.1. Path Reputation Factor Calculation. The path reputation factor (PRF) can be used to reflect the belief of path reputation for each agent involved. Below, agent a_j is considered as the target agent for demonstration purposes.

The main idea in calculating the path reputation factor is to transform the evidence space of the path reputation into a belief value. In each PR, if the positive and negative evidences are treated equally in the transformation, the belief of this PR for each agent will be underestimated, because the negative evidence may be not caused by the action of a_j but rather by other agents within the path. For this reason, the *suspicion probability* of negative evidence for a_j needs to be taken into account. Therefore, the path reputation factor is defined as follows, based on the framework of evidence–belief transformation [28–32].

Let PR_k^p and PR_k^n denote the number of pieces of positive and negative evidence of PR_k, respectively. The path reputation factor of PR_k can be defined as follows:

$$\mathrm{PRF}_j^{\mathrm{PR}_k} = \frac{\mathrm{PR}_k^p + \left(1 - \varepsilon_j^{\mathrm{PR}_k}\right)\mathrm{PR}_k^n}{\mathrm{PR}_k^p + \mathrm{PR}_k^n + 1}, \tag{5}$$

where $\varepsilon_j^{\mathrm{PR}_k}$ denotes the suspicion probability of agent a_i for the negative evidence of PR_k. Thus, $(1 - \varepsilon_j^{\mathrm{PR}_k})\mathrm{PR}_k^n$ denotes the partial belief based on the negative evidences.

In our model, the detection process is executed independently by each agent, none of whom can know the behavior of others (i.e., whether other agents behave properly or maliciously). Thus, the probabilities of other agents behaving maliciously are considered to be 0.5 to reflect neutral opinions. Thus, we have the following:

Theorem 1. *The suspicion probability of each agent for negative evidence is*

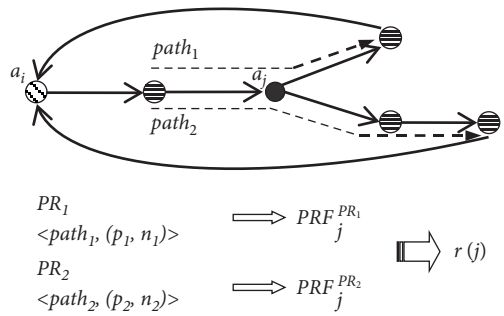

Figure 4: Example for aggregation from path reputations to individual reputations of agents. (The aggregation is taken by agent a_i; and a_j is the target agent).

$$\varepsilon_j^{PR_k} = \frac{\sum_{x=0}^{l-1} C_{l-1}^x}{\sum_{x=1}^{l} C_l^x}, \tag{6}$$

where l is the length (number of agents) along the path of PR_k ($l \geq 1$) and C_l^x indicates the combination in discrete mathematics, which means the number of subsets including x elements from a set of l distinct items.

Proof of Theorem 1. From the perspective of discrete mathematics, the suspicion probability for a_j for each instance of negative evidence should be equal to the ratio of the quantity of combination q that a_j may behave maliciously, no matter how others behave, to the quantity of all possible combinations q'.

$$\begin{aligned} q &= C_{l-1}^0 + C_{l-1}^1 + \cdots + C_{l-1}^{l-1} = \sum_{x=0}^{l-1} C_{l-1}^x, \\ q' &= C_l^1 + C_l^2 + \cdots + C_l^l = \sum_{x=1}^{l} C_l^x. \end{aligned} \tag{7}$$

Therefore, the suspicion probability is represented by the ratio q/q', i.e., $\sum_{x=0}^{l-1} C_{l-1}^x / \sum_{x=1}^{l} C_l^x$ □

From (6), it is observed that the suspicion probability is negatively correlated to the length of the path. If the length is shorter, the suspicion probability of negative evidence for each agent will be higher. According to (6), the suspicion probability for an agent ranges from 0.5 to 1.0. If the length of the path of PR_k is 1, the suspicion probability should have the maximum value of 1.0, and if the length of the path is infinite, the suspicion probability should have the minimum value of 0.5. □

4.2.2. Reputation Aggregation. The idea for the aggregation to evaluate the reputation of the target agent is to consider the superposition of its related path reputation factors (Figure 4). However, the extent of each path reputation factor to be referred to should be different because of their different amounts of evidence.

For this reason, we also investigate the weight of the PRF by considering that the more evidence the PRF is based on, the more dependable it should be. Thus, more evidence will lead to a higher weight value of a PRF. Based on Jøsang's uncertainty proposition in [28, 29], we can define the weight of the PRF of PR_k as follows:

$$w\_PRF_j^{PR_k} = 1 - \frac{1}{PR_k^p + PR_k^n + 1} = \frac{PR_k^p + PR_k^n}{PR_k^p + PR_k^n + 1}. \tag{8}$$

By considering the weight of each PRF, the reputation of a_j is equal to the weighted mean value of all its related path reputation factors. The larger the weight of a PRF is, the more reliable it is for aggregation purposes. Thus, the reputation of a_j as calculated by a_i is as follows:

$$r_i(j) = \frac{\sum_{\forall PR_k \in PR[j]} PRF_j^{PR_k} \times w\_PRF_j^{PR_k}}{\sum_{\forall PR_k \in PR[j]} w\_PRF_j^{PR_k}}, \tag{9}$$

where PR $[j]$ is the set of all relevant path reputations of a_j. PR $[j]$ belongs to PR_i, which is the set of path reputations produced by a_i.

4.3. Analyses of the FPTI Model

4.3.1. Detection Accuracy. The expected reputation of agent, $r_i(j)$, is computed by aggregating all the related path reputation factors. According to (9), we have the following:

$$\Delta_j \leq \max_{1 \leq x \leq |PR[j]|} e_{pa}^x, \tag{10}$$

where Δ_j is the reputation detection error of a_j and e_{pa}^x is the detection error (difference) between the path reputation factors PRF_j and the actual reputation factor AR_j. (Here, the actual reputation factor means the belief of the agent calculated by its real behavior history for each path reputation.) For this reason, we analyze the detection error e_{pa} between each PRF_j and AR_j below.

We set $AR_j = bp_j/(bp_j + bn_j + 1)$ to be the actual reputation factor of a_j here (which is proposed by Jøsang [28] to represent the belief value of an agent), where bp_j and bn_j represent the real number of past proper and malicious behaviors, respectively, of a_j in PRF_j. The total number of pieces of evidence in the path reputation factor PRF_j equals $(bp_j + bn_j)$, i.e., $PR^p + PR^n = bp_j + bn_j$. Note that $PR^p \geq 0$, $PR^n \geq 0$, $bp_j \geq 0$, and $bn_j \geq 0$.

Theorem 2. *The detection error between the path reputation factor and the actual reputation factor of a_j is as follows:*

$$e_{pa} = \left| \left(1 - \varepsilon_j\right) - \frac{\left(1 - \varepsilon_j \left(\prod_{a_k \in A_{pa} - a_j} \omega_k \right)\right) bp_j - \left(1 - \varepsilon_j\right)}{bp_j + bn_j + 1} \right|, \tag{11}$$

where A_{pa} represents the set of agents comprising the path of PRF_j, ω_k is the probability of other involved agent a_k behaving properly within PRF_j, $0 \leq \omega_k \leq 1$, and bp_j and bn_j represent the real number of past proper and malicious behaviors, respectively, of a_j in PRF_j.

Proof of Theorem 2.

$$e_{pa} = \left|\mathrm{PRF}_j - \mathrm{AR}_j\right| = \left|\frac{\mathrm{PR}^p + \left(1-\varepsilon_j\right)\mathrm{PR}^n}{\mathrm{PR}^p + \mathrm{PR}^n + 1} - \frac{bp_j}{bp_j + bn_j + 1}\right|. \tag{12}$$

All the proper behaviors of agents within the path can generate one instance of positive evidence, while one or more agents behaving maliciously will generate one instance of negative evidence. Suppose that the probability of other involved agents a_k behaving properly is ω_k $(0 \le \omega_k \le 1)$. We then have the following:

$$\begin{aligned} &\mathrm{PR}^p + \mathrm{PR}^n = bp_j + bn_j = \Omega, \\ &\mathrm{PR}^p = bp_j\left(\prod_{a_k \in A_{pa} - a_j} \omega_k\right), \\ &\mathrm{PR}^n = bp_j + bn_j - bp_j\left(\prod_{a_k \in A_{pa} - a_j} \omega_k\right). \end{aligned} \tag{13}$$

Hence, $e_{pa} = |(bp_j(\prod_{a_k \in A_{pa}-a_j} \omega_k) + (1-\varepsilon_j)(\Omega - bp_j(\prod_{a_k \in A_{pa}-a_j} \omega_k)))/(\Omega+1) - bp_j/(\Omega+1)|, = |(1-\varepsilon_j) - ((1-\varepsilon_j(\prod_{a_k \in A_{pa}-a_j} \omega_k))bp_j - (1-\varepsilon_j))/(bp_j + bn_j + 1)|$ □

From (11), we find that the detection error e_{pa} should have the minimum value ($e_{pa} = 0$) when bp_j and bn_j satisfy $(1 - \prod_{a_k \in A_{pa}-a_j} \omega_k)\varepsilon_j bp_j = (1-\varepsilon_j)(bn_j + 2)$.

Significantly, we observe one property of the detection accuracy of the FPTI model from (11). In addition to the parameters bp_j and bn_j, which reflect the behavior pattern of a_j, the detection accuracy is also influenced by the parameters ε_j and ω_k, where ε_j is mainly determined by the length of the corresponding diffusion path from equation (6); that is, the number of other involved agents and ω_k indicates the probability of other involved agents behaving properly in diffusion processes along this path. Thus, we have the following: □

Property 1. The detection accuracy of the FPTI model is contextually influenced; that is, the detection accuracy of the FPTI model is determined not only by the behavior pattern of the target agent, but also by the number of other involved agents in the diffusion paths and their behavior patterns.

Based on Property 1, we arrive at the following conclusions, according to (11).

(i) If $bn_j > bp_j$, the larger the difference between them, the greater the degree to which the error e_{pa} is influenced by the suspicion probability ε_j. Assuming that $bn_j >> bp_j$ *and* bn_j is infinite, e_{pa} should equal $1 - \varepsilon_j$.

(ii) If $bp_j > bn_j$, the larger the difference between them, the greater the degree to which the error e_{pa} is influenced by both the suspicion probability ε_j and the probability of other agents behaving properly, ω_j. Assuming that $bp_j >> bn_j$ and bp_j is infinite, e_{pa} should equal $(1 - \prod_{a_k \in A_{pa}-a_j} \omega_k)\varepsilon_j$.

Thus, the more maliciously an agent behaves, the detection accuracy is more likely to be influenced by the number of other involved agents in the diffusion paths; and the more properly an agent behaves, the detection accuracy is more likely to be influenced by both the number and the behavior patterns of other involved agents in the diffusion paths.

4.3.2. Feasibility of FPTI Model. In this section, we analyze the conditions for the implementation of FPTI in the following. Given a SNS, $N = <A, E>$, where A is the set of agents, $\forall <a_i, a_j> \in E$ indicates the edge directed from agent a_i to a_j. Let P_{ij} be a directed path from a_i to a_j. Then, we have the following theorems.

Theorem 3. *Let $C = <A^C, E^C>$ be a subnetwork of N, where $A^C \subseteq A$, $E^C \subseteq E$. If C is a simple cycle (a cycle with no repetitions of agents or edges), then $a_i \in A^C$ can perform feedback detection of FPTI.*

Proof of Theorem 3. $C = <A^C, E^C>$ is a simple cycle and a subnetwork of N. Thus, $a_i \in A^C$ must be a tail of an edge $<a_i, a_x> \in E^C$, and a head of an edge $<a_y, a_i> \in E^C$ where $a_x, a_y \in A^C$; and there exists a directed path P_{xy} from a_x to a_y. Hence, a message can be diffused initially from a_i, then through P_{xy}, and finally back to a_i, where C is the basis on which the feedback cross can form, and a_i is the cross agent of such feedback cross. Therefore, $a_i \in A^C$ can perform feedback detection of FPTI. □ □

Theorem 4. *Let $D = <A^D, E^D>$ be a subnetwork of N, where $A^D \subseteq A$, $E^D \subseteq E$. If D is acyclic (with no cycle), $a_i, a_x \in A^D$, and $\exists P_{xi}, P_{xi}' \subseteq D$, then a_i can perform feed-forward detection of FPTI.*

Proof of Theorem 4. $D = <A^D, E^D>$ is acyclic and a subnetwork of N, and $a_i, a_x \in A^D$. Hence, if $\exists P_{xi}, P_{xi}' \subseteq D$, then $P_{xi} \neq P_{xi}'$. P_{xi} and P_{xi}' provide two different paths for information diffusion from a_x to a_i, and there exist nonoverlapped parts between them. Thus, a message can be diffused respectively through P_{xi} and P_{xi}' and finally reach a_i, so that a feed-forward crossing situation can be formed and a_i is the cross agent. Therefore, $a_i \in A^D$ can perform feed-forward detection of FPTI. □ □

5. Enhanced FPTI Reputation Detection Model

In Section 4, we have presented the FPTI model for reputation detection in information diffusion scenarios in SNS. However, in SNS, the capacity of agents is often limited, for example, the limited capacity of communication [43], and the limited capacity of executing tasks [5, 7]. Hence, the limited capacity of agents in reputation detection should also

be taken into account. As the load of the agent's local message storage increases during the information diffusion process, the detection costs of FPTI sustained by the agents should be larger. Therefore, in this section, we investigate how to achieve satisfactory detection performance but with lower detection costs.

In FPTI, the number of messages used for detection is the key parameter that determines the detection costs. Thus, we design a message filtering method to filter a limited number of messages that are of highest *usability* for reputation detection from the agent's local message storage. The message filtering method promotes the FPTI model to the *enhanced FPTI* (*eFPTI*) model (see Figure 5).

5.1. Message Usability Evaluation. In eFPTI, the effect of the filtered messages on reputation detection can directly determine the reputation detection performance. Thus, to improve the performance of eFPTI, the different effect of the messages on reputation detection should be measured. Hence, we define the *detection value* of the message to reflect its effect on reputation detection. The factors that can reflect the effect of a message on detection performance in FPTI have been shown in Table 2. These factors jointly determine the detection value of a message.

Let S_1^m, S_2^m, S_3^m and S_4^m be the outputs of the four factors in Table 2 for the message m, respectively. The detection value of message m can be defined as

$$V_m = S_1^m \left(\alpha \cdot S_2^m + \beta \cdot S_3^m + \gamma \cdot S_4^m\right), \tag{14}$$

where α, β, and γ are parameters, which reflect the importance of the factors, respectively, shown in Table 2, and $\alpha + \beta + \gamma = 1$, $\alpha > \beta > \gamma$.

Besides the detection value for reputation detection, the *elapsed time* of a message, since it has been received, also needs to be taken into account, because of the timeliness of information diffusion (limited lifetime of the diffusion of the message [44]). If a message has been stored for longer time than other messages, it is considered to have lower probability to be used for reputation detection.

Therefore, jointly considering the detection value and the elapsed time, we give the definition of *usability* of a message. Let T_m denote the elapsed time of the message m; ψ is an attenuation function ($0 \le \psi \le 1$), and the value of $\psi(x)$ decreases monotonically as x increases. The *usability* of m is defined as

$$U_m = \psi(T_m) \cdot V_m. \tag{15}$$

5.2. Usability-Based Filtering. When agents intend to filter messages for reputation detection, they can refer to the usability of each message in their local message storages M_i and then filter the messages with the highest usability for eFPTI.

The filtering method is called *usability-based filtering* and can be described as follows.

[Step 1] Before a_i makes reputation detection, the usability of each message in M_i should be calculated according to (15).

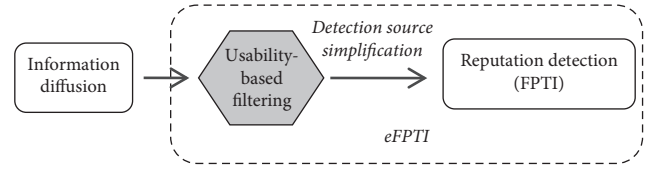

Figure 5: The enhanced FPTI model (eFPTI).

[Step 2] Then, the messages can be sorted according to their usability values.

[Step 3] Finally, the set of messages M_i' with the highest usability will be filtered for eFPTI, where $\forall m' \in M_i'$, $\forall m'' \in M_i - M_i'$, $U_{m'} > U_{m''}$ and $|M_i'| < |M_i|$.

After *usability-based filtering*, the messages, which are most useful for reputation detection in eFPTI, can be available, while the other worthless messages can be excluded from the reputation detection.

5.3. Analyses of the Enhanced FPTI Model

5.3.1. Detection Cost. The detection costs of reputation detection following the pattern "from path to individual" are composed of the following two parts: (1) the detection costs from the detection source (the messages used in detection) to the path reputations, and (2) the detection costs of aggregation from path reputations to individual reputations of agents.

The path reputation detection can be conducted by firstly executing the feedback detection and then executing the feed-forward detection in turn. For the feedback detection, it only needs to check the diffusion path of each recently received message after last detection and update the corresponding path reputation if it meets the conditions (details can be seen in Section 4.1.1); thus, the time complexity is $O(\mu \cdot k)$, where μ is the number of messages received after the last detection, and $k = |E|/|A|$ is the average degree of the system (considering that the length of the information diffusion path can be effectively estimated as proportional to the average degree of the system). For the feedforward detection, it needs to check the diffusion path of each recently received message by comparing with the messages in the local storage and update the related path reputations if it meets the conditions (details can be seen in Section 4.1.2); let $|M|$ be the number of messages in the local storage, and the time complexity is $O(\mu|M|k^2)$, since the time complexity of generating the detection region (paths) and updating the evidence space is $O(k^2)$. Hence, the time complexity of path reputation detection is $O(\mu|M||k|^2)$.

The reputation aggregation transforms the path reputations into individual reputations of agents by firstly calculating the path reputation factors for each agent involved and then evaluating each agent's reputation by superimposing the belief values of multiple paths on which this agent has participated in past information diffusion processes. After path reputation detection, there will be as most $|M|(|M|+1)$ pieces of path reputations ($|M|$ for feedback detection and $|M|^2$ for feed-forward detection); hence, the

Table 2: Factors for evaluating the detection value of a message.

Factors	Measures	Importance* (reason)
Has the message been used for producing path reputation? (F_1)	*Yes,* decreases the value of the message ($S_1^m = 0$) *No,* increases the value of the message ($S_1^m = 1$)	Most important (A message can have little chance to make further advantage for reputation detection if it has been used yet)
Whether the message can be utilized by the feedback detection? (F_2)	*Yes,* increases the value of the message($S_2^m = 1$) *No,* decreases the value of the message($S_2^m = 0$)	Very important (feedback cross can be reliable for path reputation detection)
Whether the message can be utilized by the feed-forward detection? (F_3)	*Yes,* increases the value of the message($S_3^m = 1$) *No,* decreases the value of the message ($S_3^m = 0$)	Important (feed-forward cross cannot be as reliable as feedback cross for path reputation detection)
The diffusion path length of the message. (F_4)	*Longer* length indicates the message has a higher value; *Shorter* length indicates the message has a lower value ($S_4^m = 1 - 1/l$)	Fair (The length of the diffusion path mainly influences the reusability of the corresponding path reputation for reputation aggregation)

time complexity for the calculation of path reputation factors for each agent involved is $O(|M|^2|k|)$. Then, for each agent, the reputation aggregation is conducted by superimposing the belief values of the multiple paths it involved; and the time complexity is $O(|A||M|^2)$. Hence, considering that $k << |A|$ in real social networks, the time complexity of reputation aggregation is $O(|M|^2|A|)$.

The detection costs of reputation detection following the pattern "from path to individual" are composed of (a) the detection costs of path reputation detection, and (b) the detection costs for reputation aggregation. Therefore, the time complexity of the presented FPTI model is $O(\mu|M|k^2 + |M|^2|A|)$. Moreover, the time complexity of eFPTI is $O(\mu|M'|k^2 + |M'|^2|A|)$, where $|M'|$ is the number of messages filtered, while the usability-based filtering is $O(|M'|\log|M'|)$; thus, the detection costs can be reduced effectively because $|M'|$ can be much smaller than $|M|$.

5.3.2. Detection Performance. Let $|M_i'|$ be the limited number of messages in usability-based filtering, let $\mathfrak{t}$ denote the time interval between each implementation of eFPTI to detect agents' reputations (here, we assume the time interval is uniform), and let τ represent the probability that a message can be engaged in the formation of crossing situation. Then, the following theorem can be derived:

Theorem 5. *The optimal limited number of messages of usability-based filtering is $|M_i'|_{OPT} = (Em \cdot \mathfrak{t}) \cdot \tau$, where Em is the expected number of messages stored into the local message storage in a time unit.*

Proof of Theorem 5. The usability-based filtering aims to achieve the best reputation detection performance with the lowest detection costs. Thus, (1) the messages that are valuable for reputation detection should be available after filtering; (2) the limited number of messages in usability-based filtering should be the minimum. Assume that such minimum number is $|M_i'|_{\min}$. In a time interval, $Em \cdot \mathfrak{t}$ is the number of messages received by an agent; thus, $(Em \cdot \mathfrak{t}) \cdot \tau$ can just be the number of messages, which can form the crossing situations that are valuable for reputation detection in eFPTI, so that we can have $|M_i'|_{\min} = (Em \cdot \mathfrak{t}) \cdot \tau$. Therefore, if the eFPTI model is implemented uniformly in such interval, the aim mentioned can be satisfied if $|M_i'|_{\text{OPT}} = |M_i'|_{\min} = (Em \cdot \mathfrak{t}) \cdot \tau$. □

6. Experimental Validation and Analyses

The proposed reputation detection models (FPTI and eFPTI) are validated by experimental evaluations from the following perspectives:

(i) *Feasibility & Effectiveness*: we evaluate the reputation detection performance of our models (FPTI and eFPTI) by using Twitter datasets [45], and we also compare the performance of our two models.

(ii) *Properties*: we first confirm the robustness of the models in different types of dynamic environments. Then, we test the effect of the key parameter, suspicion probability, in the models.

(iii) *Applicability*: we test the applicability of our models by implementing the models into a typical application scenario in information diffusion—misinformation suppression.

6.1. Experimental Settings. The information diffusion scenarios were constructed according to the model presented by Gruhl et al. in their research on information diffusion through blogspace [33]. The details of the information diffusion process in our experiments are described below, and one sketch of the diffusion process is shown in Figure 6. In the information diffusion scenarios considered in this paper, the upstream neighbors of an agent a_i represent the agents that can diffuse messages to a_i, and the downstream neighbors of a_i represent the agents that can receive messages diffused by a_i.

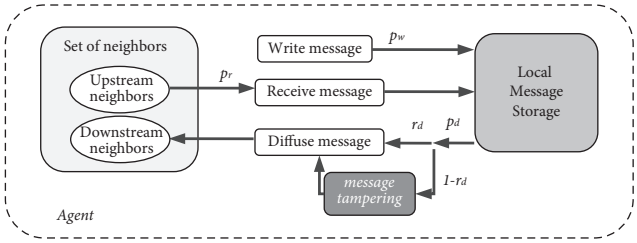

Figure 6: The experimental environment settings.

At the initial state, agents write messages, with probability p_w. At the successive states, agents have the opportunity to receive those messages, with probability p_r. Agents who receive a message can choose whether to diffuse it with diffusion probability p_d. Then, by considering the decay property of information diffusion [26], p_r decreases according to a decreasing function of the time elapsed, which is $p_r = \mathrm{X}(t' - t) \times p_r'$, where t is the time at which the message was initially diffused by the upstream agent, t' is the current time, $\mathrm{X}(t' - t)$ is a function that decreases from 1.0 to 0.0 as $(t' - t)$ increases, and p_r' is the inherent probability of agents receiving messages. Therefore, in the experiments, for each time step, each agent has an opportunity to write messages, receive messages, and diffuse messages, with probabilities of p_w, p_r', and p_d, respectively. The decreasing function $\mathrm{X}(t' - t)$ for receiving probability modification is set to $1/(t' - t)^2$.

The default reputation r_d for each agent is set randomly ranging from 0.0 to 1.0. $1 - r_d$ is the probability that the agent will behave maliciously; for instance, if the r_d of an agent is 0.7, there is a 30% probability that it will engage in malicious behavior at each time step. Moreover, in the eFPTI model, the limited number of message filtering methods, $|M_i'|$, is set to 20.

6.2. Feasibility and Effectiveness of the Models. In this section, we validate the feasibility and effectiveness of our models by using Twitter datasets extracted by Greene and Cunningham [45]: Football (FB), which is the network dataset, consists of 248 football players and clubs active on Twitter and 3819 edges among them, Olympics (OLY), which is the network dataset consists of 464 Twitter accounts of athletes and organizations in London 2012 Summer Olympics and 10642 edges among the accounts, Politics-ie (POL), which is the network dataset of Twitter users including 348 Irish politicians and political organizations and 16856 edges among these users, and Rugby (RUG), which is the dataset of 854 international Rugby Union players, clubs, and organizations active on Twitter and 35757 edges among them. The details of the datasets are shown in Table 3. The datasets include not only the data of network structure, but also the retweeting data among Twitter users, that is, the users and edges actually observed in the retweeting processes, which can be also used to investigate the feasibility of our models.

6.2.1. Feasibility Tests for Path Reputation Detection. To validate the feasibility of FPTI and eFPTI models, we first use the retweeting data (including retweeting relations between paired users and corresponding retweeting weights) to construct real retweeting paths through Twitter users, which are represented by retweeting networks among users. Then, feasible feedback and feed-forward crosses in the retweeting networks, which can support the implementation of reputation detection of the presented FPTI and eFPTI models, have been investigated in depth-first order [46] and breadth-first order [47], respectively.

Table 3: Summary of datasets [45].

Dataset	Users	Edges	Retweeting users	Retweeting edges
Football (FB)	248	3819	234	1350
Olympics (OLY)	464	10642	440	3740
Politics-ie (POL)	348	16856	307	3019
Rugby (RUG)	854	35757	827	12472

Figures 7(a) and 7(b) show the number of feedback and feed-forward crosses discovered from the retweeting networks of the four Twitter datasets. The results show that there are a great number of feasible feedback and feed-forward crosses (even in FB retweeting network with the least nodes and relations) that can be sufficient to support the path reputation detection of FPTI and eFPTI models; namely, the discovered crosses can satisfy the conditions for reputation detection demonstrated by Theorems 2 and 3. Moreover, by comparing the results in Figures 7(a) and 7(b), we find that the numbers of feasible feed-forward crosses in retweeting networks can be much larger than that of feedback crosses; it indicates the higher feasibility of feed-forward detection of our models in path reputation detection. In conclusion, verified by the retweeting data from the Twitter datasets, there are feasible information diffusion structures that can support the implementation of the presented FPTI and eFPTI models for reputation detection in information diffusion scenarios.

6.2.2. Coverage and Accuracy Tests. To test the effectiveness of our models, we first introduce the following baseline model. *The ideal interaction model* (*Ideal model*): in this model, each activity of an agent can be ideally observed by the agent's neighbors immediately as if they have direct interactions during the whole process. In fact, this model cannot be applied in real information diffusion scenarios, but it can be set as the standard (upper bound) for performance evaluation.

The effectiveness tests have been conducted in information diffusion scenarios (see Section 6.1) on Twitter user networks shown in Table 3. The parameters for information diffusion are set as follows: $p_w = 0.05$, $p_r' = 0.1$, and $p_d = 0.1$. The results are obtained at the 500^{th} step of the information diffusion processes.

(1) Coverage Tests. Coverage tests focus on what percentage of the agents in the network can be detected by the reputation model. The detection coverage is defined as $\mathrm{Cov} = |A'|/|A|$, where $|A'|$ is the number of agents whose reputations have been detected, and $|A|$ is the total number of agents in the network.

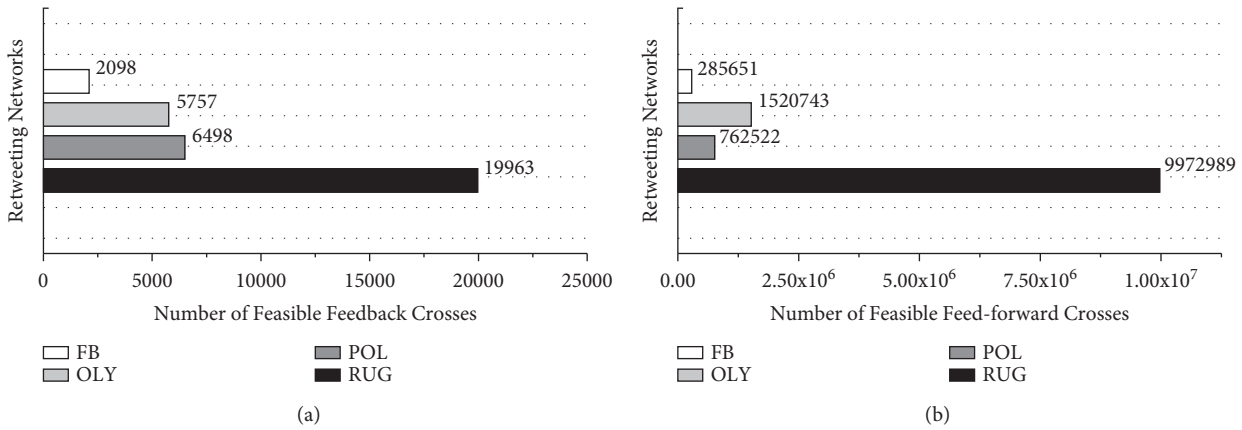

Figure 7: Feasibility validation of path reputation detection of the presented models. (a) Feedback detection. (b) Feed-forward detection.

If employing the ideal model, all the activities of the agents can be ideally observed by their neighbors (which is actually impossible in reality), so that the coverage of the ideal model can keep 1.0 during all the periods. Hence, the results of detection coverage by using the ideal model are omitted here. Table 4 shows the results of the detection coverage of our models (FPTI and eFPTI) in Twitter networks. From Table 4, we find that, using FPTI model, the detection coverage can be equal or greater than 0.74; and in the networks of POL and RUG with relatively higher average degree, the detection coverage can be larger than 0.95, which is close to the optimal results. Then, using eFPTI model, the detection coverage can be closer to that using FPTI model if the average degree of the users is higher; in the POL and RUG networks, the performance loss of eFPTI model can be very low, and the coverage can achieve 0.9. The performance loss using eFPTI is caused by the message filtering introduced in Section 5.

(2) Accuracy Tests. Let er_x be the difference between the detected reputation of an agent and its default reputation set initially. The detection accuracy is defined as $\mathrm{Acc} = \sum_{\forall er_x \in \{er\}} (1 - er_x)/|\{er\}|$, where $\{er\}$ is the set of er_x. The initial er_x in the simulation is set to 0.5.

Figure 8 reports the accuracy test results. The ideal model can obviously have the best performance on detection accuracy. There are two reasons: (1) each activity of an agent can be ideally observed by the agent's neighbors immediately; and (2) the transformation of ideal model from the observed evidences (neighbors' activities) into agents' reputations is set to uniform, which coincides with our experimental settings of agents' behavior pattern. Hence, the ideal model can have a very high accuracy in reputation detection (close to 0.9 in FB and OLY networks, and close to 0.95 in POL and RUG networks).

In Figure 8, we can find that the detection accuracy employing our models can achieve 0.7 on the Twitter user networks. The performance gap between our models and the ideal model is mainly caused by (1) the incomplete information that agents can only obtain in the information diffusion processes, (2) and the transformation error from path reputation into reputations of agents. For the former aspect, the ideal model can have complete information of agents' behaviors in the reputation detection that is actually impossible in reality; then, for the latter aspect, as introduced before, it is very difficult to estimate the reputations of agents from the obtained path reputation because of the concatenation of agents' behaviors through paths in information diffusion scenarios. Therefore, compared with the ideal model, the detection employing FPTI and eFPTI models can be considered to be of high accuracy and satisfying.

Table 4: Detection coverage in twitter networks.

Dataset	FPTI	eFPTI
Football (FB)	0.747 (±0.023)	0.586 (±0.036)
Olympics (OLY)	0.798 (±0.014)	0.718 (±0.015)
Politics-ie (POL)	0.960 (±0.006)	0.939 (±0.006)
Rugby (RUG)	0.980 (±0.002)	0.975 (±0.003)

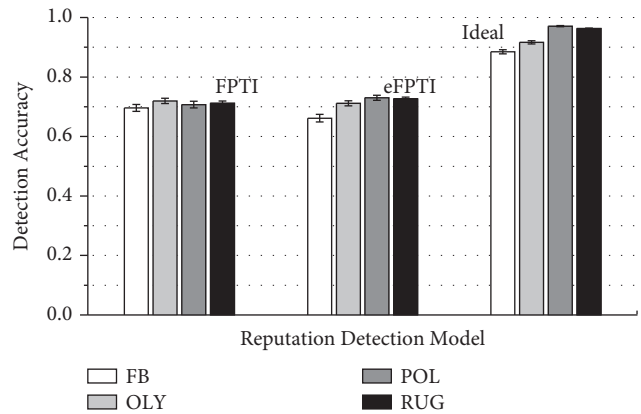

Figure 8: Detection accuracy in twitter networks.

6.2.3. Comparison between Our Two Models. In this section, we compare our presented eFPTI model with the FPTI model. Besides the detection coverage and accuracy, we also compare the detection costs of the two models. Figure 8

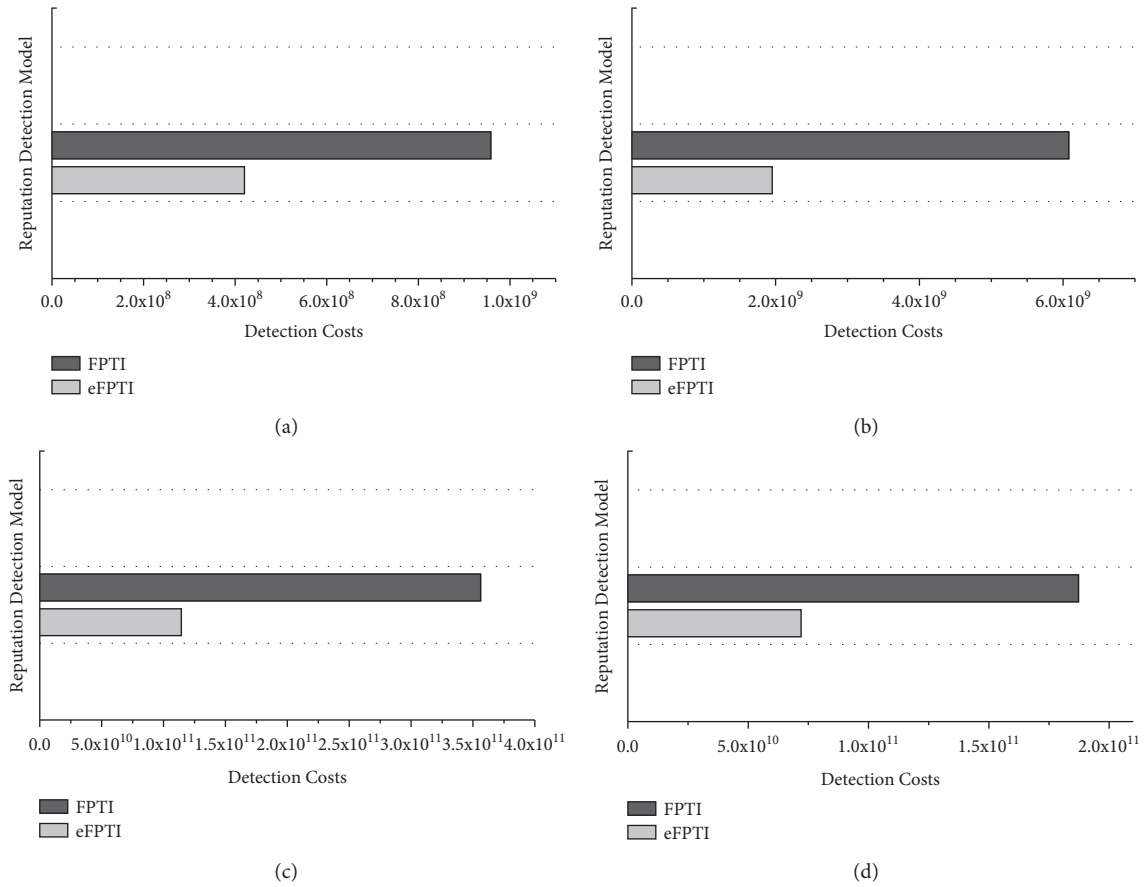

Figure 9: Comparison of the proposed reputation detection models (FPTI vs. eFPTI) on the detection costs. (a) Detection costs in FB network. (b) Detection costs in OLY network. (c) Detection costs in POL network. (d) Detection costs in RUG network.

shows that the eFPTI model can perform as well as the FPTI model on the reputation detection accuracy in all the tested Twitter networks; then, Table 4 indicates that the eFPTI performs a little worse on the detection coverage than the FPTI model, and the performance of eFPTI can be closer to that of FPTI if the network average degree is larger. Finally, in Figure 9, we observe that the reputation detection costs of eFPTI are much lower than those of FPTI in the tested networks. These results validate the advantage of eFPTI. Therefore, the eFPTI model reaches the expected objective to achieve satisfactory performance of reputation detection with lower detection costs.

In conclusion, the presented FPTI and eFPTI models both achieve the corresponding objectives for reputation detection in information diffusion scenarios in SNS, which are verified by several Twitter datasets. The FPTI model performs well on the detection coverage and accuracy; the detection coverage ranges from 0.74 to 0.98, and the detection accuracy can be up to 0.7. The eFPTI model also achieves satisfying performance on detection coverage and accuracy that are close to those of FPTI model in most of the cases, and it can have much lower costs in reputation detection.

6.2.4. Comparison with the Representative. We compare the presented FPTI and eFPTI models with the representative reputation model, *the direct interaction model* (DI) [17, 18] in this section. This benchmark model uses the direct interaction experiences among agents to assess their reputations. It is often considered as the most important component in most of the integrated reputation models, such as Regret [16], FIRE [17], and FIRE+ [20], and can also be used as the source to generate the indirect reputation factors in these models.

The experiments are conducted in a specially set environment where forming bidirectional relationships are facilitated by setting the same probability to construct the relations in both directions between paired users. In the traditional direct interaction model, the agents evaluate the reputations of their neighbors by their direct interaction experiences during the whole information diffusion process.

Figures 10(a) and 10(b) show the results of the detection coverage and accuracy of the presented models and the DI model, respectively. From Figures 9(a) and 9(b), we observe that the presented FPTI and eFPTI models can have much better performance than the DI model on the detection coverage and accuracy. The performance advantage of our models on the detection coverage compared with the DI model is large, which is nearly 0.75; and then, for the detection accuracy, our models can be 0.13 higher than the DI model (only the agents that can be detected are considered).

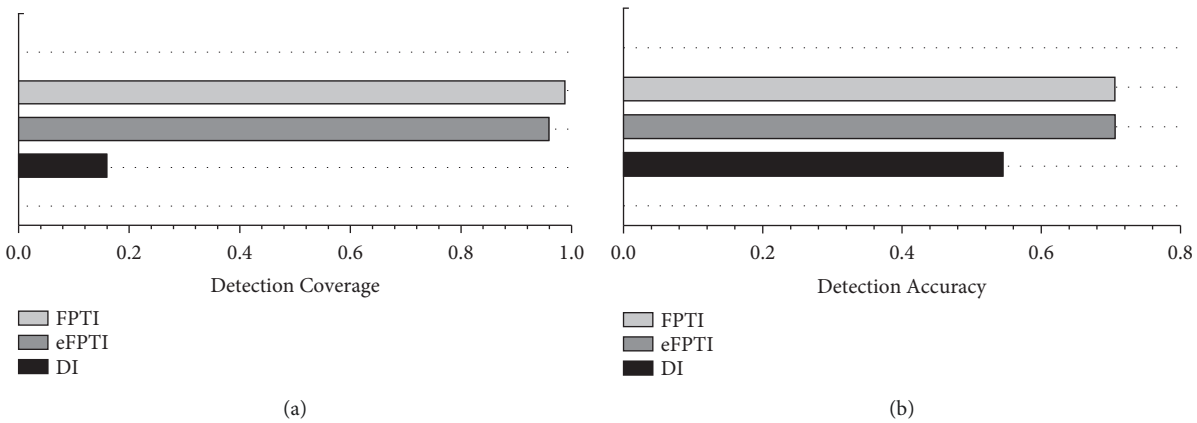

Figure 10: Reputation detection performance of the presented models (FPTI and eFPTI) vs. the direct interaction model (DI). (a) Results of detection coverage. (b) Results of detection accuracy.

The potential reasons for the observed results are as follows: (1) compared with the DI model, our models can detect much more evidences of the agents' behaviors by using path reputation detection through a large amount of diffusion crosses during the information diffusion process, while the DI model can only obtain evidences from the direct interaction experiences, which largely restrict the detection scope and the evidence quantity; (2) then, because more evidences can lead to more accurate assessment of the agents' reputations, the less evidence quantity of the DI model will lead to a lower detection accuracy. In fact, there is another explanation that can be easier to understand: the DI model can be just considered as a special case in the feedback detection of the FPTI and eFPTI models when the path length of the feedback cross is 2. In conclusion, the direct interaction reputation model cannot be well adapted to the information diffusion scenarios considered in this paper. This also gives an insight into the problem that traditional models may have in the information diffusion environment.

6.3. Key Properties of the Models. We investigate the key properties of the presented models: (1) the robustness in dynamic environments, and (2) the effect of suspicion probability in the presented models. For the convenience of property investigation, the initial network for information diffusion is constructed according to the random social network model [48], which initially contains 500 nodes, and the average degree of the initial networks is 10. The parameters for information diffusion are set as follows: $p_w = 0.1$, $p_r' = 0.2$, and $p_d = 0.2$.

6.3.1. Robustness for Dynamic Environments. The dynamic environments in the experiments are set as follows:

(i) Agent behavior pattern reset (*dynamic type i*): the probabilities of agents to behave maliciously can be dynamically reset; namely, the values of their default reputations are reassigned; in this robustness test, the probabilities of all the agents in the system to behave maliciously are reassigned randomly.

(ii) Network relationship rewiring (*dynamic type ii*): the network relationships of the system can be dynamically rewired; namely, old relationships between agents can be destroyed, and, at the same time, new relationships will be created; in this robustness test, there is a 50% probability of rewiring for each edge in the system by selecting paired agents randomly.

(iii) New agent entrance (*dynamic type iii*): considering the open environment, agents can dynamically enter the system and construct relationships with other agents; in this robustness test, new agents, the number of whom is 10% of the initial number of agents, will join the system (i.e., 50 new agents will join the system for each dynamic change).

We also set the mixed dynamic environments (*dynamic type i + ii + iii*) to test the robustness of our models (FPTI and eFPTI). The dynamic changes of the system are conducted at the 100^{th}, 200^{th}, 300^{th}, and 400^{th} steps of the experiments, respectively.

Figure 11 shows the performance of the reputation detection of our models (FPTI and eFPTI) in these dynamic environments. In Figure 11(a), when the probabilities of agents to behave maliciously are dynamically reset, the reputation detection accuracy decreases dramatically. The reason is that the past observations for the agents' reputation estimation can not reflect their behavior pattern after reset. Such situation makes a challenge of fast convergence of reputation detection. But from the plot, we can see that the detection accuracy of our models can recover soon after a short period of time and converge to the former state. In Figure 11(b), we observe that the network relationship rewiring of the system does not have an obvious impact on the performance of our models. The potential reason is that, after relationship rewiring, the past observations that can be used for reputation detection can also reflect the behavior pattern of engaged agents. Thus, our models are robust in this type of dynamic environments where network relationships may be rewired. Figure 11(c) indicates the robustness of our models in the environments where new

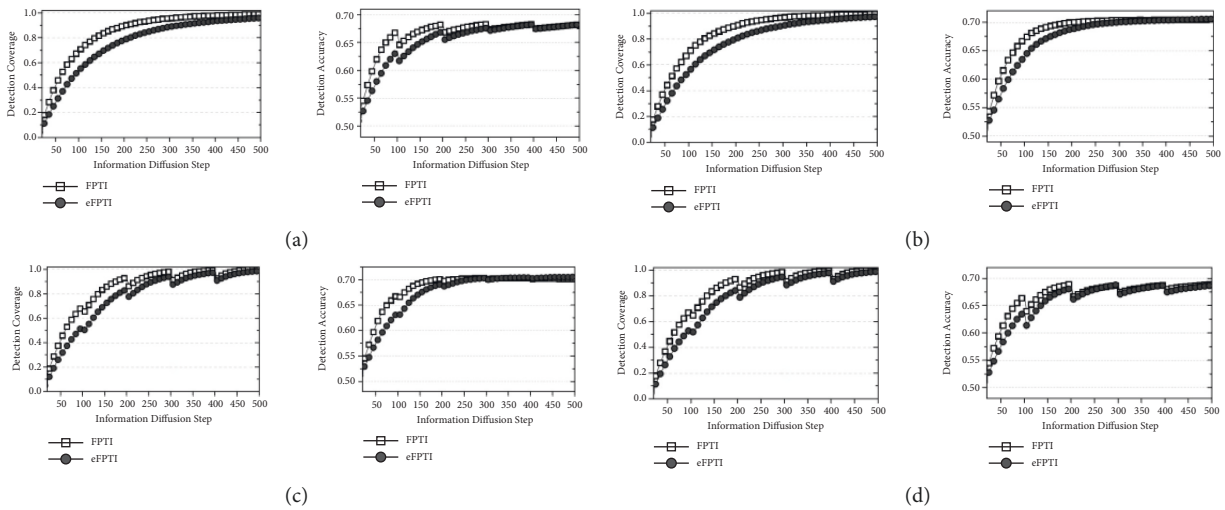

Figure 11: The robustness tests of the FPTI and eFPTI models in different types of dynamic environments. (a) Agent behavior pattern reset. (b) Network relationship rewiring. (c) New agent entrance. (d) Mixed dynamic environment.

agents can enter. We find that when new agents enter the systems, the detection coverage and accuracy have been both influenced. Unlike the dynamic of agent behavior pattern reset, the detection coverage of our models in this type of dynamic environment has obvious fluctuations. But from this plot, we can observe that our models can recover soon and also achieve the expected results. Figure 11(d) shows the test results of our models in the mixed dynamic environments. With several dynamic situations combined in the environment, the detection coverage and accuracy of our models both have obvious fluctuations. But similar to the results in previous dynamic environments, our models can also be robust in this mixed dynamic environment and can achieve good performance. In conclusion, the presented models (FPTI and eFPTI) are robust for the reputation detection in several dynamic environments where agents may dynamically change their behavior patterns, network relationships may be rewired, and new agents may enter the system.

6.3.2. Effect of Suspicion Probability in Reputation Aggregation. In this section, we aim to confirm the effect of suspicion probability introduced in our models. We first ignore the suspicion probability in our models (FPTI and eFPTI) and then employ such modified models to perform the same tests as those in previous section. By comparing the corresponding results, the effect of the suspicion probability can be proved. Here, we only compare their detection accuracy performance, because the modification (ignoring the suspicion probability) cannot influence the detection coverage.

Figure 12(a) shows that there is a large performance difference between the original models and the modified models without considering the suspicion probability. The detection accuracy of modified models is nearly 0.11–0.13 lower than that of the original models. Such results obviously indicate the benefit of considering suspicion probability in reputation aggregation.

Then, in Figure 12(b), we can see how the suspicion probability takes effect in the reputation detection. We first give the definition of the error distribution ratio (*EDR*) as follows: $\mathrm{EDR} = N_{\text{err-}n}/N_{\text{err-}p}$, where $N_{\text{err-}n}$ and $N_{\text{err-}p}$ represent the number of negative detection and positive detection, respectively. The positive (negative) detection indicates that the detected reputation of an agent is higher (lower) than its default reputation set initially. In Figure 12(b), the EDRs of the modified models are much larger than those of the origin FPTI and eFPTI models; namely, there are much more negative detections when not considering the suspicion probability. This validates the aim of introducing suspicion probability into reputation detection, which is to revise the effect of obtained negative evidences on reputation aggregation. If no such revision has been carried out, agents' reputations could be significantly underestimated.

6.4. Applicability of the Models on Misinformation Suppression. In this section, we apply our models (FPTI and eFPTI) in information diffusion scenarios and test the effects of agents' reputations detected by our models on misinformation suppression. A threshold method utilizing the detected reputations is used to suppress the influence of malicious behaviors. Let I_m be the ratio of the number of messages that have been tampered with, thus taking misinformation to the total number of messages in the system, and I_m' be the ratio of the number of messages that take misinformation to number of messages after the suppression approach is implemented. The details of the threshold method are described below. Let A_u and A_d be the set of upstream and downstream neighbors of an agent a_i, and let $r_i(j)$ be the reputation of a_j evaluated by a_i. The agent a_i can first set the threshold values α and β for upstream and downstream neighbors, respectively, and then, it can only receive messages from A_u' and diffuses messages to A_d', where $A_u' \subseteq A_u$, $A_d' \subseteq A_d$, $\forall\ r_i(a_u') > \alpha\ (a_u' \in A_u')$, and $\forall\ r_i(a_d') > \beta\ (a_d' \in A_d')$. In the experiments, we set α and β to be equal to 0.7.

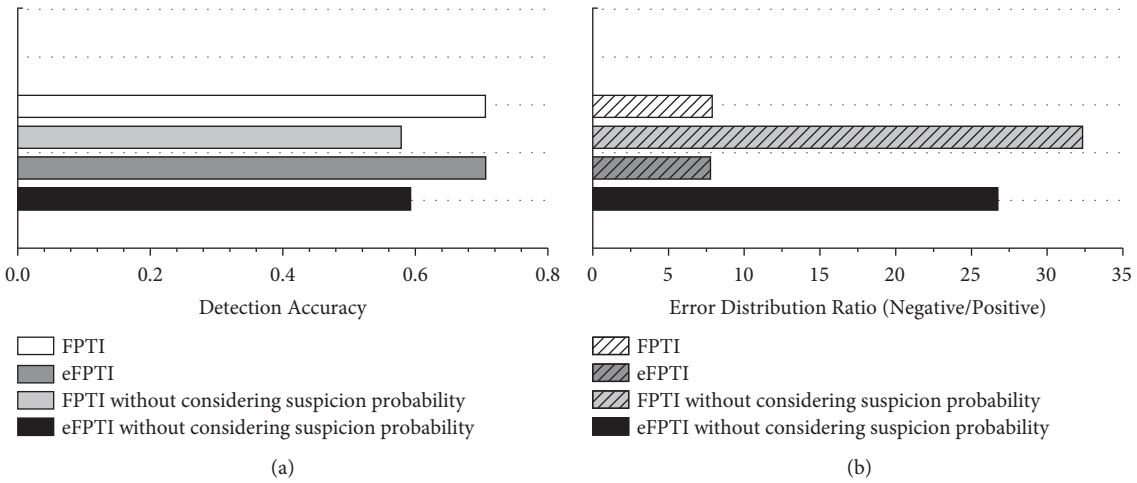

Figure 12: The effects of suspicion probability in the proposed models on (a) the detection accuracy, and (b) the error distribution. (a) Results of detection accuracy. (b) Results of error distribution ratio.

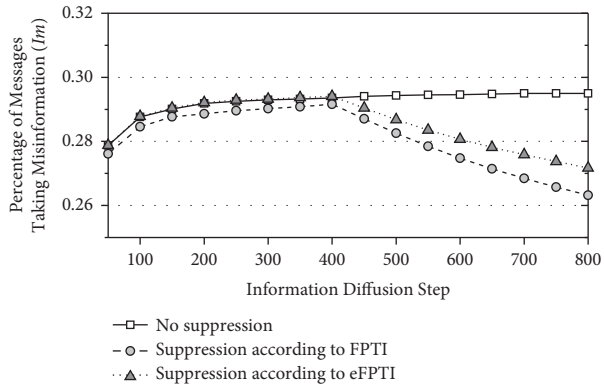

Figure 13: The effect of reputations of agents (generated by the proposed models) for suppressing the influence of malicious behaviors (the suppression approach is implemented at the 400th execution step).

For example, let $A_u = \{a_1, a_2, a_3\}$ be the set of upstream neighbors of agent a_i; that is, there are edges directed from the agent a_1, a_2 and a_3 to a_i, respectively, and $r_i(a_1) = 0.35$, $r_i(a_2) = 0.76$ and $r_i(a_3) = 0.91$; let $A_d = \{a_4, a_5, a_6, a_7\}$ be the set of upstream neighbors of agent a_i; that is, there are edges directed from the agent a_i to a_4, a_5, a_6 and a_7, respectively, and $r_i(a_4) = 0.21$, $r_i(a_5) = 0.83$, $r_i(a_6) = 0.96$ and $r_i(a_7) = 0.62$. If the threshold value for upstream neighbors α is set to 0.7, then the agent a_i can only receive messages from a_2 and a_3 for misinformation suppression; and if the threshold value for downstream neighbors β is set to 0.7, then the agent a_i can only diffuse messages to a_5 and a_6 for misinformation suppression.

Figure 13 provides insight into the effect of the reputations detected by our models in weakening the influence of malicious behaviors in information diffusion. This plot first shows that, with no suppression on malicious behaviors, I_m increases rapidly in the early stages and then gradually tends towards stability; that is, the number of messages tampered with increases as the total number of messages increases. Then, from the results implementing the suppression approach, we can see that a gradual decrease in I_m occurs after the suppression approach is implemented at the 400^{th} execution step. Finally, at the 800^{th} step, the results obtained using the suppression approach can be much better. (The percentage of misinformation after misinformation suppression based on the reputation detection results by FPTI and eFPTI declined by 30.4% and 20.6%, respectively).

7. Conclusion and Future Works

We present a novel distributed reputation detection pattern "*from path to individual*," which can overcome the problem that it may be difficult or impossible to determine interaction reputations in the absence of direct interactions in scenarios of information diffusion in SNS. The main idea is that the positive (negative) observation of an information diffusion process increases (decreases) the belief of the corresponding diffusion path, which further increases (decreases) the reputation of each involved agent.

Based on the detection pattern "*from path to individual*," we then propose the FPTI and eFPTI models. The FPTI model effectively addresses the following issues for the diffusion in SNS: (a) how to detect path reputations from information diffusion process, and (b) how to aggregate obtained path reputations into reputations of agents. Furthermore, the eFPTI (enhanced FPTI) model is proposed in order to address an additional important issue: how to effectively reduce the detection costs on the premise that satisfactory detection performance can be achieved.

Through theoretical analyses and experimental evaluations, we have shown that, in information diffusion scenarios in SNS, (1) the presented models (FPTI and eFPTI) can be effective and efficient in reputation detection, (2) the reputations of agents determined using the presented models can be considered as appropriate alternatives to interaction reputations, and (3) the obtained agents' reputations are valuable for suppressing the influence of malicious behaviors.

In future work, we plan to extend our model in the following ways:

(i) Collusion between agents is not currently considered in the model. However, agents in social network systems may collude to achieve their selfish goals [49]. For this reason, we plan to extend our model for reputation detection in the future to consider collusion between agents in information diffusion scenarios in SNS.

(ii) Recently, the multiplex nature of social networks has received considerable attention [50, 51]. This feature of social networks suggests that it may be useful to study reputation models that suit the characteristics of multiplex social network systems. Thus, we also plan to extend our model to multiplex social network systems by considering their particular network characteristics, for example, diverse relative bias for diffusion in different network layers [51] and the relevance of connectivity between multiple network layers [52].

Data Availability

The data that support the findings of this study are available upon request from the corresponding author.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This research was supported by the National Natural Science Foundation of China (Nos. 61807008, 61806053, and 62076060) and the Natural Science Foundation of Jiangsu Province of China (BK20180369 and BK20180356). Some preliminary results of this paper were presented at the Proceedings of the 12th IEEE/WIC/ACM International Conference on Intelligent Agent Technology.

References

[1] H. Kwak, C. Lee, H. Park, and S. Moon, "What is twitter, a social network or a news media?" in *Proceedings of the 19th International Conference on World Wide Web (WWW'10)*, pp. 591–600, Raleigh, NC, USA, April 26-30, 2010.

[2] H. U. Khan, S. Nasir, K. Nasim, D. Shabbir, and A. Mahmood, "Twitter trends: a ranking algorithm analysis on real time data," *Expert Systems with Applications*, vol. 164, Article ID 113990, 2021.

[3] M. M. Skeels and J. Grudin, "When social networks cross boundaries: a case study of workplace use of facebook and LinkedIn," in *Proceedings of the ACM 2009 International Conference on Supporting Group Work (GROUP'09)*, pp. 95–104, Sanibel Island, Florida, USA, May 10–13, 2009.

[4] H. Yu, C. Miao, B. An, C. Leung, and V. R. Lesser, "A reputation management approach for resource constrained trustee agents," in *Proceedings of the Twenty-Third International Joint Conference on Artificial Intelligence (IJCAI'13)*, pp. 418–424, Beijing, China, August 3-9, 2013.

[5] Y. Jiang and J. C. Jiang, "Understanding social networks from a multiagent perspective," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 10, pp. 2743–2759, 2014.

[6] H. Ohtsuki, C. Hauert, E. Lieberman, and M. A. Nowak, "A simple rule for the evolution of cooperation on graphs and social networks," *Nature*, vol. 441, no. 7092, pp. 502–505, 2006.

[7] Y. Jiang, Y. Zhou, and W. Wang, "Task allocation for undependable multiagent systems in social networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 8, pp. 1671–1681, 2013.

[8] M. M. de Weerdt, Y. Zhang, and T. Klos, "Multiagent task allocation in social networks," *Autonomous Agents and Multi-Agent Systems*, vol. 25, no. 1, pp. 46–86, 2012.

[9] V. Krishnamurthy and H. V. Poor, "A tutorial on interactive sensing in social networks," *IEEE Transactions on Computational Social Systems*, vol. 1, no. 1, pp. 3–21, 2014.

[10] J. Sabater and C. Sierra, "Review on computational trust and reputation models," *Artificial Intelligence Review*, vol. 24, no. 1, pp. 33–60, 2005.

[11] S. D. Ramchurn, D. Huynh, and N. R. Jennings, "Trust in multi-agent systems," *The Knowledge Engineering Review*, vol. 19, no. 1, pp. 1–25, 2004.

[12] E. Franchi and A. Poggi, "Multi-agent systems and social networks," *Handbook of Research on Business Social Networking*, IGI Global, Pennsylvania, pp. 84–97, 2012.

[13] F. Bergenti, E. Franchi, and A. Poggi, "Enhancing social networks with agent and semantic web technologies," *Collaboration and the Semantic Web: Social Networks, Knowledge Networks, and Knowledge Resources*, pp. 83–100, 2012.

[14] J. Yao, W. Tan, S. Nepal et al., "ReputationNet: reputation-based service recommendation for e-science," *IEEE Transactions on Services Computing*, vol. 8, no. 3, pp. 439–452, 2015.

[15] D. Artz and Y. Gil, "A survey of trust in computer science and the semantic web," *Journal of Web Semantics*, vol. 5, no. 2, pp. 58–71, 2007.

[16] J. Sabater and C. Sierra, "Reputation and social network analysis in multi-agent systems," in *Proceedings of the First International Conference on Autonomous Agents and Multi-agent Systems (AAMAS'02)*, pp. 475–482, Bologna, Italy, July15-19, 2002.

[17] T. D. Huynh, N. R. Jennings, and N. R. Shadbolt, "FIRE: an integrated trust and reputation model for open multi-agent systems," in *Proceedings of the 16th European Conference on Artificial Intelligence (ECAI'04)*, pp. 18–22, Valencia, Spain, August 22-27, 2004.

[18] eBay, "eBay," http://www.ebay.com, 2004.

[19] G. Zacharia and P. Maes, "Trust management through reputation mechanisms," *Applied Artificial Intelligence*, vol. 14, no. 9, pp. 881–907, 2000.

[20] B. Qureshi, G. Min, and D. Kouvatsos, "Countering the collusion attack with a multidimensional decentralized trust and reputation model in disconnected MANETs," *Multimedia Tools and Applications*, vol. 66, no. 2, pp. 303–323, 2013.

[21] K. Kravari and N. Bassiliades, "DISARM: a social distributed agent reputation model based on defeasible logic," *Journal of Systems and Software*, vol. 117, pp. 130–152, 2016.

[22] J. Carbo, J. M. Molina, and J. Davila, "Trust management through fuzzy reputation," *International Journal of Cooperative Information Systems*, vol. 12, no. 01, pp. 135–155, 2003.

[23] Q. Wu, Q. Zhu, and P. Li, "A neural network based reputation bootstrapping approach for service selection," *Enterprise Information Systems*, vol. 9, no. 7, pp. 768–784, 2015.

[24] F. Cornelli, E. Damiani, S. Vimercati, S. Paraboschi, and P. Samarati, "Choosing reputable servents in a P2P network," in *Proceedings of the 11th International Conference on World Wide Web (WWW'02)*, pp. 376–386, Honolulu, Hawaii, USA, May 7-11, 2002.

[25] C. Lee, H. Kwak, H. Park, and S. Moon, "Finding influentials based on the temporal order of information adoption in twitter," in *Proceedings of the 19th International Conference on World Wide Web (WWW'10)*, pp. 1137-1138, Raleigh, NC, USA, April 26-30, 2010.

[26] J. Yang and J. Leskovec, "Modeling information diffusion in implicit networks," in *Proceedings of the 2010 IEEE International Conference on Data Mining (ICDM'10)*, pp. 599–608, Sydney, Australia, December 14-17, 2010.

[27] Y. Zhou and Y. Jiang, "From path to individual: a distributed reputation detection model for information diffusion," in *Proceedings of the 12th IEEE/WIC/ACM International Conference on Intelligent Agent Technology (IAT'12*, pp. 188–195*)*, Macau, China, December 4-7, 2012.

[28] A. JØsang, "A subjective metric of authentication," in *Proceedings of the Computer Security — ESORICS 98*, vol. 1485, pp. 329–344, Louvain-la-Neuve, Belgium, September 16-18, 1998.

[29] A. Jøsang, "A logic for uncertain probabilities," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 09, no. 03, pp. 279–311, 2001.

[30] Y. Wang and M. P. Singh, "Formal trust model for multiagent systems," in *Proceedings of the 20th International Joint Conference on Artificial Intelligence (IJCAI'07)*, pp. 1551–1556, Hyderabad, In-dia, January 6-12, 2007.

[31] Y. Wang and M. P. Singh, "Trust representation and aggregation in a distributed agent system," in *Proceedings of the Twenty-first National Conference on Artificial Intelligence (AAAI'06)*, pp. 1425–1430, Boston, Massachusetts, USA, July 16-20, 2006.

[32] C. Hang, Y. Wang, and M. P. Singh, "Operators for propagating trust and their evaluation in social networks," in *Proceedings of the Eighth International Conference on Autonomous Agents and Multiagent Systems (AAMAS'09)*, pp. 1025–1032, Budapest, Hungary, May 10-15, 2009.

[33] D. Gruhl, D. Liben-Nowell, R. Guha, and A. Tomkins, "Information diffusion through blogspace," in *Proceedings of the 13th International World Wide Web Conference (WWW'04)*, pp. 491–501, New York, NY, USA, May 17-20, 2004.

[34] J. L. Iribarren and E. Moro, "Impact of human activity patterns on the dynamics of information diffusion," *Physical Review Letters*, vol. 103, no. 3, Article ID 038702, 2009.

[35] A. Mohaisen, T. AbuHmed, T. Zhu, and M. Mohaisen, "Collaboration in social network-based information dissemination," in *Proceedings of the IEEE International Conference on Communications (ICC'12)*, Ottawa, ON, Canada, June 10-15, 2012.

[36] Y. Jiang, "Concurrent collective strategy diffusion of multiagents: the spatial model and case study," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 39, no. 4, pp. 448–458, 2009.

[37] Y. Jiang and T. Ishida, "A model for collective strategy diffusion in agent social law evolution," in *Proceedings of the 20th International Joint Conference on Artificial Intelligence (IJCAI'07)*, pp. 1353–1358, Hyderabad, India, January 6-12, 2007.

[38] D. Lin and T. Ishida, "Coordination of local process views in interorganizational business process," *IEICE - Transactions on Info and Systems*, vol. E97-D, no. 5, 2014.

[39] Y. Jiang and J. C. Jiang, "Diffusion in social networks: a multiagent perspective," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 45, no. 2, pp. 198–213, 2015.

[40] C. Gao, J. Liu, and N. Zhong, "Network immunization with distributed autonomy-oriented entities," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 7, pp. 1222–1229, 2011.

[41] D. Liben-Nowell and J. Kleinberg, "Tracing information flow on a global scale using internet chain-letter data," *Proceedings of the National Academy of Sciences*, vol. 105, no. 12, pp. 4633–4638, 2008.

[42] J. Caverlee, L. Liu, and S. Webb, "Socialtrust: tamper-resilient trust establishment in online communities," in *Proceedings of the 8th ACM/IEEE-CS Joint Conference on Digital Libraries (JCDL'08)*, pp. 104–114, Pittsburgh, Pennsylvania, USA, June 16-20, 2008.

[43] G. Miritello, R. Lara, M. Cebrian, and E. Moro, "Limited communication capacity unveils strategies for human interaction," *Scientific Reports*, vol. 3, no. 1, p. 1950, 2013.

[44] I. Taxidou and P. Fischer, "Realtime analysis of information diffusion in social media," *Proceedings of the VLDB Endowment*, vol. 6, no. 12, pp. 1416–1421, 2013.

[45] D. Greene and P. Cunningham, "Producing a unified graph representation from multiple social network views," in *Proceedings of the 5th Annual ACM Web Science Conference (WebSci'13)*, pp. 118–121, Paris, France, May 1–5, 2013.

[46] R. Tarjan, "Depth-first search and linear graph algorithms," *SIAM Journal on Computing*, vol. 1, no. 2, pp. 146–160, 1972.

[47] D. E. Knuth, *The Art of Computer Programming*, Vol. Vol 1, Addison-Wesley, Boston, 3rd ed edition, 1997.

[48] M. E. J. Newman, D. J. Watts, and S. H. Strogatz, "Random graph models of social networks," *Proceedings of the National Academy of Sciences*, vol. 99, no. suppl_1, pp. 2566–2572, 2002.

[49] Z. Rui, T. Fu, D. Lai, and Y. Jiang, "Cooperation among malicious agents: a general quantitative congestion game framework," in *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems (AAMAS'12)*, pp. 1331-1332, Valencia, Spain, June 4-8, 2012.

[50] J. Gómez-Gardeñes, I. Reinares, A. Arenas, and L. M. Floría, "Evolution of cooperation in multiplex networks," *Scientific Reports*, vol. 2, no. 1, 620 pages, 2012.

[51] O. Yağan and V. Gligor, "Analysis of complex contagions in random multiplex networks," *Physical Review A*, vol. 86, no. 3, Article ID 036103, 2012.

[52] M. Berlingerio, M. Coscia, F. Giannotti, A. Monreale, and D. Pedreschi, "Multidimensional networks: foundations of structural analysis," *World Wide Web*, vol. 16, no. 5-6, pp. 567–593, 2013.