Copyright ⓒ2017 KSII

TSTE: A Time-variant Stochastic Trust Evaluation Model in Social Networks

Jingru Li[1], Li Yu[1], Jia Zhao[2], Chao Luo[2] and Jun Zheng[1]

[1] School of Electronic Information and Communications, Huazhong University of Science and Technology, Wuhan, Hubei 430074, China

[2] Wuhan Zhongyuan Electronics Group Co., Ltd., Wuhan, Hubei 430074, China

[e-mail:li1jingru@163.com; hustlyu@mail.hust.edu.cn; zhaojiakitty@163.com; lc19851205@gmail.com; junzheng@hust.edu.cn]

*Corresponding author: Li Yu

Received June 11, 2016; revised January 7, 2017; accepted March 30, 2017; published June 30, 2017

Abstract

Building appropriate trust evaluation models is an important research issue for security guarantee in social networks. Most of the existing works usually consider the trust values at the current time slot, and model trust as the stochastic variable. However, in fact, trust evolves over time, and trust is a stochastic process. In this paper, we propose a novel time-variant stochastic trust evaluation (TSTE) model, which models trust over time and captures trust evolution by a stochastic process. Based on the proposed model, we derive the time-variant bound of untrustworthy probability, which provides stochastic trust guarantee. On one hand, the time-variant trust level of each node can be measured by our model. Meanwhile, by tolerating nodes with relatively poor performance, our model can effectively improve the node resource utilization rate. Numerical simulations are conducted to verify the accuracy and consistency of the analytical bounds on distinguishing misbehaved nodes from normal ones. Moreover, simulation results on social network dataset show the tradeoff between trust level and resource utilization rate, and verify that the successful transmission rate can be improved by our model.

Keywords: Trust evaluation model, Time-variant, Stochastic trust guarantee, Social networks

This work was supported by the National Natural Science Foundation of China (NSFC) (No. 61231010), National High Technology Research and Development Program (No. 2015AA015901)

https://doi.org/10.3837/tiis.2017.06.025 **ISSN : 1976-7277**

1. Introduction

Social networks become increasingly popular as an accessible medium for people to disseminate information and connect to their friends [1]. The recent explosive development of mobile devices makes social networks ubiquitous [2-4]. With the ability to share information, social networks have even attracted enterprises and governments to exploit them for delivering services to customers and citizens [5]. The normal operation of social networks for interacting information or services in all above organizations relies on the trust level between members. Without trust guarantee, social networks will suffer from serious privacy and security crisis [2, 6-9]. In recent years, the media has reported many attack incidents of leaking users' privacy and network fraud through social networks [10]. It is thus essential and important to evaluate the trustworthiness of nodes accurately and effectively to guarantee the trust level in social networks.

Most existing works about online trust in social networks focus on the trust at the current time slot and are not concerned with trust-related state changes [4, 11-13]. The trust is updated based on the observed historical trust information. However, in fact, trust evolves over time [12, 14] and is found to be highly related to nodes' behaviors, which is dynamic. For example, in the initial period, when a fresh node is just activated, it is trustworthy with a high trust value. Later, it may suffer from the risk of malicious attacks and its trust value decreases. Then if the node starts the repair mechanism (e.g., forgetting mechanism [15]), its trust value would recover. Thus, trust is not dependent on the judgment at the current time slot only but on a long-term observation. Therefore, it is meaningful to consider the historical trust as well as the current trust to describe the overall variation of trust on the timeline. In view of this, it is necessary to model the time-evolving formulation process of trust, which helps to predict more accurately whether a node is trustworthy.

In addition, trust at each time slot is random due to many factors such as sudden external attack events and stochastic behaviors of nodes. In other words, most current models regard trust as stochastic variable and assume trust states are independent from slot to slot. In fact, according to the sociological research, trust is a stochastic process [16], and trust states at different time slots are dependent on each other.

Lastly, efficient use of energy is also an important concern in social networks. If only nodes with high trustworthiness are used, the node utilization rate will be largely decreased. Then congestion and delay will be caused to slow down the information diffusion in social networks. Therefore, when building a trust model, the tradeoff between resource utilization rate and trust level need to be achieved.

Recently, there has been a growing interest in studying how to describe the time-evolving nature of trust. Based on fluid dynamics theory, W. Jiang et al. [14] proposed a recommendation system, which aggregated opinions of multiple time slots to a final prediction, and and can improve prediction accuracy of trust based recommendation system.Based on social science theory, J. Tang et al. [12] improved prediction accuracy of online applications in social networks. X. Li et al. [17] used time fading function to describe dynamics of trust. However, none of these existing works have modeled trust as stochastic process, and considered the tradeoff between trust level and resource utilization rate.

In this paper a time-variant stochastic trust evaluation (TSTE) model is proposed, where the variation of trust on the timeline is described and trust is regarded as a stochastic process. The stochastic trust value model and the stochastic trustworthiness threshold model are proposed to derive the *upper bound of untrustworthy probability* (called *warning probability*). Based on warning probability, our model can distinguish misbehaved nodes from normal ones effectively. When warning probability of some node is low, this node can be regarded as reliable and can participate in network operations.Moreover, to establish the tradeoff between trust level and resource utilization rate, we introduce a safety threshold. In this way, some nodes with weak trust can be tolerated and have potential on information diffusion in a few cases. Intuitively, our model can improve the resource utilization rate while trust level is guaranteed, which is further verified by numerical results and simulations.

The rest of this paper proceeds as follows. In Section 2, related works on trust evaluation models are introduced. Next, network model and notions are presented in Section 3. Then our proposed TSTE model is provided in Section 4. In Section 5, the numerical calculation and the experiment results analysis are given. In Section 6, simulations are implemented on SimEvents, and the results demonstrate the effectiveness and practicability of the proposed TSTE model; Moreover, tradeoff between trust level and resource utilization rate is analyzed, and the resource utilization rate can be improved by our model. Finally, the paper is concluded in Section 7.

2. Related Work

With the increasing development of social networks, researchers have paid high attention on trust models which are important for successful social networks [5, 18-23]. By leveraging the mobility contact processes based on social network's small-world property, S. Trifunovic et al. [24] proposed explicit social trust and implicit social trust to secure user interactions. Nepal et al. [25] propose STrust, a social trust model based only on interactions within the social network. In [8], L. A. Cutillo et al. capitalized on the trust relationships to build trusted and privacy-preserving mechanisms and to defense against intruders or malicious users. Z. Li and H. Shen developed a social network aided spam filter, where an adaptive trust management scheme was established based on the additiveincrease/multiplicative-decrease algorithm (AIMD), to adjust nodes' trust values and further block emails from low-trust nodes [26]. In order to mitigate the risk of receiving untrustworthy information from mobile user in mobile social networks, F. Hao et al. [3] proposed a new fuzzy trust inference mechanism to evaluate the trust value between two mobile users. L. Li et al. [27] studied opinion dynamics in a social group and modeled the trust that may exist between like-minded agents through a trust function, which was a discontinuous non-increasing function of the opinion distance.

However, most of the existing work only considers the trust values at the current time slot, but in fact, trust evolves over time. On the time-variant or dynamic nature of trust, Y. Li et al. [15] proposed adaptive forgetting scheme to describe the dynamic decrement of trust observation results at each moment, effectively distinguishing normal nodes from malicious nodes. In [28], trust value was dynamically computed using dynamic strategies based on nodes' behaviors. In [29], trust value of the node was set to increase linearly by time $tv_i = tv_i + k$, where k is a environment parameter which can be dynamically adjusted in different network conditions. Therefore, if a node is detected as malicious by mistake, the dynamic property makes it to be used again later. Nevertheless, the existing trust evaluation models in social networks seldom consider the variation process of trust on the timeline, which can help measure trust more accurately.

What's more, various models have been proposed to measure the uncertainty of trust. One of the major examples is Bayesian system [30], where trust is defined as a conditional probability, and the unknown trust values are computed through Bayesian network analysis. In [31] authors presented entropy-based trust model and probability-based trust model to measure the uncertainty of trust. Moreover, grey theory is also suitable in dealing with uncertainty [32]. F. Zhang et al. adopted the system cloud grey model SCGM(1,1), effectively improving the precision ability on tendency prediction aspect [32]. These models lead to significant improvements in the accuracy of computed trust, as well as effectively detecting malicious behaviors. That is to say, these work regard trust as stochastic variable, but has not taken into consideration the time dependence of trust.

Thirdly, while the development of social networks and mobile devices bring convenience to people's life, it also has brought large energy consumption [33]. How to save resources as much as possible as well as guarantee the user requirements and trust level need to be taken into consideration. There is not much work on this topic, and our work has filled this gap.

Few existing research works have simultaneously considered the above points. Therefore, in this paper the TSTE model is proposed to measure trust in social networks more accurately.

3. Network Model and Notations

3.1 Network Model

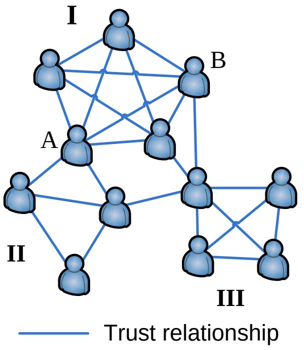


Fig. 1. A social network model

Fig. 1 illustrates an example social network, which reveals the relationship among staffs of three departments (i.e. I , II and III) in a company. The solid lines represent the trust relationship between acquainted staffs based on interaction and observation. In this paper, the standard definition of trust in computer science introduced in [5] is adopted: trust is a subjective expectation an entity has about another entity's future behavior. For clarity, here the first entity is referred to as the *subject* and the second entity as the *object*. And in the following context, they will refer to the two parties in trust relationship.

Specifically, trust values between acquainted staffs are uncertain for each time slot, since one cannot have certain assessment about another one's future behavior. The randomness of inner or external attacks also leads to the stochastic nature of trust. For different time slots on the timeline, trust between staffs evolves with time, since trust evaluation relies on observation about nodes' behaviors which can be highly dynamic. So trust is in fact a stochastic function of time and the accuracy of trust evaluation will be improved if trust on the whole timeline is taken into account.

3.2 Basic Notations

Our TSTE model adopts some expressions in stochastic network calculus [34]. The basic notations of stochastic network calculus [34, 35] involved in this paper are firstly introduced here.

(1) Function sets F and $\overline{F}$

F denotes the set of non-negative wide-sense increasing functions, or

$$F = \left\{ f(\cdot) : \forall 0 \le x \le y, f(x) \ge 0, f(x) \le f(y) \right\}, \tag{1}$$

and by $\overline{F}$ the set of non-negative wide-sense decreasing functions, or,

$$\overline{F}=\{f(\cdot):\forall 0\le x\le y, f(x)\ge 0, f(y)\le f(x)\}. \tag{2}$$

The function sets F and $\overline{F}$ are applied in *the stochastic trust value model* in Section 4.1.3, to illustrate the characteristics of the *stochastic trust value (s.t.v.)* curve $\alpha(\in F)$ and bounding function $f(\in\overline{F})$. It is necessary to use F and $\overline{F}$ herein, because the characteristics of α and f are important for explaining the physical meaning of the *stochastic trust value model.*

Similarly, to illustrate the characteristics of the *stochastic trustworthiness threshold (s.t.t.)* curve $\beta(\in F)$ and bounding function $g(\in\overline{F})$, F and $\overline{F}$ are used in *the stochastic trustworthiness threshold model* in Section 4.1.3.

Additionally, to illustrate the characteristic of $\overline{F}_X(\in\overline{F})$ and $\overline{F}_Y(\in\overline{F})$, $\overline{F}$ is used in *Lemma 1* in Section 4.1.3. The characteristic of $\overline{F}$ is necessary for deriving the conclusion of *Lemma 1*.

(2) $F_X(x)$ and $\overline{F}_X(x)$ for random variable X

For any random variable X , its distribution function, denoted by

$$F_X(x)\equiv P\{X\le x\}, \tag{3}$$

belongs to F and its complementary distribution function, denoted by

$$\overline{F}_X(x)\equiv P\{X>x\}, \tag{4}$$

belongs to $\overline{F}$.

$\overline{F}_X(x)$ is used in *Lemma 1* in Section 4.1.3, to denote the complementary distribution function of random variables X,Y and $Z=X+Y$.

(3) (min,+) convolution operation $\otimes$

The following operation will be adopted: The *(min,+) convolution* of function f and g under the (min,+) algebra [36] is defined as:

$$(f\otimes g)(t)\equiv\inf_{0\le s\le t}[f(s)+g(t-s)]. \tag{5}$$

This operation $\otimes$ is used in *Lemma 1* in Section 4.1.3, to denote the upper bound expression of the complementary distribution function of $Z = X + Y$. *Lemma 1* is the necessary condition for the proof of *Theorem 1*, which is the core of our proposed TSTE model.

In *Theorem 1*, $\otimes$ is used to denote the upper bound expression of the untrustworthy probability, $UT(s,t)$, and the lower bound expression of the trustworthy probability, $T(s,t)$. Both bound expressions are mentioned repeatedly later in the paper. The usage of $\otimes$ makes the description of the paper more simple and mathematical.

(4) Expression $A(t)$, $S(t)$, and relevant operational formulas

$A(t)$ and $S(t)$ are used to denote the cumulative amount of trust value and trustworthiness threshold in the time interval $(0,t]$, respectively. For any $0 \le s \le t$, let $A(s,t) \equiv A(t) - A(s)$ and $S(s,t) \equiv S(t) - S(s)$. By default, $A(0) = S(0) = 0$. These expressions and formulas run through the whole model in Section 4.1.3.

The above four types of functions are the mathematical bases for the model in Section 4.1.3. Adjustments in this section can make the full paper more tight and well organized.

4. Time-variant Stochastic Trust Evaluation (TSTE) Model

In this section a novel Time-variant Stochastic Trust Evaluation (TSTE) Model is proposed, as illustrated in **Fig. 2**.

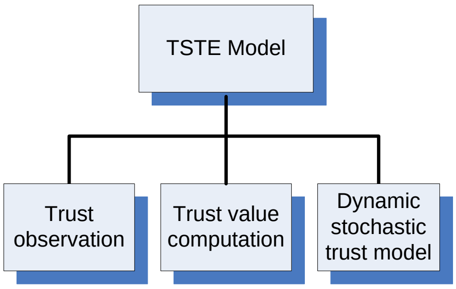


Fig. 2. TSTE Model

4.1 Trust evaluation model

Trust evaluation model is proposed to measure trust between pairs of acquaintances which have direct interaction with each other, by taking full account of the stochastic and time-variant properties of trust.

4.1.1 Trust observation (experience-based trust information collection)

In social networks, trust information can be collected for trust computation from three main sources: attitudes, behaviors, experience [5].

- *Attitudes*. Attitudes mean the positive/negative views of the subject to the object.
- *Behaviors*. Based on the object's behaviors in interaction, the subject can infer the trust degree to the object.
- *Experience*. Experience is the perception of the subject in the interaction with the object.

All the above three factors affect trust computation, however, experience affects attitudes and behaviors. Specifically, positive experiences encourage the subjects to interact frequently with the objects, leading to a change in behavior of the two parties. Moreover, they may also lead to changes in attitudes and make the subjects more receptive towards similar information about the objects. Thus, experience is chosen and collected to compute trust in social networks in this paper.

Experience can be captured by feedback mechanism [5]. Specifically, positive and negative ratings are collected and taken as the trust information. Herein α and β are used to represent the amount of positive and negative ratings respectively. In the following subsection 4.1.2, the relationship between α / β and the amount of positive/negative behaviors a / b will be given. In fact, this is a combination of attitudes and experience. Most of previous research focused on a single factor, and our method achieves a combination of two factors for holistic analysis of trust in social networks.

In order to show the computation steps of the TSTE model more clearly, we give the corresponding algorithm for each component of the model in subsection 4.1.1-4.1.3. Take the social network in the form of **Fig. 1** as an example, we compute trust of the object B over time from the view of subject A. The algorithm to collect the object B's trust information at time $t_n = n * \Delta t \left(n = 1, 2, 3 \cdots\right)$ from view of A would proceed as in Algorithm 1.

Algorithm 1 Experience-based trust information collection

Iteration:

```
for $n = 1 : M$ \* collecting the trust information of B in the $n$th time interval
  Initialization: Set the amount of B's positive behaviors observed by A: $a=0$, and the
    amount of B's negative behaviors observed by A: $b=0$.
  Based on feedback mechanism [5], observe and record if the behavior of B is normal or
    misbehaved at the node A.
  for $t = 1 : N$ do
    if A observes that B is normal behaved, then
      $a = a + 1$;
    else $b = b + 1$;
    end if
    if $t=n*\Delta t\left(n=1,2,3\cdots\right)$ then
      record and return the triple $\left\{a_n,b_n,t_n\right\}\leftarrow\left\{a,b,t\right\}$ at node A. \* used to compute B's trust
          value at time $t$ from A in Algorithm 2.
      break;
    end if
  end for
end for
Output:
  the object B's trust information at node A at time $t_n=n*\Delta t\left(n=1,2,3\cdots\right)$, i.e. the triples
$\left\{a_n,b_n,t_n\right\}\left(n=1,2,3\cdots\right)$;
```

4.1.2 Trust value computation for single time slot

Based on the experience information collected in trust observation component, trust value can be computed by Bayesian system, where positive factor α and negative factor β are taken to statistical update the beta probability density functions (PDF). Bayesian system is chosen for an important reason that beta distribution is flexible and simple to store because it is characterized by just two parameters [37]. The trust value is the probability expectation value of the beta PDF, which can be denoted by [38]

$$\mathrm{beta}\left(p\middle|\alpha,\beta\right)=\frac{\Gamma\left(\alpha+\beta\right)}{\Gamma\left(\alpha\right)\Gamma\left(\beta\right)}p^{\alpha-1}\left(1-p\right)^{\beta-1}, \tag{6}$$

where $0\leq p\leq 1,\alpha,\beta>0$.

The probability expectation value of the beta distribution is:

$$\mathrm{E}\left(p\right)=\alpha/\left(\alpha+\beta\right). \tag{7}$$

Here α and β represent the total amount of positive and negative ratings respectively. By simple analysis in [33], after observing a positive and b negative outcomes, $\alpha=a+1,\beta=b+1$, where a and b can be captured by feedback mechanism [5].

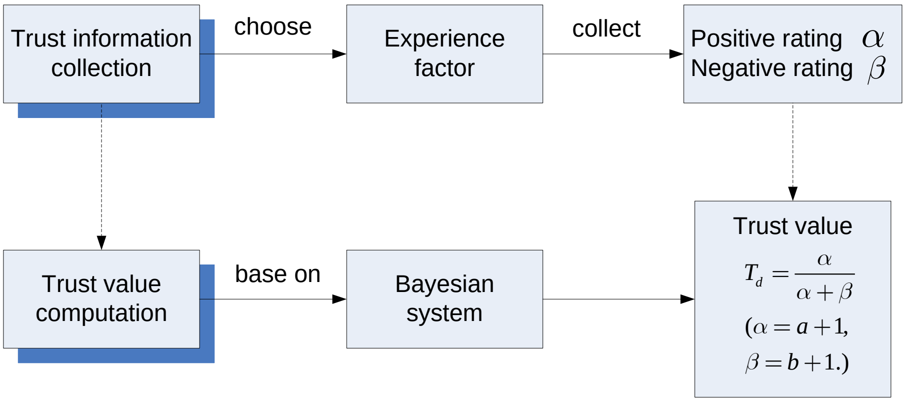
Thus the trust value is

$$t_d=\frac{a+1}{a+b+2}. \tag{8}$$

The logical relationship between Section 4.1.1 and Section 4.1.2 is clarified in **Fig. 3** as below. Based on the Bayesian system, trust value can be represented as

$$t_d=\frac{\alpha}{\alpha+\beta}=\frac{a+1}{a+b+2}.$$

In this way, the logical relationship between Section 4.1.1 and Section 4.1.2 are closely connected to each other by the medium of a and b.



* a, b represent the amount of observed outcomes, and collected in trust information collection step.

Fig. 3. Logical relationship between Section 4.1.1 and Section 4.1.2

In order to describe the dynamic influence of events on trust evaluation, forgetting scheme is introduced [15]. It is easy to understand that the influence of the old observations on current trust metrics will decrease as time goes on. Apparently, the weight of an older observation is less that that of a recent observation. The forgetting scheme is used to model this influence decreasing phenomenon. That is, performing K good actions at time t_1 is equivalent to performing $K\beta^{t_2-t_1}$ good actions at time $t_2\left(t_2 > t_1\right)$, where $\beta(0<\beta\leq 1)$ is referred to as the forgetting factor.

To integrate the forgetting scheme into our trust evaluation model, each node needs to maintain values of a and b, as well as the time t when this record was last updated, for each trust relationship. Assuming that there are Δ_a and Δ_b additional normal behaviors and misbehaviors obtained between time t_1 and t_2. Then, at time t_2, a is updated to $(a\beta^{t_2-t_1}+\Delta_a)$ and b is updated to $(b\beta^{t_2-t_1}+\Delta_b)$.

The convergence of trust values can be sped up inspired by a social phenomenon in which consistently good behavior for a long time is required to achieve a good reputation but only a few bad actions are enough to ruin it [39]. Therefore, the forgetting factor is set to be a variable related with the current trust value to achieve this fast convergence of trust value. Specifically, if t_d is the current trust value, then β can be chosen as

$$\beta = 1 - t_d, \tag{9}$$

or

$$\beta = \begin{cases} \beta_1 \; t_d \geq 0.5 \\ \beta_2 \; t_d < 0.5 \end{cases} \tag{10}$$

where $0 < \beta_1 << \beta_2 \leq 1$. In this way, the higher trust value, the lower forgetting factor, then the less influence of the historical good behaviors on current trust value; and vice versa.

The algorithm to compute trust value for single time slot is summarized in Algorithm 2.

Algorithm 2 Trust value computation algorithm for single time slot

Initialization:

Set the forgetting factor $\beta (0 < \beta \leq 1)$;

Let a_n', b_n' represent the amouts of positive and negative behaviors of B based on forgetting scheme at the time instance $t_n = n * \Delta t \left(n = 1, 2, 3 \cdots \right)$ from view of node A. Set $a_1' = a_1,\ b_1' = b_1$;

Iteration:

```
for $n = 1{:}N$ do \* compute the trust value of B at time $t_n = n * \Delta t \left( n = 1, 2, 3 \cdots \right)$
    if $n = 1$ then \* compute the trust value of B at time $t_1 = \Delta t$
        $T_{d,t_n} = \frac{a_n' + 1}{a_n' + b_n' + 2}$.
    else \* compute the trust value of B at time $t_n = n * \Delta t \left( n = 2, 3 \cdots \right)$
        $a_n' = a_{n-1}' \beta^{\Delta t} + a_n, b_n' = b_{n-1}' \beta^{\Delta t} + b_n$;
        $T_{d,t_n} = \frac{a_n' + 1}{a_n' + b_n' + 2}$.
    end if
end for
```

Output:

the object B's trust value $T_{d,t_n} \left(n = 1, 2, 3 \cdots \right)$ at the time instance $t_n = n * \Delta t \left(n = 1, 2, 3 \cdots \right)$

from view of node A.

4.1.3 Trust evaluation model on the timeline

In this part, a new trust evaluation model is proposed, where the stochastic trust function on timeline is described. From the trust function, the bounds of untrustworthy probability and trustworthy probability are derived both at a certain time slot and in a certain period, which detect and prevent both sudden and long attacks.

When the trust value of a node is computed, it will be compared with a trustworthiness threshold to identify the trustworthiness of nodes. Denote trust value as A , and trustworthiness threshold as S . Then

- when $A \geq S$, the node is regarded as trustworthy.
- when $A < S$, the node is regarded as untrustworthy.

Moreover, the reliable nodes are defined as follows.

Definition: A node is regarded as reliable, if its untrustworthy probability

$$P\{S - A > 0\} \tag{11}$$

is very low, or equivalently its trustworthy probability

$$P\{S - A \leq 0\} \tag{12}$$

is very high.

Our idea is that, provide the upper bound of the untrustworthy probability; when it is no larger than a certain threshold, the node is reliable.

The meanings of providing the upper bound of the untrustworthy probability are as follows.

- The practical meaning of the upper bound comes from security consideration: when the network wants to assign important tasks to some node, the system need to guarantee the node is well-behaved. If the untrustworthy probability is very low, then the node is very likely to be a good node, and can undertake important tasks. Thus, normal operation of the network can be ensured.
- The upper bound represents the worst case. When it is no larger than a certain threshold, the worst case can be limited, and the trust level of nodes can be guaranteed.

The modeling process for deriving the upper bound of the untrustworthy probability is as follows.

The stochastic trust value model: The cumulative trust value $A(t)$ is said to follow *stochastic trust value (s.t.v.)* curve $\alpha \in F$ with bounding function $f \in \overline{F}$, denoted by $A \sim_{stv} \langle f, \alpha \rangle$, if for all $0 \leq s \leq t$ and all $x \geq 0$,

$$P\left\{\alpha(t-s)-A(s,t)>x\right\}\leq f(x), \tag{13}$$

where $f(x)$ is generally a very small probability.

The practical meaning of (13) is that the cumulative amount of trust value, $A(t)$, is lower bounded by $\alpha(t)$. That is to say, in any time period $(s,t]$, there is a certain probability $f(x)$ such that the practical amount of cumulative trust values $A(s,t)$ is less than the stochastic lower bound $\alpha(t-s)$ for x. This can be easily understood with the aid of **Fig. 4**.

As in **Fig. 4**, the shaded part represents the area of that $\alpha(t)$ exceeds $A(t)$ in time period $(s,t]$, i.e. $\alpha(t-s)-A(s,t)$. Since $f(x)$ is generally a very small probability, then the physical interpretation of (13) is that, trust values are lower bounded by $\alpha(t)$. Therefore, (13) can meet trust guarantee requirement, since misbehavior can be limited. Thus based on the proposed trust model, network security can be at a high level and the service quality can be guaranteed.

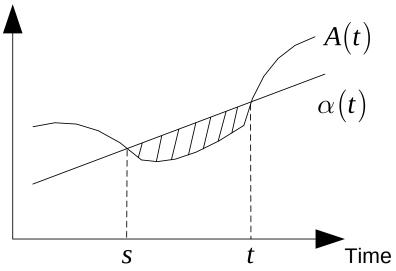


Fig. 4. Stochastic trust model

Similarly, the trustworthiness threshold is regarded as a stochastic process, as in the following dynamic stochastic trustworthiness threshold model.

The stochastic trustworthiness threshold model: The cumulative trustworthiness threshold $S(t)$ is said to follow *stochastic trustworthiness threshold (s.t.t.)* curve $\beta\in F$ with bounding function $g\in\overline{F}$, denoted by $S\sim_{stt}\langle g,\beta\rangle$, if for all $0\leq s\leq t$ and all $x\geq 0$,

$$P\left\{S(s,t)-\beta(t-s)>x\right\}\leq g(x). \tag{14}$$

In general, $g(x)$ is a very small probability, then (14) means that $\beta(t)$ is used to upper bound the actual cumulative trustworthiness threshold $S(t)$. This is because that, if the trustworthiness threshold is too high, then the number of reliable nodes is too small. This will result in heavy load on few reliable nodes and congestion will happen at these important nodes.

In above models, cumulative trust value and trustworthiness threshold are used instead of instantaneous amounts for two reasons:

- Trust models are often used in applications such as routing, which have high stability requirements. So cumulative trust value and trustworthiness threshold are used to guarantee the stability of trust measurement.
- Since trust value and trustworthiness threshold are stochastic, so trust measurement based on instantaneous amounts may be erroneous. Once misbehaved nodes are misjudged as normal nodes, then network security will be seriously threatened. In order to decrease this misjudgment, stochastic trust value and stochastic trustworthiness threshold models where cumulative amounts are built in this paper.

With a certain node, if the cumulative trust value is less than the cumulative trustworthiness threshold, i.e.

$$S(s,t) - A(s,t) > 0, \tag{15}$$

this node is *untrustworthy*. The aim of our trust evaluation model is to make sure that untrustworthy probability

$$UT(s,t) = P\{S(s,t) - A(s,t) > 0\} \tag{16}$$

is as small as possible. Equivalently, trustworthy probability in any time interval $(s,t](0 \le s \le t)$ is defined as

$$T(s,t) = 1 - UT(s,t) = 1 - P\{S(s,t) - A(s,t) > 0\}, \tag{17}$$

then it can be guaranteed that trustworthy probability is as high as possible.

When $s = 0$, $UT(0,t)$ (or $UT(t)$) and $T(0,t)$ (or $T(t)$) are respectively the untrustworthy probability and trustworthy probability at any time instant t

$$UT(t) = P\{S(t) - A(t) > 0\}, \tag{18}$$

$$T(t) = 1 - UT(t), \tag{19}$$

which are the special cases of (16) and (17). In the following sections, the general cases of (16) and (17) are discussed only.

For any trust-aware application, in order to judge whether a node is reliable or not, it makes sense to know the upper bound of untrustworthy probability $UT(s,t)$, or equivalently the lower bound of trustworthy probability $T(s,t)$.

To derive the above bounds, we begin with the following lemma [34].

Lemma 1: Assume that the complementary cumulative distribution functions (CCDF) of random variables X, Y are $\overline{F}_X \in \overline{F}$ and $\overline{F}_Y \in \overline{F}$, respectively. Assume that $\overline{F}_X(x) \le f(x)$ and $\overline{F}_Y(x) \le g(x)$. Denote $Z = X + Y$. Then no matter whether X and Y are independent or not, there holds $\forall x \ge 0$,

$$\overline{F}_Z(x) \le f \otimes g(x). \tag{20}$$

Based on this Lemma, the following Theorem can be derived.

Theorem 1: If a certain node $N_i(i=1,2,\cdots,n)$ has the cumulative trust value $A(t) \sim_{stv} \langle f, \alpha \rangle$ and the cumulative trustworthiness threshold $S(t) \sim_{stt} \langle g, \beta \rangle$, then in any time interval $(s,t](0 \le s \le t)$, the untrustworthy probability, $UT(s,t)$, is upper bounded by

$$UT(s,t) \le f \otimes g\left(\alpha(t-s) - \beta(t-s)\right); \tag{21}$$

and correspondingly, the trustworthy probability, $T(s,t)$, is lower bounded by

$$T(s,t) \ge 1 - f \otimes g\left(\alpha(t-s) - \beta(t-s)\right). \tag{22}$$

Proof:

$$S(s,t) - A(s,t) = \left[S(s,t) - \beta(t-s)\right] + \left[\alpha(t-s) - A(s,t)\right] + \left[\beta(t-s) - \alpha(t-s)\right]. \tag{23}$$

Let $B(s,t) = \left[S(s,t) - \beta(t-s)\right] + \left[\alpha(t-s) - A(s,t)\right]$, then from (13),(14) and LEMMA 1, it follows that

$$P\left\{B(s,t) > x\right\} \le f \otimes g(x). \tag{24}$$

Since

$$\begin{aligned} UT(s,t) &= P\{S(s,t)-A(s,t)>0\} \\ &= P\{B(s,t)+[\beta(t-s)-\alpha(t-s)]>0\} \\ &= P\{B(s,t)>\alpha(t-s)-\beta(t-s)\}, \end{aligned} \tag{25}$$

if $\alpha(t-s)-\beta(t-s)\geq 0$, it can be naturally derived that

$$UT(s,t)\leq f\otimes g(\alpha(t-s)-\beta(t-s)) \tag{26}$$

from (24) and (25); if $\alpha(t-s)-\beta(t-s)<0$, (26) holds trivially since $f\otimes g(y)=+\infty$ for any $y<0$ [35].

Correspondingly, the trustworthy probability, $T(s,t)$, is lower bounded by

$$\begin{aligned} T(s,t) &= 1-UT(s,t) \\ &\geq 1-f\otimes g(\alpha(t-s)-\beta(t-s)). \end{aligned} \tag{27}$$

Therefore *Theorem 1* follows. ■

Herein, the upper bound of untrustworthy probability, $f\otimes g(\alpha(t-s)-\beta(t-s))$, is named as *warning probability*, and the lower bound of trustworthy probability is named as *confidence probability*.

The larger the warning probability, the more likely that a node is malicious; on the contrary, it is more likely to be well-behaved. Therefore, malicious nodes can be distinguished from normal nodes by comparing their warning probabilities.

Further, the *safety threshold* f_o is introduced to identify the reliability of nodes and adjust the tradeoff between trust level and resource utilization rate.

- According to the practical demand on security level, set the *safety threshold* f_o. When the warning probability is no larger than the safety threshold, i.e.

$$f\otimes g(\alpha(t-s)-\beta(t-s))\leq f_0, \tag{28}$$

the node can be regarded as reliable. Thus basic trust level can be guaranteed.

- The nodes with untrustworthy probability $P\{S-A>0\}>0$ are permitted for network operations, instead of only using nodes with $P\{S-A>0\}=0$. Then the scope of reliable nodes is extended, and the resource utilization rate can be improved.

In conclusion, our model can simultaneously meet the requirements of ensuring the basic safety demand and improving the resources utilization rate in social networks. According to the actual security needs, select the appropriate f_o, then the appropriate tradeoff can be achieved.

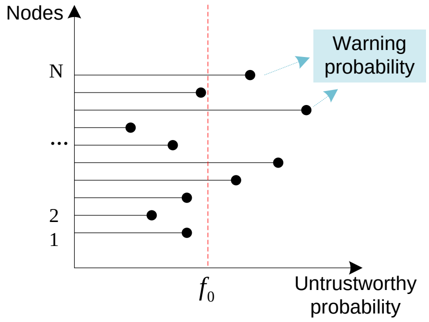


Fig. 5. Illustration graph for our trust evaluation method

As in **Fig. 5**, the x-axis represents the untrustworthy probabilities for each node, and the right-side endpoint of each horizontal line represents the warning probability for each node. For a fixed f_o, when the warning probability is on the left side of f_o, i.e. no larger than f_o, these nodes are reliable; otherwise, the nodes are unreliable. The less f_o, the fewer the reliable nodes, and the higher the trust level in the network; and vice versa.

The less f_o, the higher the requirement on security, or equivalently the lower the tolerance level. So f_o is defined as a measure of *tolerance level*. Then the physical meaning of (28) is that, in the time interval $(s,t]$ or at the time instance t (when $s=0$), when the warning probability of a node $f \otimes g\left(\alpha(t-s)-\beta(t-s)\right)$ is no larger than f_o, the node is reliable. The lower f_o, the higher the requirement on security, the fewer reliable nodes in the network.

Algorithm 3 shows our algorithm for trust evaluation on the timeline.

Algorithm 3 Trust evaluation algorithm on the timeline for TSTE model

Initialization:

According to the practical demand on security level, set the *safety threshold* f_o.

1.Compute the cumulative trust value in the time interval $(0,t_N]$: $A(t_N)=\sum_{n=1}^{N} T_{d,t_n}$;

and the cumulative trustworthiness threshold in the time interval $\left(0,t_N\right]$: $S\left(t_N\right)=\sum_{n=1}^{N}s_{t_n}$, where s_{t_n} represents the trustworthiness threshold at the time instance t_n=$n*\Delta t\left(n=1,2,3\cdots\right)$.

2. According to *the stochastic trust value model* in the paper, derive the *stochastic trust value (s.t.v.)* curve $\alpha\left(t\right)$ and the *bounding function* $f\left(x\right)$;
3. According to *the stochastic trustworthiness threshold model* in the paper, derive the *stochastic trustworthiness threshold (s.t.t.)* curve $\beta\left(t\right)$ and the *bounding function* $g\left(x\right)$;
4. According to Theorem 1, derive that in any time interval $\left(s,t\right]\left(0\le s\le t\right)$,

   the upper bound of the untrustworthy probability $UT\left(s,t\right)$, i.e. the *warning probability* is $f\otimes g\left(\alpha\left(t-s\right)-\beta\left(t-s\right)\right)$;

   and the lower bound of the trustworthy probability $T\left(s,t\right)$, i.e. the *confidence probability* is $1-f\otimes g\left(\alpha\left(t-s\right)-\beta\left(t-s\right)\right)$.

   And when $s=0,t=t_N$, the upper bound of the untrustworthy probability $UT\left(t_N\right)$, i.e. the *warning probability* is $f\otimes g\left(\alpha\left(t_N\right)-\beta\left(t_N\right)\right)$;

   and the lower bound of the trustworthy probability $T\left(t_N\right)$, i.e. the *confidence probability* is $1-f\otimes g\left(\alpha\left(t_N\right)-\beta\left(t_N\right)\right)$;
5. Warning probability represents the worst case that the object node may be malicious. And malicious nodes can be distinguished from normal nodes by comparing their warning probabilities.
6. Furthermore, the warning probability is compared with the *safety threshold* f_o to identify the reliability of the object node. When the warning probability is no larger than the safety threshold, the node can be regarded as reliable. Thus basic trust level can be guaranteed.

4.2 Discussion on applications and significance

The proposed trust evaluation model provides the following basic guidance in trust-aware applications in social networks:

- Based on the above TSTE model, the warning probability that a subject node on any other object node can be evaluated in a social network. For a certain time instance, the warning probabilities for all object nodes can be listed and ranked. Then the malicious nodes may be detected by selecting the top- N nodes. In addition, malicious nodes can be clearly distinguished from normal ones based on the variation trend of the evolution curve of warning probability on the timeline.
- Based on the proposed trust evaluation model, the trust values of a node over a time period can be showed, making up the defect of only considering the current trust values. Thus some attacks like on-off attack [32, 40] can be resisted, because given overall performance of nodes, temporary good performance of attackers will not confuse us.
- Based on the proposed model, grading trustworthiness measurement service can be provided. According to the practical demand on security level, set the appropriate safety threshold f_o. Then the reliability of nodes can be measured for different businesses.
- Tradeoff between trust level and resource utilization rate can be achieved by choosing adaptive f_o in our model.

5. Numerical Results and Analysis

5.1 On-Off Trust Value Model

Trust values of nodes alternate between high level and low level, due to various trust events which either increase or decrease trust values [41]. In the output view, trust value of any node has two states, i.e. on state (trustworthy) and off state (untrustworthy) for most simplified case. Therefore, cumulative trust value $A(t)$ for each one-hop neighbor can be regarded as two-state/on-off Markov chain [41,42], where we assume that the transition rate from on state to off state is λ and the transition rate from off state to on state is μ as in **Fig. 6**. Normal nodes and misbehaving nodes are different in transition rates.

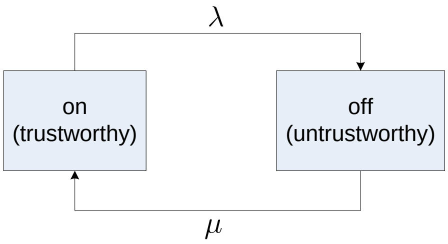


Fig. 6. On-off Markov trust value model

It is not difficult to understand that the cumulative trust value $A(t)$ has stationary increments, i.e. the increment of cumulative trust value over a time period is only related to the time interval, but independent of the initial trust value. For on-off trust value model, while there is little (approximated as zero for simplification) cumulation when the Markov chain is in off state, the cumulative process has a constant rate h when the chain is in on state.

Based on the derivation in [42], the on-off trust value process has a stochastic trust value curve

$$\alpha(t)=\rho(\theta)\cdot t \tag{29}$$

where

$$\rho(\theta)=\frac{1}{2\theta}\left(\theta h+\lambda+\mu-\sqrt{(\theta h-\lambda+\mu)^2+4\lambda\mu}\right), \tag{30}$$

with bounding function

$$f(x)=e^{-\theta x}, \quad \forall\theta>0. \tag{31}$$

5.2 Deterministic Trustworthiness Threshold Model

For the trustworthiness threshold model, the simplest case is considered, i.e. trustworthiness threshold is constant, which is assumed to be c . Then the cumulative trustworthiness threshold will be $S(t)=ct$, which is also chosen as the d.s.t.t. curve, then

$$\beta(t)=ct, \tag{32}$$

with bounding function

$$g(x)=0. \tag{33}$$

Since the actual cumulative trustworthiness threshold $S(t)$ is equal to $\beta(t)$, so according to (14), the probability that $S(t)$ exceeds $\beta(t)$ is zero, i.e. $g(x)=0$.

5.3 Warning Probability and Confidence Probability

According to the above results, since $g(x)=0$, then in any time interval $(s,t]\,(0\le s\le t)$, the untrustworthy probability, $UT(s,t)$, is upper bounded by

$$\begin{aligned} UT(s,t) &= P\left\{S(s,t) - A(s,t) > 0\right\} \\ &\leq f\left(\alpha(t-s) - \beta(t-s)\right), \end{aligned} \tag{34}$$

and the trustworthy probability, $T(s,t)$, is lower bounded by

$$\begin{aligned} T(s,t) &= 1 - UT(s,t) \\ &\geq 1 - f\left(\alpha(t-s) - \beta(t-s)\right). \end{aligned} \tag{35}$$

where $\alpha(t), f(x), \beta(t)$ are derived from results in section 5.1 and 5.2.

5.4 Experiment Results and Analysis

Table 1. Parameters table

Parameters	Normal node	On-off attacker
h (cumulation rate of trust values in on state)	0.88	0.27
λ (transition rate from on state to off state)	0.4	0.7
μ (transition rate from off state to on state)	0.6	0.2
c (trustworthiness threshold)	0.2	0.2
$e^{-\theta\left(\left[\rho(\theta)t-ct\right]\right)}$ (warning probability)	$e^{-0.1338t}$	$e^{-0.0086t}$
$1-e^{-\theta\left(\left[\rho(\theta)t-ct\right]\right)}$ (confidence probability)	$1-e^{-0.1338t}$	$1-e^{-0.0086t}$

For example, in an online social network, a user hopes to detect the malicious users with a certain warning probability, or equivalently determine the warning probability that a user is an attacker. Then by ranking and comparing the warning probabilities, the malicious nodes can be filtered. In order to verify our trust model, the warning probabilities and confidence probabilities of the normal node are compared with those of the on-off attacker. The parameters adopted in this case study are shown in **Table 1**.

The reasons that the parameters in **Table 1** are set as such are shown as follows:

(1) h (cumulation rate of trust values in on state):

① Trust process is stochastic process, and trust value evolves over time. Then, h (cumulation rate of trust values in on state) can be equivalent to the average of the trust values in on state on the whole timeline.

② For on-off trust value model, there is little cumulation when the Markov chain is in off state [37]. Then we can assume that, the cumulation rate of trust values in off state is approximated as zero. Thus it can be inferred that, h (cumulation rate of trust values in on state) can be equivalent to the average of the trust values on the whole timeline.

③ In this numerical experiment, in order to verify the effectiveness of our model more clearly, two types of nodes with typical behaviors are chosen as experiment objects.

To make the numerical experiment more realistic, we take the parameters of h based on the data in the simulation in Section 6.1. Specifically, the node represented by the top curve in **Fig. 9** is chosen as the normal node, whose normal behaviors far exceed its misbehaviors. While the node represented by the bottom curve in **Fig. 9** is chosen as the on-off attacker, whose misbehaviors far exceed its normal behaviors. In the simulation, the average trust value of this normal node and on-off attacker are around 0.9 and 0.3 respectively on the timeline. Since trust value is stochastic, random values are taken around these two average trust values (0.9 and 0.3) for more realistic numerical experiment. As a result, we take 0.88 and 0.27 respectively as the parameters of h for two nodes in the numerical experiment in Section 5.4.

(2) λ (transition rate from on state to off state) and μ (transition rate from off state to on state):

The transition rate from on state to off state λ for normal node is lower than that for on-off attacker. The reason is that, normal node behaves well for most of time and rarely misbehaves; and on the contrary for on-off attacker. Similarly, the transition rate from off state to on state μ for normal node is higher than that for on-off attacker. Specifically, based on the work in [44, 45], the transition probabilities of the Markov chain can be estimated. And a set of experience values are set for the parameters in our numerical experiment.

(3) c (trustworthiness threshold):

The same trustworthiness threshold is chosen for both nodes to ensure the same baseline. A lower trustworthiness threshold is set to make more nodes reliable. With relaxed constraints, more candidates would be joined and regarded as trustworthy nodes for transmission. Thus the network can be fully used and the practicability of networks can be improved. In Section 6.2 later in the paper, tradeoff between trust level and resource utilization rate of network has been studied. Higher utilizaiton rate is hoped to be achieved at a high trust level. To ensure the consistency of the paper, herein parameters are set to improve resource utilizaiton rate.

(4) $e^{-\theta([\rho(\theta)t-ct])}$ (warning probability) and $1-e^{-\theta([\rho(\theta)t-ct])}$ (confidence probability):

These two parameters are evaluated based on the above parameters. Specifically,

① for the normal node, $\rho(\theta)=0.3338$ according to the equation (30) in Section 5.1. Then,

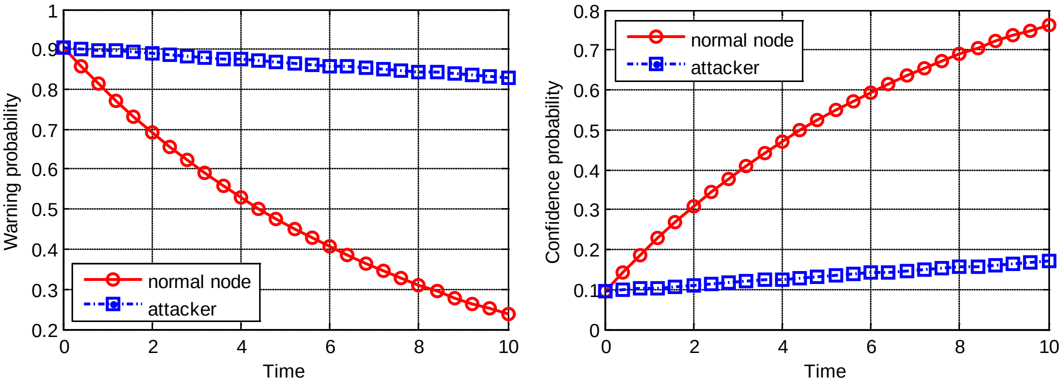
$e^{-\theta([\rho(\theta)t-ct])}=e^{-(0.3338t-0.2t)}=e^{-0.1338t}$, and $1-e^{-\theta([\rho(\theta)t-ct])}=1-e^{-0.1338t}$.

② for the on-off attacker, $\rho(\theta)=0.2086$ according to the equation (30) in Section 5.1. Then,

$e^{-\theta([\rho(\theta)t-ct])}=e^{-(0.2086t-0.2t)}=e^{-0.0086t}$, and $1-e^{-\theta([\rho(\theta)t-ct])}=1-e^{-0.0086t}$.

Fig. 7 shows the relationship of warning probability with time. It can be seen that the warning probabilities of normal node and on-off attacker both decrease with time, yet the former one decreases much faster.

As in **Fig. 7(a)**, as time goes on, warning probabilities of both normal node and on-off attacker decrease. This is because in social networks users can obtain more and more acquaintance with others through their close friends in the same community. Then as time goes on, trustworthiness for other nodes will increase. However, due to their more malicious behaviors, the warning probability of the attacker decreases rather slowly. Although confidence probability is the complementarily of warning probability, it still shows valuable result. As in **Fig. 7(b)**, confidence probability of normal node increases quickly over time, which indicates that with our trust evaluation model, normal node can be distinguished efficiently from attacker.



(a) (b)

Fig. 7. Variation of warning probability and confidence probability with time (a) Variation of warning probability with time; (b) Variation of confidence probability with time

5.5 The Consistency of Numerical and Simulation Results

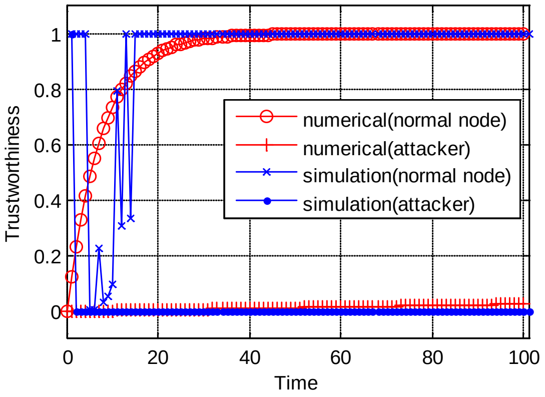


Fig. 8. Comparison of numerical and simulation results for trustworthiness of normal node and attacker

Herein the confidence probability is regarded as the trustworthiness of nodes. **Fig. 8** presents the numerical and simulation results. The upper two curves depict the trustworthiness of normal nodes. It can be seen that, as time goes on, trustworthiness rises to high level gradually for both curves. The numerical curve rises smoothly, while the simulation curve changes with fluctuations, which is normal for stochastic simulation experiment. Nevertheless, the variation trends of two curves are consistent. The below two curves describe the trustworthiness of attackers. They both increase slowly, showing low trust level. Moreover, both curves are close to each other, verifying the consistency of numerical and simulation results.

From the above analysis, the practicability of the TSTE model can be demonstrated.

6. Performance evaluation

In this section, the proposed TSTE model is analyzed by conducting a set of simulations in a social network. Through simulation results, the efficiency in measuring trustworthiness is demonstrated by adopting the TSTE model.

6.1 Distinguish normal nodes from misbehaved nodes

In this section, the simulation is implemented using SimEvents, which provides a discrete-event simulation engine and component library. We construct a social network, where the member nodes are set with different behaviors with time labels. A subject node is chosen, and the trust value processes and warning probabilities of other nodes in the network can be evaluated based on our TSTE model. In the simulations, trust values with Beta distribution are computed, and two important parameters, a and b, are used to denote the magnitude of normal behaviors misbehaviors respectively. Six typical object nodes with different behavior performance are picked out, and their stochastic trust value processes are given as in **Fig. 9**. It can be seen from these figures that, the more the number of normal behaviors exceeds that of misbehaviors, the higher the trust values are.

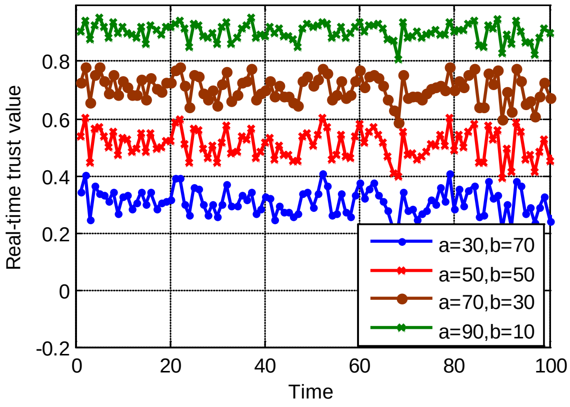


Fig. 9. Trust value processes

The warning probability curves with time evolution for six object nodes are plotted in **Fig. 10**. It can be seen that, when observing the overall evolution of warning probabilities on the timeline in **Fig. 10**, attacker nodes can be clearly distinguished from normal ones.

- ♦ Node 1 represents the typical malicious node, where the number of normal behaviors is fewer than that of misbehaviors, i.e. $a < b$ (the top curve). According to the previous theoretical model, the warning probability will be very high. One of the important reasons is that, a mass of bad behaviors would ruin the trust. In the simulation result, warning probability remains stable to 1. That is to say, based on the TSTE model, the misbehaved nodes can be rapidly and clearly identified by the warning probability.
- ♦ Nodes 3 to 6 represent typical normal nodes, for which the number of normal behaviors exceeds that of misbehaviors, i.e. $a > b$ (the bottom four curves). From the theoretical model, nodes would have low warning probability. While in simulation results, the warning probabilities drop rapidly to 0. Thus, it can be seen that, our model is able to fast and efficiently recognize normal nodes.
- ♦ For the neutral node 2, i.e. the number of normal behaviors is approximately equal to that of misbehaviors (the top second curve). Based on the trust value equation and the social phenomenon in which consistent and lasting good behavior is required to achieve a good reputation but a few bad actions are enough to ruin it. This type of node would have higher warning probability than obviously well-behaved nodes (i.e. the bottom four curves). The top second curve gradually declines and forms a boundary between normal nodes and malicious nodes.

This is the reason why trust is measured as an evolution process on the timeline, i.e. our model can accurately and clearly distinguish normal and misbehaved nodes apart with rapid convergence.

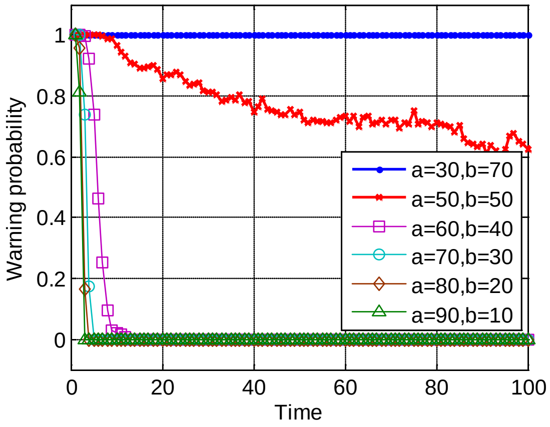


Fig. 10. Warning probability curves

From **Fig. 10**, another important observation can be obtained. Simulation results are consistent with the numerical results from the perspective of changing trend of warning probabilities. As time goes on, warning probability of normal nodes show faster decline rate than that of misbehaved ones. The decrement of warning probability means the improvement of trust level. Then normal nodes can be distinctly identified from misbehaved ones with time passing. It can be seen from simulation results that, the better nodes behave, the lower warning probability is.

Furthermore, the simulation in this subsection is representative to real-world social networks from the following aspects.

- The simulation platform SimEvents accords with the feature of real-world social networks, where trust information is observed and collected based on discrete events.
- In the simulation we construct a social network, where the member nodes are set with different behaviors with time labels. And the situation is the same in real-world social networks composed of member nodes with different behaviors with time labels.
- In the simulation, the magnitude of normal behaviors misbehaviors of object nodes, a and b, are collected to compute trust values for object nodes. In real-world social networks, also the same information is collected to compute trust value.
- In the stochastic trust value processes given in the simulation, the more the number of normal behaviors exceeds that of misbehaviors, the higher the trust values are. And in real-world social networks, if we observe more positive behaviors than negative behaviors about other people, we will make a decision that they are more likely trustworthy. And furthermore, the similar results would be obtained as in **Fig. 10** in real-world social networks.

6.2 Simulations on MIT social network dataset

We conduct the simulation experiments on MIT Reality Mining data set [43], which records user interaction data on 104 Nokia 6600 cellphone over 9 months by Reality Mining project of MIT Media Lab. In this paper, the Bluetooth interaction data is used, including encounter frequency and time period among users, and 94 effective user data are selected for our experiment.

6.2.1 Analysis on the tradeoff of security level and utilization rate

The *node utilization rate* is defined as the ratio of reliable nodes in the network. And the overall *security level* is defined as the mean of confidence probabilities of reliable nodes in the network.

Then the relationship between security level and utilization rate for several fixed time are shown as follows.

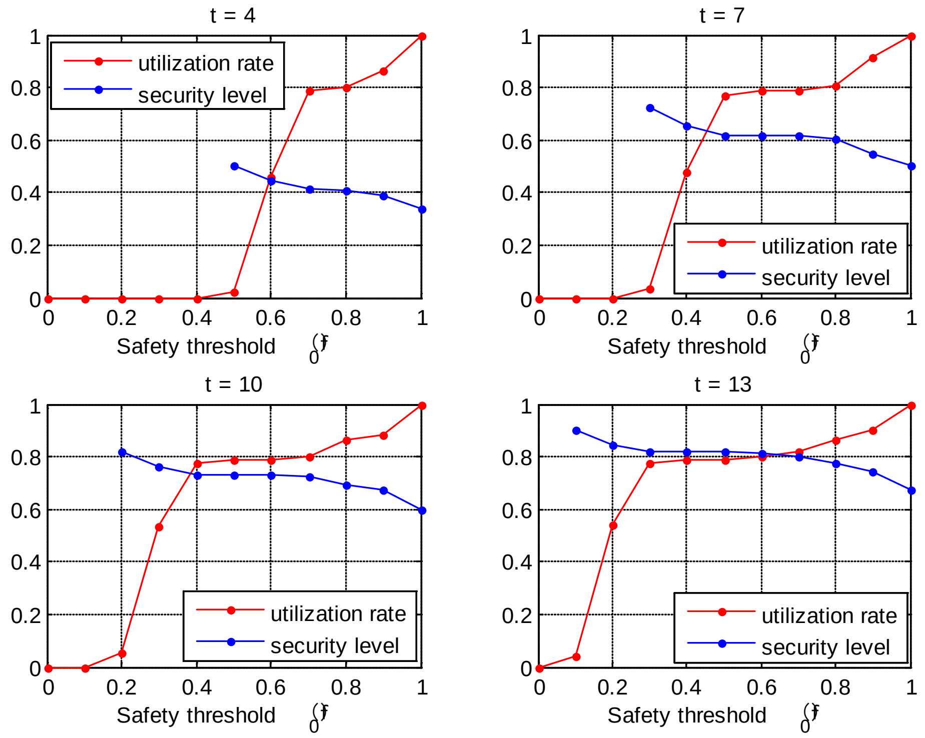


Fig. 11. Tradeoff of security level and utilization rate

Fig. 11 shows the variation of security level and node utilization rate as f_o increases in different time slots. We have the following observations:

- The higher the security level, the lower the node utilization rate. And the security level and the node utilization rate can be balanced by adjusting the safety threshold f_o.
- At each moment, with the increase of f_o, node utilization rate increases, the network security level drops. This is because, when f_o increases, network security level requirement is lower, the number of reliable nodes is larger, and the average confidence probability will reduce. When utilization rate is 0, the corresponding part of security level curve does not exist. The reason is that, according to the definition of security level, when utilization rate is 0, there is no reliable node, then security level cannot be defined and computed.
- As time goes on, utilization rate increases rapidly (i.e., for the same f_o, utilization rate becomes higher and higher), and security level is rising. The reason is that, as time goes on,

more and more trust information is collected, and the overall confidence probabilities of nodes are increased. Thus, the security level is higher and higher, and the number of reliable nodes increases.

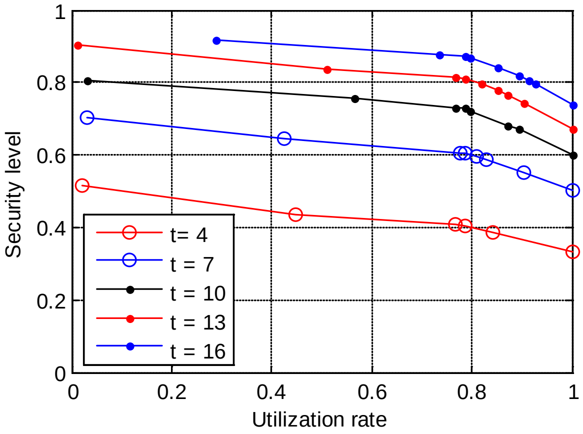


Fig. 12. Tradeoff of security level and utilization rate for different time t

The tradeoff between security level and node utilization rate in different time is shown in **Fig. 12**.

- Overall, for each moment, when utilization rate increases, security level decreases. For fixed utilization rate, security level increases with time passing. This is because, the overall security level increases with the increase of confidence probabilities of nodes.
- In the tradeoff between security level and node utilization rate, another phenomenon is that, the front part is almost flat, and the subsequent curve falls more obviously. For instance, at the time instant $t=13$, when the utilization rate is from 0 to 0.8, security level reduces not that much; however, in the latter part, the utilization rate increases by only 0.2, but at the sacrifice of more security level. It is visible that, the point of utilization rate 0.8 is relatively optimal. Moreover, there exists an inflection point (near utilization rate = 0.8) on each tradeoff curve corresponding to each time instance. Before the inflection point, security level nearly keeps still with the increase of utilization rate; while after the inflection point, security level decreases much sharper. The meaning of inflection point is that, at this point, both security level and utilization rate can be achieved as high as possible. Each (utilization rate, security level) binary pair corresponds to a f_o. Then the inflection point can be applied as follows. Set f_o as the f_o value corresponding to the inflection point. Use our model to implement trust evaluation, then the optimal tradeoff between security level and utilization rate can be achieved, and network resource can be used fully at high trust level.

6.2.2 Improvement on successful transmission rate based on our method

The experimental setting is as follows. At each moment, according to our method, it can be identified if each node is available (1 or 0), and a sequence can be obtained as:

$$T = [t_1\, t_2 \cdots t_N], \tag{36}$$

where

$$t_i = \begin{cases} 1, & \text{if node } i \text{ is identified as reliable,} \\ 0, & \text{if node } i \text{ is identified as unreliable.} \end{cases} \tag{37}$$

And then reliability identification matrix $\mathbf{T}$ between any two nodes can be obtained as follows,

$$\mathbf{T} = [t_{ij}], \tag{38}$$

where

$$t_{ij} = \begin{cases} 1, \text{if node } j \text{ is identified as reliable for node } i, \\ 0, \text{if node } j \text{ is identified as unreliable for node } i. \end{cases} \tag{39}$$

Assume the adjacent matrix of the network is denoted by $\mathbf{A}$. Then the matrix $\mathbf{A} * \mathbf{T}$ represents *adjacent and reliable matrix*.

$$(\mathbf{A} * \mathbf{T})_{ij} = \begin{cases} 1, & \text{if node } j \text{ is linked with } i \text{ and reliable to } i, \\ 0, & \text{otherwise.} \end{cases} \tag{40}$$

When the node M is connected to the node N, and node N is reliable for node M, i.e. $(\mathbf{A} * \mathbf{T})_{MN} = 1$, data can be transmitted reliably from M to N.

Compared with our model, the baseline model is used as follows: firstly, compute instantaneous trust values; then, at each moment when it exceeds the trustworthiness threshold, the node will be identified as reliable.

We define a *connected and reliable route* as a route on which any following node is linked and reliable for the previous node. Given any source node and destination node, if there exists any connected and reliable route between these two nodes, data packets can be successfully transmitted from source to destination node.

As in **Fig. 13**, based on our model and baseline model, *successful transmission rate* (called *STR* in short) at each moment can be obtained by repeating 1000 random experiments. Moreover, the average *STR* based on each method are computed in **Table 2**.

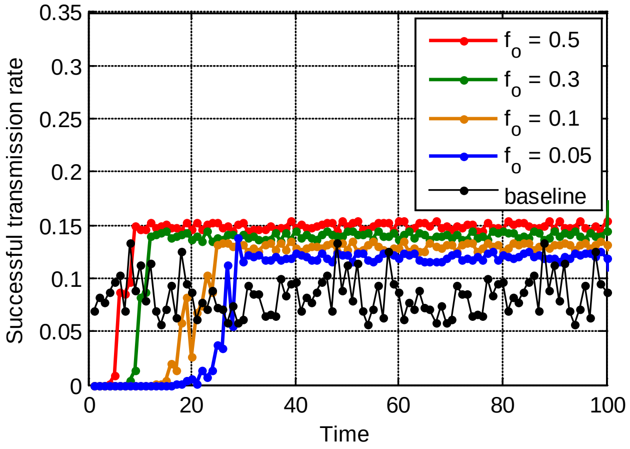


Fig. 13. Comparison with baseline model

Table 2. Average successful transmission rate

Our TSTE model				**Baseline model**
$f_0 = 0.5$	$f_0 = 0.3$	$f_0 = 0.1$	$f_0 = 0.05$	
0.1493	0.1382	0.1305	0.1190	0.0847

The following analysis results can be obtained:

- As a whole, our model outperforms the baseline model in *STR* in the long-term experiment results. In details, the average *STR* based on our model are higher than those of baseline model in **Table 2**. This can verify the advantage of our model, i.e. our model can improve *STR*.
- Based on our model, *STR* is relatively lower in the initial period and shows its advantage after a short period. This is because, in our model a period of trust accumulation is needed to accurately measure the trust levels of nodes. This means sacrificing time for high *STR*. Therefore, our model is suitable for the situation of high security and *STR* requirements but loose delay requirement.
- For each f_o in our model, *STR* increases from 0 to a stable value. This is because, our model is based on cumulative measurement over a period. In the initial period, there are no observed and evaluation results to identify reliable nodes. Then there are few routes on which data can be successfully transmitted, and consequently *STR* is low. With the passage of time, the more trust data are, the more the reliable nodes are, then the higher *STR*. Finally, over a period of accumulation, reliable nodes can be stably identified, so *STR* keeps stable.
- The higher f_o is, the faster *STR* increases, and the higher the final stable value is. This is because, the higher f_o, the higher the tolerance of network on the nodes reliability, and the

more reliable nodes. Then the higher *STR*.

- ◆ f_o=0.1 and 0.05 represent high security levels. In this case, *STR* stable values are still higher than those of baseline model. This can verify the practicality and advantage of our model.
- ◆ Compared with our model, *STR* based on the baseline model fluctuates more obviously. The reason is that, the baseline is based on instantaneous trust values, while our trust model is based on the cumulative trust values, then the stability of trust evaluation can be ensured.

In general, the following conclusions can be obtained through **Fig. 13**:

- ◆ In stable state, higher *STR* can be obtained based on our model.
- ◆ our model is suitable for the situation of high security and *STR* requirements but loose delay requirement.
- ◆ When f_o is very small, which means high security levels, higher *STR* still can be obtained based on our model. This can verify the practicality of our model.

The MIT Reality Mining dataset used in this subsection is collected from a real-world social network. All the above evaluations on the experiment metrics are based on this dataset. Hence, the simulation in this subsection is representative to the real-world social network.

Our model is not only suitable for small social networks, and is also scalable for a large social network for two main reasons as follows.

(1) Based on the proposed TSTE model, we evaluate trust between every pair of adjacent nodes (i.e. nodes which have direct interaction with each other) in social networks. This belongs to the distributed algorithm, and does not involve the evaluation between nonadjacent nodes. The distributed algorithm is suitable for large scale networks.

(2) Each node need to have the following abilities:

① certain memory space to save the amounts of positive/negative behaviors and trust value of neighbor node at each time instance.

② certain computing power to compute the trust values of object nodes.

In the current age, high storage and computing power are available for computers or nodes.

Thus our proposed model applies to social networks with any scale, including the large social networks.

7. Conclusion

In this paper, trust is first regarded as a stochastic process, and a time-variant stochastic trust evaluation model is proposed, in which a stochastic trust function is given. Stochastic trust value and trustworthiness threshold models are presented. Bounds of untrustworthy and trustworthy probability are derived and used to judge the reliability of each node. In the numerical calculation, on-off Markov process is used to represent trust value variation process, and experiment results show that our model can distinguish normal nodes from misbehaved nodes effectively. Moreover, the consistency of numerical and simulation results verifies the practicability of our TSTE model. Several simulations are implemented with SimEvents, further confirming the effectiveness of the proposed TSTE model. Finally, simulation on a real social network dataset shows the tradeoff between trust level and resource utilization rate, and verifies that the successful transmission rate can be improved by our model.

References

[1] H. Hu, Jin. Guo, J. Chen, "Modeling online social networks based on preferential linking," *Chinese Physics B*, vol. 21, no. 11, pp. 118902, 2012. Article (CrossRef Link).

[2] R. Lu, X. Lin, Z. Shi, J. Shao, "Plam: A privacy-preserving framework for local-area mobile social networks," *INFOCOM*, pp. 763–771, 2014. Article (CrossRef Link).

[3] F. Hao, G. Min, M. Lin, C. Luo, L. Yang, "Mobifuzzytrust: An efficient fuzzy trust inference mechanism in mobile social networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 11, pp. 2944–2955, 2014. Article (CrossRef Link).

[4] X. Liang, X. Lin, X. Shen, "Enabling trustworthy service evaluation in service-oriented mobile social networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 310–320, 2014. Article (CrossRef Link).

[5] W. Sherchan, S. Nepal, C. Paris, "A survey of trust in social networks," *ACM Computing Surveys (CSUR)*, vol. 45, no. 4, pp. 47, 2013. Article (CrossRef Link).

[6] M. Sirivianos, K. Kim, X. Yang, "Socialfilter: Introducing social trust to collaborative spam mitigation," *INFOCOM*, pp. 2300–2308, 2011. Article (CrossRef Link).

[7] G. Wang, F. Musau, S. Guo, M. Abdullahi, "Neighbor similarity trust against sybil attack in p2p e-commerce," *IEEE Transactions on Parallel and Distributed Systems*, pp. 1, 2014. Article (CrossRef Link).

[8] L. Cutillo, R. Molva, T. Strufe, "Safebook: A privacy-preserving online social network leveraging on real-life trust," *IEEE Communications Magazine*, vol. 47, no. 12, pp. 94–101, 2009. Article (CrossRef Link).

[9] R. Gross, A. Acquisti, "Information revelation and privacy in online social networks," in *Proc. of ACM CONFERENCE of the 2005 ACM Workshop on Privacy in the Electronic Society, WPES '05*, pp. 71–80, 2005. Article (CrossRef Link)

[10] A. L. Young, A. Quan-Haase, "Information revelation and internet privacy concerns on social network sites: A case study of facebook," in *Proc. of ACM CONFERENCE of the Fourth International Conference on Communities and Technologies*, pp. 265–274, 2009. Article (CrossRef Link).

[11] G. Liu, Q. Yang, H. Wang, X. Lin, M. Wittie, "Assessment of multi-hop interpersonal trust in social networks by three-valued subjective logic," *INFOCOM*, pp. 1698–1706, 2014. Article (CrossRef Link).

[12] J. Tang, H. Gao, H. Liu, A. Das Sarma, "etrust: Understanding trust evolution in an online world," in *Proc. of ACM Proceedings of the 18th ACM SIGKDD international conference on Knowledge discovery and data mining*, pp. 253–261, 2012. Article (CrossRef Link).

[13] Tavakolifard, M., Almeroth, K.C., "Social computing: an intersection of recommender systems, trust/reputation systems, and social networks," *IEEE Network*, vol. 26, no. 4, pp. 53–58, 2012. Article (CrossRef Link).

[14] W. Jiang, J. Wu, G. Wang, H. Zheng, "Fluidrating: A time-evolving rating scheme in trust-based recommendation systems using fluid dynamics," *INFOCOM*, pp. 1707–1715, 2014. Article (CrossRef Link).

[15] L. Yu, J. Li, Z. Liu, "Semiring trust model based on adaptive forgetting scheme," *Journal of Electronics and Information Technology*, vol. 33, no. 1, pp. 175–179, 2011. (in Chinese). Article (CrossRef Link).

[16] D. Khodyakov, "Trust as a process a three-dimensional approach," *Sociology*, vol. 41, no. 1, pp. 115–132, 2007. Article (CrossRef Link).

[17] X. Li, F. Zhou, X. Yang, "Scalable feedback aggregating (sfa) overlay for large-scale p2p trust management," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 10, pp. 1944–1957, 2012. Article (CrossRef Link).

[18] V. Arnaboldi, M. L. Gala, A. Passarella, M. Conti, "The role of trusted relationships on content spread in distributed online social networks," in *Proc. of The Second Workshop on Large Scale Distributed Virtual Environments on Clouds and P2P (LSDVE 2014)*, 2014. Article (CrossRef Link).

[19] X. Chen and L. Wang, "A Cloud-Based Trust Management Framework for Vehicular Social Networks," in *Proc. of IEEE Access*, vol. 5, no. , pp. 2967-2980, 2017. Article (CrossRef Link).

[20] W. Jiang, J. Wu, F. Li, G. Wang and H. Zheng, "Trust Evaluation in Online Social Networks Using Generalized Network Flow," *IEEE Transactions on Computers*, vol. 65, no. 3, pp. 952-963, March 1 2016. Article (CrossRef Link).

[21] C. Huang, Z. Yan, N. Li and M. Wang, "Secure Pervasive Social Communications Based on Trust in a Distributed Way," *IEEE Access*, vol. 4, pp. 9225-9238, 2016. Article (CrossRef Link).

[22] Z. Yan and M. Wang, "Protect Pervasive Social Networking Based on Two-Dimensional Trust Levels," *IEEE Systems Journal*, vol. 11, no. 1, pp. 207-218, March 2017. Article (CrossRef Link).

[23] V. Sharma; I. You; R. Kumar; P. Kim, "Computational offloading for efficient trust management in pervasive online social networks using osmotic computing," *IEEE Access* , vol.PP, no.99, pp.1-1, 2017. Article (CrossRef Link).

[24] S. Trifunovic, F. Legendre, C. Anastasiades, "Social trust in opportunistic networks," in *Proc. of INFOCOM IEEE Conference on Computer Communications Workshops*, pp. 1–6, 2010. Article (CrossRef Link).

[25] S. Nepal, W. Sherchan, C. Paris, "Strust: a trust model for social networks," in *Proc. of IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 841–846, 2011. Article (CrossRef Link).

[26] Z. Li, H. Shen, "Soap: A social network aided personalized and effective spam filter to clean your e-mail box," *INFOCOM*, pp. 1835–1843, 2011. Article (CrossRef Link).

[27] L. Li, A. Scaglione, A. Swami, Q. Zhao, "Consensus, polarization and clustering of opinions in social networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 6, pp. 1072–1083, 2013. Article (CrossRef Link).

[28] F. Liu, X. Li, Y. Ding, H. Zhao, X. Liu, Y. Ma, B. Tang, "A social network-based trust-aware propagation model for p2p systems," *Knowledge-Based Systems*, vol. 41, pp. 8–15, 2013. Article (CrossRef Link).

[29] G. Han, J. Jiang, L. Shu, J. Niu, H.-C. Chao, "Management and applications of trust in wireless sensor networks: A survey," *Journal of Computer and System Sciences*, vol. 80, no. 3, pp. 602–617, 2014. Article (CrossRef Link).

[30] L. V. Orman, "Bayesian inference in trust networks," *ACM Transactions on Management Information Systems (TMIS)*, vol. 4, no. 2, pp. 7, 2013. Article (CrossRef Link).

[31] Y. L. Sun, W. Yu, Z. Han, K. R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 305–317, 2006. Article (CrossRef Link).

[32] F. Zhang, Z.-P. Jia, H. Xia, X. Li, H.-M. Sha Edwin, "Node trust evaluation in mobile ad hoc networks based on multi-dimensional fuzzy and markov scgm (1, 1) model," *Computer Communications*, vol. 35, no. 5, pp. 589–596, 2012. Article (CrossRef Link).

[33] L. Zhao, J. Cai, H. Zhang, "Radio-efficient adaptive modulation and coding: green communication perspective," in *Proc. of IEEE 73rd Vehicular Technology Conference (VTC Spring)*, pp. 1–5, 2011. Article (CrossRef Link).

[34] Y. Jiang, Y. Liu, "Stochastic network calculus," *Springer*, 2008.

[35] Y. Jiang, "A basic stochastic network calculus," *ACM SIGCOMM Computer Communication Review*, Vol. 36, pp. 123–134, 2006. Article (CrossRef Link).

[36] J.-Y. Le Boudec, P. Thiran, "Network calculus: a theory of deterministic queuing systems for the internet," *Springer*, Vol. 2050, 2001. Article (CrossRef Link).

[37] J. Li, R. Li, J. Kato, "Future trust management framework for mobile ad hoc networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 108–114, 2008. Article (CrossRef Link).

[38] A. Josang, R. Ismail, C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision support systems*, vol. 43, no. 2, pp. 618–644, 2007. Article (CrossRef Link).

[39] H. Yu, Z. Shen, C. Miao, C. Leung, D. Niyato, "A survey of trust and reputation management systems in wireless communications," in *Proc. of the IEEE*, vol. 98, no. 10, pp. 1755–1772, 2010. Article (CrossRef Link).

[40] Y. L. Sun, Z. Han, K. R. Liu, "Defense of trust management vulnerabilities in distributed networks," *IEEE Communications Magazine*, vol. 46, no. 2, pp. 112–119, 2008. Article (CrossRef Link).

[41] B.-J. Chang, S.-L. Kuo, "Markov chain trust model for trust-value analysis and key management in distributed multicast manets," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 4, pp.

1846–1863, 2009. Article (CrossRef Link).

[42] Y. Jiang, "A note on applying stochastic network calculus," in *Proc. of SIGCOMM*, Vol. 10, pp. 16-20, May, 2010. Article (CrossRef Link).

[43] A. Pentland, N. Eagle, D. Lazer, "Inferring social network structure using mobile phone data," in *Proc. of the National Academy of Sciences (PNAS)*, vol. 106, no. 36, pp. 15274–15278, 2009. Article (CrossRef Link).

[44] N. Welton, A. Ades, "Estimation of markov chain transition probabilities and rates from fully and partially observed data: uncertainty propagation, evidence synthesis, and model calibration," *Medical Decision Making*, vol. 25, no.6, pp. 633-645, 2005. Article (CrossRef Link).

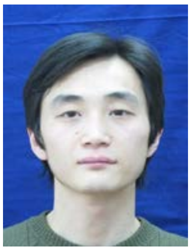
[45] B. Craig, P. Sendi, "Estimation of the transition matrix of a discrete-time Markov chain," *Health Economics*, vol. 11, no.1, pp. 33-42, 2002. Article (CrossRef Link).

Jingru Li received the B.S. degree from the School of Electronic Information and Communications, Huazhong University of Science and Technology, Wuhan, China, in 2009, and is currently pursuing the PH.D. degree in the School of Electronic Information and Communications, Huazhong University of Science and Technology, Wuhan, China. Her current research interests include social networks and trust evaluation models.

Li Yu received the B.S. and Ph.D. degrees from Huazhong University of Science and Technology, Wuhan, China, in 1992 and 1999, respectively. Currently, she is a Professor with and the Director of the Multimedia and Communication Network Center, School of Electronic Information and Communications, Huazhong University of Science and Technology

Zhaojia received the B.S. and Ph.D. degrees from Huazhong University of Science and Technology, Wuhan, Hubei, China, in 2009 and 2016, repectively. She is currently a researcher in ZYE Corporation. Her research interests include social networks and MANETs

Chao Luo received the B.S. and M.S. degrees from the School of Information and Engineering, Wuhan University of Technology, Wuhan, China, in 2007 and 2010, respectively, and received the PH.D. degree in the School of Electronic Information and Communications, Huazhong University of Science and Technology, Wuhan, China. His research interests include wireless Ad hoc networks and network performance analysis



Jun Zheng received the B.S. and M.S. degrees from the College of Physical Science and Technology, Huazhong Normal University, Wuhan, China, in 2002 and 2006, respectively, and is currently pursuing the PH.D. degree in the School of Electronic Information and Communications, Huazhong University of Science and Technology, Wuhan, China. His current research interests include performance evaluation and modeling of cognitive radio networks