International Journal of Security and Its Applications
Vol.9, No.10 (2015), pp.361-372
http://dx.doi.org/10.14257/ijsia.2015.9.10.33

Node Trust Assessment and Prediction in Mobile Ad Hoc Networks

Shaojie Zhou[1], Hui Xia[2, 3, 4]

1. School of Measurement-Control Technology and Communications Engineering, Harbin University of Science and Technology, Harbin 150080, China
2. Postdoctoral Research Station of System Science, Qingdao University, Qingdao 266071, China
3. Shandong Provincial Key Laboratory of Software Engineering, Ji'nan 250101, China
4. College of Information Engineering, Qingdao University, Qingdao 266071, China
zhoushaojie1001@163.com; *xiahui@sdu.edu.cn*

Abstract

There is an inherent reliance on collaboration among the participants of mobile ad hoc networks in order to achieve the aimed functionalities. Collaboration is productive only if all participants operate in an honest manner. However, this is not always the case and these networks are subjected to a variety of malicious attacks. One of the key factors to ensure high communication quality is an efficient assessment scheme for node's prediction trust, to choose potential cooperative nodes and reduce the probability of risk occurrence for next interaction. In this paper, firstly we propose a node's trust assessment model based on node's historical behaviors, in which the trust decision factors include the subjective reputation and indirect reputation. Then we try to combine an improved grey model with the Markov chain together to effectively predict the node's trust. Experiment has been conducted to evaluate the effectiveness of the proposed mechanism.

Keywords: *ad hoc network; malicious attack; prediction trust; trust assessment; improved grey model; Markov chain*

1. Introduction

A mobile ad hoc network (MANET) is a set of limited range wireless nodes. Due to self-organizing and rapid deployment capability, this network can be applied to different applications including battlefield communications, emergency relief scenarios, public meetings and other security-sensitive computing environments. There is an inherent reliance on collaboration among the participants of MANETs in order to achieve the aimed functionalities. Collaboration is productive only if all participants operate in an honest manner. However, this is not always the case and the MANETs are subjected to a variety of attacks by malicious nodes in particular for attacks on the packet routing. Security is critical for such networks when nodes are deployed in hostile environments, and security concerns remain a serious impediment to widespread adoption of these wireless networks. Currently, attacks on ad hoc routing come from both the exterior networks and the interior nodes. The exterior attacks are always taken by nodes outside the network through injecting erroneous route messages, replaying invalid route messages and so on. The interior attacks are usually caused by the internal nodes which have compromised to the malicious nodes in the network by behaving badly, abruptly or arbitrarily. Trust management mechanism is an effective method to solve the above

ISSN: 1738-9976 IJSIA

mentioned problems, which can also enhance the security of the whole network effectively. Most of the current trust assessment methods proposed in such mechanisms mainly focus on how to obtain an accurate node's trust value, researches on the environmental impact attributes of trust and calculate the weights of those attributes.

In human sociology, risk can be defined as the uncertainty of loss, the consequences of uncertainty and the negative deviation from the expected target. In network environment, risk can defined as poor transport state, e.g., bigger packet loss rate, link failure. Obviously, risk also exists in the network interaction, especially when the malicious nodes exist in the network. For example, when the requested (transmitter) node receives a packet transmission request, it is hard for the requesting node to evaluate whether the requested node is willing to provide the service or not. If the trend of events can be predicted accurately, the probability of risk occurrence can be reduced. And, one of the key factors to ensure high communication quality is an efficient assessment scheme for node's prediction trust and to choose cooperative potential nodes, to reduce the probability of risk occurrence for next interaction. Trust prediction, an abstract psychological cognitive process, is one of the most complex concepts in social relationships, involving factors such as assumptions, expectations and behaviors. All above makes it very difficult to quantify and forecast trust accurately. Moreover, there is no enough and efficient work proposed for trust prediction.

Due to the complexity of trust concept, it is very hard to establish an effective model to predict its value for the next or the future time interval, especially combing with the incomplete trust assessment information, uncertainty small samples and a lack of experience. Grey theory is suitable in dealing with the above conditions. The focal point of the grey system theory involves using a finite amount of available information to build a grey model [1] (GM) in order to approximate the dynamic behavior of a system. This theory has good ability to deal with small sample and information shortage of the index series, through data mining technique to get the change rules of the index. Some references use this theory to solve some problems in ad hoc network. The essential of grey model is that exponential curve is used to fit original trust value, and geometry graph of the results is a smooth curve. However, it is not very good to fit for the heavy random fluctuate data sequences. Trust value is a dynamic character value, and time series data have biggish volatility, leading to the change trend is non-stationary stochastic process, so pure grey theory is not suitable for solving this problem. Markov chain is a kind of stochastic process without after effect, which describes the stochastic phenomenon: probability distribution of the future state has nothing to do with the past states. In Markov chain, state transition probability [2] is used to reflect influence degree of the stochastic factors. Therefore, we can apply Markov chain to make time original series data that have biggish stochastic volatility precise. Moreover, we introduce the method of fuzzy clustering to make a reasonable way in state division of Markov matrix.

In this paper, we focus on the security issues in MANETs. Firstly, we propose a new node trust assessment model based on node's historical behaviors, in which the trust decision factors include the subjective reputation and indirect reputation. Then we try to combine an improved grey model with the Markov chain together to effectively predict the node's trust. Experiment has been conducted to evaluate the effectiveness of the proposed prediction mechanism.

2. Related Work

The authors [3] focus on computational trust frameworks based on the 'beta' probability distribution, the principle of exponential decay and derive a precise analytical formula for the estimation error they induce, via using hidden Markov models to represent principal behaviors. This new mechanism allows potential adopters of beta-based computational trust frameworks and algorithms to better understand the implications of their choice.

Based on interactive Markov chains (IMC), the measurement of performance feature besides function feature is introduced [4]. In the expected behavior description, the function expectation is described through a model of transition system and the performance expectation is described through relating path probability indicating dependability to the time expectation in which a certain specific behavior function is achieved.

In reference [5], the authors propose a new statistical predictive model of trust based on the well-known methodologies of the Markov model and Local Learning technique. Repeatedly appearing similar subsequences in the trust time series constructed from history of direct interactions or recommended trust values collected from intermediaries over a sequence of time slots are clustered into regime. Each regime is learnt by a local model called as local expert. The time series is then modeled as a coarse-grain transition network of regimes by using a Markov process and value of the trust at any future time is predicted by selecting the local expert with the help of the Markov matrix.

A distributed trust model G-Trust is proposed [6] to resolve the inaccurate information problem, in which the grey system theory is adopted. In G-Trust, in order to guide the agent to utilize the recommendation from witnesses reasonably and avoid the negative impact from all kinds of inaccurate factors, a mechanism is designed to rate the witnesses recommendation action, and the grey fixed weight clustering approach is used to determine the trust to witnesses.

Based on the theories of fuzzy recognition with feedback, SCGM(1,1) model and Markov chain, Zhang et al. [7] present a pattern of prediction making. The analysis and experimental computation show that this scheme is efficient in trust prediction for ad hoc networks.

A new approach is proposed in paper [8] for bootstrapping trust of Web services in which the interactions of a Web service with a user are observed during a certain time frame. The observations sequence is modeled as a hidden Markov model and matched against pre-defined trust patterns in order to assess the behavior of such Web service. The pre-defined trust patterns are specifications of possible behaviors of Web services such as trusted, malicious, betraying, oscillating, and redemptive.

Considering a requested (transmitter) node's historical trust value and its capability of providing services, we proposed a new method [9] to predict the node's trust value, based on the fuzzy logic rules prediction mechanism. The new method offers an accurate prediction of future behaviors, which obviously can reduce the probability of risk occurrence for next interaction.

3. Trust Model

Managing trust in a distributed mobile ad hoc network is challenging when collaboration or cooperation is critical to achieving mission and system goals such as reliability, availability, scalability, and re-configurability.

3.1. Trust Definition

The concept of trust in MANETs can be used to measure an expectation or uncertainty that a mobile node has about another's future behaviors. Before confirming the trust of neighbor node' behavior, we need to define key attributes which should reflect the behavior characteristics of the node well, in order to make the trust assessment objective and efficient.

3.2. Trust Model Assumption

In our trust model, passive acknowledgement is used as the main observable factor for assessing trust. Passive acknowledgement uses promiscuous mode to monitor neighbors' behaviors in the wireless radio channel, which allows a node to detect any transmitted

packet in its communication range, irrelevant of their destinations [7, 9]. We make the following assumptions: (1) Assume each node should be able to detect behavior exhibited by malicious nodes indicative of Sybil attacks. Distributed IDSs can fulfill this requirement as every node possesses an IDS and can detect attacks from other nodes in its radio range; (2) The malicious node drops packet occasionally rather than invariably; In our model, at time t, $TV(t)$ denotes for a node's trust, which is defined in a continuous range between 0 and 1 (i.e., $0 \leq TV_{ij}(t) \leq 1$). Let v_i and v_j represent the monitoring and monitored nodes, respectively.

3.3. Node Trust Assessment

We set a monitoring interval Δt, an evaluating node begins to monitor its neighbor node when its neighbor node sends a packet to the next hop, to observe whether this neighbor node normally deals with the packet. After each interaction, node *j* checks whether the neighbor *k* forwards the packet correctly. Any evaluating node who receives reputation exchange packets (*REP*, Reputation Exchange Packet) sent by other nodes, it will firstly evaluate the trust value of the sending nodes. It will accept the updating information only if it believes in those sending node, and then it updates trust value and indirect observation (*IR*, Indirect Reputation, it obtains from exchanging the experience information with corresponding nodes) in its own trust table.

3.3.1. Trust Derivation: The node's trust value '*TV*' could be calculated according to the following formula:

$$TV = w_1 * SR + w_2 * IR \quad (w_1+w_2=1 \text{ and } w_1 > w_2) \tag{1}$$

Where w_1 and w_2 separately denote for the weight values of *SR* (Subjective Reputation) and *IR* (Indirect Reputation), usually the value of w_1 is greater than w_2, which is used to prevent the enemy's malicious slander. Each node in our model additionally owns a trust table with items defined as follows.

Table 1. Node v_1's Trust Table

Nb	T_{in}	SR_{in}	IR_{in}	T_{out}	SR_{out}	IR_{out}	ΔR^t	*Black-list*
v_2	0.90	0.92	0.85	0.92	0.95	0.85	0.1	*No*
v_3	0.79	0.88	0.58	0.23	0.4	0.17	0.1	*Yes*

In each row of the table, *Nb* denotes node v_1's neighbor that can communicate with v_1 via a single-hop. T_{in} is the trust value that the neighbor node gets about node v_1; SR_{in} is the subjective reputation that the neighbor node gets about node v_1; IR_{in} is the indirect reputation that the neighbor node gets about node v_1; T_{out} is the trust value that node v_1 has about the neighbor; SR_{out} is the subjective reputation that node v_1 has about the neighbor; IR_{out} is the indirect reputation that node v_1 has about the neighbor; ΔR^t denotes for the deviation threshold; *Black-List* indicates whether v_1 considers this neighbor as a malicious node (e.g., the black-list trust threshold η as discussed in Table 1 is set to 0.3 in this example).

3.3.2 Calculation of SR: Each node initials the subjective reputation *SR* of its neighbor node to be 0.7 (e.g., according to Table 1), and then updates this value by monitoring its neighbor node's behaviors. The sender places itself in promiscuous mode after the transmission of any packet so as to overhear the retransmission by the forwarding node. Using this method, a node can know whether the packet which has been sent to its neighbor is indeed forwarded or not. Firstly the monitoring node would keep a copy of the transmission packet in its cache when its neighbor transmits this packet. If it receives a report for the correct transmission, it will remove the copy from its cache, otherwise if an error happens, the copy will be still kept its cache during a monitoring interval (Δt). We

start monitoring from the first error package, in an interval ΔT, if the number of error packages is smaller than L, this phenomenon is thought to be normal, the reason can be regarded as normal network congestion, environmental influence, and other congestion problems. We think that the node has aggressive behavior if this number of error packages is bigger than L. The phenomenon is thought to be abnormal and the punishment rate is bigger than the reward rate (It hints that the trust obtains hardly while it loses easily.)

The normal phenomenon: in a time interval ΔT, the number of error packets is smaller than the threshold L, it will have a linear increment in SR. After each normal time interval, it adds a *changevalue1* to SR, according to the following formula:

$$SR = SR + ChangeValue1 \tag{2}$$

The abnormal phenomenon: in a time interval ΔT, the number of error packets is bigger than the threshold L. There will have an exponential decrement in SR accompanied with n.

$$SR = SR - ChangValue2 * 2^{n-1} \tag{3}$$

Where n represent for the penalty coefficient. For instance, if the error packets are 3 times bigger than L, then the value of n is set to 3. *Changevalue2* should be appropriately bigger than *Changevalue1*, if the number of error packets is smaller than L in an interval ΔT, then we will re-count the number of error packets in the next interval. The values of ΔT and L depend on the current network conditions and packet transmission capacity. The value of L depends on the actual environment situation, if the value is too big, the attacker node is possible to intentionally make L-1 error packets; if the value is too small, the penalty coefficient will be too large to make a reasonable attenuation in SR.

3.3.3. Calculation of IR: IR is the indirect reputation which node obtains from other nodes while they exchange trust information with each others. Each node initializes the value IR of its neighbor nodes to be 0.7, the update rate to this value is related with the supplier's trust value TV, greater trust value with higher update rate. The value of IR updates in two ways: triggered update and periodical update. ΔR^t denotes for the deviation threshold.

Triggered update: if the change of trust value exceeds a threshold ΔR (via SR or IR changes), the node will broadcast the change information within three hops for saving the energy. This method requires an field ΔR adding to the reputation table which is used to describe the changes of reputation (i.e., 'trust'), $\Delta R = \Sigma \Delta R_i$ (i.e., ΔR_i represents the change value of the ith time). If the value of ΔR exceeds a certain threshold ΔR^t, the node will broadcast a packet *REP*. After broadcasting this packet, the value of ΔR is set to be 0. Those nodes who receive the *REP* packet will update their own value of IR corresponding to the nodes appeared in the packet by the following formula:

$$IR_{ik} = IR_{ik} + \Delta R * TV_{ij} \tag{4}$$

i represents the evaluating node, j represents the third party node, k represents the evaluated node. TV_{ij} represents the trust value of node j evaluated by node i.

Periodical update: all nodes periodically broadcast the information which is included in their own trust list. A node updates the value of IR corresponding to other nodes using the following formula:

$$IR_{ik} = IR_{ik} + \frac{\sum_{j=1, j\neq i, j\neq k}^{n} (TV_{jk} - IR_{ik}) * TV_{ij}}{n} \tag{5}$$

n represents the number of received different packets.

Each node, based upon its personal experiences, rewards collaborative nodes for their benevolent behaviors and punishes malicious nodes for their malevolent actions. To minimize the risk of transmission failure, nodes should interact with the trusted ones whose trust value is above the trust requirements of packets.

3.4. Node Trust Prediction

Trust prediction, an abstract psychological cognitive process, is one of the most complex concepts in social relationships, involving factors such as assumptions, expectations and behaviors. Due to the inherent characteristics of MANETs, it is hard for a monitoring node to assess whether the monitored node is trustworthy or not (e.g., willing to provide a requesting service or not). If the trend of the above events can be predicted accurately, the probability of risk occurrence can be eliminated or reduced.

3.4.1. Unbiased Grey Model GM(1,1): For the purpose of reducing or eliminating the bias that existed in the conventional GM(1,1) model [10, 11], the unbiased grey model is introduced to fit those statistical data.

For a special data sequence:

$$X^{(0)} = \{x^{(0)}(1), x^{(0)}(2), x^{(0)}(3), ..., x^{(0)}(n)\} \tag{6}$$

$$where\ x^{(0)}(i) > 0,\ i=1,2,...,n$$

We can firstly compute the values of grey parameters (a and b) based on the conventional grey model, and then obtain the values of unbiased grey parameters via the following equation:

$$\alpha = \ln\frac{2-a}{2+a},\ \beta = \frac{2b}{2+a} \tag{7}$$

Then the unbiased grey model is constructed:

$$\hat{x}^{(0)}(k) = \begin{cases} x^{(0)}(1) & (k=1) \\ \beta e^{\alpha(k-1)} & (k=2,3,...,n) \end{cases} \tag{8}$$

And the relative error is:

$$\varepsilon^{(0)}(k) = (x^{(0)}(k) - \hat{x}^{(0)}(k)) / x^{(0)}(k) \quad (k = 0,1,2\text{L}) \tag{9}$$

Where, if $\varepsilon^{(0)}(k)$ <0.2, which denotes for that the above equation can pass the relative error testing, and the model is suitable for the prediction application; Moreover, if $\varepsilon^{(0)}(k)$ <0.1, the model will have a superior predictive performance.

3.4.2. State Division based on Fuzzy Clustering: The change trend of nodes' trust value is a non-stationary stochastic process. Different state of time series has its special boundary. In this subsection, we will introduce the method of fuzzy clustering to deal with this question. Take state division, namely cluster center m_i as benchmark and then we can obtain several strip regions which parallel to m_i curve. Moreover, each strip region denotes for a state. The detail of this process is described as follows:

Firstly, we should suppose $\varepsilon^{(0)}(k)$ as interval division samples which can be classified by some categories. Our new method is shown as follows:

1. Determine a reasonable number of clustering groups C, and Initialize each clustering centers according to C;

2. Repeat the followed calculation until the degree of all samples' membership is stable.

Get the membership degree of the current clustering center via performing the following equation:

$$\mu_i\left[\varepsilon^{(0)}(k)\right] = \left(1 \Big/ \left\|\varepsilon^{(0)}(k) - m_j\right\|^2\right) \Big/ \sum_{\lambda=1}^{i}\left(1 \Big/ \left\|\varepsilon^{(0)}(k) - m_\lambda\right\|^2\right) \tag{10}$$

Calculate each cluster center with current membership degree function iteratively via equation (14):

$$m_j = \sum_{j=1}^{n}\left(\mu_i\left[\varepsilon^{(0)}(k)\right]^2 \varepsilon^{(0)}(k)\right) \Big/ \sum_{j=1}^{n}\mu_i\left[\varepsilon^{(0)}(k)\right]^2 \tag{11}$$

3. Classify each sample into different clustering groups according to the obtained cluster center via step 1 and 2. The samples in the same clustering group belong to a same Markov state, named as E_i and the corresponding cluster center is m_i.

3.4.3. Markov Transition Probability Matrix: Markov chain [2] refers to the random process $X(k)$, whose state only related to the state at the moment t_0 and nothing to do with the past states.

1. In Markov chain $\{x_n, n \in T\}$, let $P_{ij} = P\{x_{m+K} = j \mid x_m = i\}$, $(i, j \in I)$ represents for the probability of the system changing its state from i (at the moment m) to j (at the moment $m+k$). Take $P_{ij}^{(k)}$ in order and construct the transition probability matrix:

$$P^{(k)} = \begin{bmatrix} P_{11}^{(k)} & P_{12}^{(k)} & \cdots & P_{1n}^{(k)} \\ P_{21}^{(k)} & P_{22}^{(k)} & \cdots & P_{2n}^{(k)} \\ \vdots & \vdots & \vdots & \vdots \\ P_{n1}^{(k)} & P_{n2}^{(k)} & \cdots & P_{nn}^{(k)} \end{bmatrix} \tag{12}$$

Any state in the system will be certainly transferred into one of listed states via k-steps in a row, so $\sum_{j=1}^{n} P_{ij}^{(k)} = 1$. This matrix is also called k-steps transition probability matrix of Markov chain. Thus, corresponding with the above subsection, the probability of data sequence from state E_i to state E_j by m-steps transition is called m-steps transition probability and is recorded as:

$$P_{ij}^{(k)} = \frac{m_{ij}^{(k)}}{M_i} \tag{13}$$

Where $m_{ij}^{(k)}$ is the number of state E_i transferred into state E_j by m-steps; and M_j is the number of the appearance of state E_i. However, when calculating the number of M_j, the last k data must be deleted.

2. In the terms of the distance from the to the prediction time, the transition steps are defined as 1-step, 2-steps,..., j-steps, respectively. Combining with the corresponding transition probability matrixes, the row vectors of the initial states are the probability of each state appearing, and then the sum of transition probability can be calculated [12].

3. Determine the future state with the greatest sum of transition probability. Then we can obtain the most possible relative error $\hat{\varepsilon}^{(0)}(k+1) = m_i$ (i.e., as mentioned above, the error prediction value is equal to the benchmark of cluster center m_i).

4. After the relative error $\hat{\varepsilon}^{(0)}(k+1)$ determining, $\hat{x}^{(0)}(k+1)$ is also determined. Thus, the prediction value of the original data sequence $y(i)$ can also be obtained according to the definition of relative error.

$$\hat{y}(k+1) = \left[1 + \hat{\varepsilon}^{(0)}(k+1)/100\%\right] / \hat{x}^{(0)}(k+1) \tag{14}$$

4. Trust Assessment and Prediction in Simulation

In this section, a practical example is given, and demonstrates the validity of the improved grey Markov prediction method in this paper. NS-2 simulator (Version 2.35) [13] is used to evaluate the performance of these routing protocols in different conditions. The Distributed Coordination Function (DCF) of IEEE 802.11 for wireless LANs is adopted as the MAC layer protocol. We take an un-slotted Carrier Sense Multiple Access protocol with Collision Avoidance (CSMA/CA) to transmit data packets as well routing packets. Within a rectangular field of 1000m×1000m, we dispersed nodes randomly whose transmission radius of every node in one hop is fixed at 250m. The weight for trust decision factors would be set according to the setting: w1=0.7 and w2=0.3, that is the

subjective reputation is considered more important than the indirect reputation. We collected 20 sets of data from the simulation process.

Original node's trust value of different time series is used to construct patterns and clusters in the case of the improved gray Markov prediction model. According to the trust assessment model and the GM(1,1) model in Section III, we can obtain the original node's trust value, the prediction value of GM(1,1) and the data of relative error listed in the following table 2 and 3:

Table 2. The Results of Node's Trust via Using the Trust Assessment Model

Seq. No.	*Subjective Reputation*	*Indirect Reputation*	*Original Trust Value*
1	0.7061	0.7258	0.7155
2	0.7223	0.7047	0.7131
3	0.7117	0.6946	0.7057
4	0.7212	0.7029	0.7101
5	0.7036	0.7453	0.7262
6	0.7268	0.7562	0.7441
7	0.7332	0.7631	0.7599
8	0.6999	0.7418	0.7149
9	0.7923	0.7379	0.7771
10	0.7824	0.8127	0.7992
11	0.8293	0.8002	0.8144
12	0.7896	0.8327	0.8036
13	0.7944	0.8011	0.7960
14	0.8264	0.7992	0.8088
15	0.8244	0.8477	0.8310
16	0.8323	0.8239	0.8311
17	0.8364	0.8572	0.8458
18	0.8694	0.5877	0.8255
19	0.8233	0.8424	0.8310
20	0.8523	0.8273	0.8471

Table 3. The Results of Node's Trust via Using GM (1, 1) Model and the Relative Error

Original Trust Value	*GM(1,1) Fitting Value*	*Relative Error %*
0.7155	0.7034	-1.69
0.7131	0.7109	-0.31
0.7057	0.7185	1.82
0.7101	0.7261	2.25
0.7262	0.7339	1.05
0.7441	0.7417	0.33
0.7599	0.7496	-1.35
0.7149	0.7576	5.97
0.7771	0.7657	-1.47
0.7992	0.7739	-3.17
0.8144	0.7821	-3.96
0.8036	0.7904	-1.63
0.7960	0.7989	0.36
0.8088	0.8074	-0.18
0.8310	0.8160	-1.81
0.8311	0.8247	-0.77
0.8458	0.8335	-1.46
0.8255	0.8424	2.04
0.8310	0.8514	2.45
0.8471	0.8604	1.58

Then calculate the cluster center based on the fuzzy clustering mentioned in Section 3, and divide the relative error into five clustering groups, shown in table 4.

Table 4. The Cluster Center of Each State (%)

State	E_1	E_2	E_3	E_4	E_5
Cluster Center	-3.70	-1.59	-0.25	1.83	5.64

According to the criterion of five cluster centers, we can determine the state of each relative error which is showed in following table 5.

Table 5. State of Each Relative Error

Sequence No.	1	2	3	4	5
State	E_2	E_3	E_4	E_4	E_3
Sequence No.	6	7	8	9	10
State	E_3	E_2	E_5	E_2	E_1
Sequence No.	11	12	13	14	15
State	E_1	E_2	E_3	E_3	E_2
Sequence No.	16	17	18	19	20
State	E_3	E_2	E_4	E_4	E_4

Based on the Table 5 and Section 3, we can establish the Markov Transition Probability Matrix.

$$P^{(1)}=\begin{bmatrix} 1/2 & 1/2 & 0 & 0 & 0 \\ 1/6 & 0 & 3/6 & 1/6 & 1/6 \\ 0 & 3/6 & 2/6 & 1/6 & 0 \\ 0 & 0 & 1/4 & 3/4 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix} \quad P^{(2)}=\begin{bmatrix} 0 & 1/2 & 1/2 & 0 & 0 \\ 1/6 & 2/6 & 1/6 & 2/6 & 0 \\ 0 & 2/6 & 2/6 & 1/6 & 1/6 \\ 0 & 0 & 2/3 & 1/3 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$P^{(3)}=\begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1/6 & 2/6 & 0 & 3/6 & 0 \\ 0 & 2/6 & 2/6 & 1/6 & 1/6 \\ 0 & 1/2 & 1/2 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix} \quad P^{(4)}=\begin{bmatrix} 0 & 1/2 & 1/2 & 0 & 0 \\ 1/5 & 1/5 & 2/5 & 1/5 & 0 \\ 0 & 2/6 & 2/6 & 1/6 & 1/6 \\ 0 & 1/2 & 1/2 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Choose the last four data nearest to the prediction time as initial states, and obtain the transition probability of each data according to the transition probability matrix $P^{(1)}$, $P^{(2)}$, $P^{(3)}$ and $P^{(4)}$. Then we can calculate the sum of transition probability for each state shown in the following Table 6:

Table 6. Transition Probability

Sequence No.	***State***	***Transfer Steps***	E_1	E_2	E_3	E_4	E_5
17	E_2	4	1/5	1/5	2/5	1/5	0
18	E_4	3	0	1/2	1/2	0	0
19	E_4	2	0	0	2/3	1/3	0
20	E_4	1	0	0	1/4	3/4	0
Sum of transition Probability			0.2	0.7	1.82	1.28	0

As shown in the above Table 6, the biggest number in the sum of transition probability is 1.82. It is means that the most possible state that the relative error of the forecasting value is ***E3*** and the most possible relative error is -0.25%. While the node's trust prediction is 0.8696 via using GM(1,1) model, we can get that (0.8696-y)/y*100%=-0.25%, the value of y is 0.8718.

In reality, the node's trust value is calculated to be 0.8513 (in which the packet forwarding ratio is 85.37% and the node's stability is 0.83), and the precision of this prediction is about 2.41%. We can see from the results, our new trust prediction model can predict the node's trust value well.

5. Conclusions

Trust prediction, an abstract psychological cognitive process, is one of the most complex concepts in social relationships, involving factors such as assumptions, expectations and behaviors. In this paper, we propose a new node trust assessment model based on node's historical behaviors, in which the trust decision factors include the subjective reputation and indirect reputation. Then we try to combine an improved grey model with the Markov chain together to effectively predict the node's trust.

For future work, we plan to continue our work in the following two directions: 1. Make a further improvement for our trust predication model; 2. As an application of this new trust prediction model, we will propose a trust-based routing protocol, and compare with other mechanisms.

Acknowledgments

We would like to thank anonymous referees for their helpful suggestions to improve this paper.

This research is sponsored by the Natural Science Foundation of China (NSFC) under Grant Nos. 61402245 and 61272425, the Project funded by China Postdoctoral Science Foundation under Grand No. 2014M551870, the Shandong Provincial Natural Science Foundation No. ZR2014FQ010, the Project funded by Qingdao Postdoctoral Science Foundation, the Open Project Foundation of Shandong Provincial Key Laboratory of Software Engineering under Grant No. 2013SE01 and Foundation of Huawei under Grant No.YB2013120027.

References

[1] Kayacan, EHH., HHUlutas, BHH., HHKaynak, OHH.: Grey system theory-based models in time series prediction. Expert Systems with Applications. 37(2), 1784-1789 (2010)
[2] HHZhang, L.XHH., HHLam, JHH.: Necessary and sufficient conditions for analysis and synthesis of Markov jump linear systems with incomplete transition descriptions. IEEE Transactions on Automatic Control. 55(7), 1695-1701 (2010)
[3] HHElSalamouny, EHH., HHKrukow, K.THH., HHSassone, VHH.: An analysis of the exponential decay principle in probabilistic trust models. Theoretical Computer Science. 410 (41), 4067-4084 (2009)
[4] Zhuang, L., Cai, M., Shen, C.X.: HHTrusted dynamic measurement based on interactive Markov chainsHH. Journal of Computer Research and Development. 48(8), 1464--1472 (2011)
[5] HHSingh, S.IHH., HHSinha, S.KHH.: A new trust model based on time series prediction and Markov model. In: Das, V.V., Vijaykumar, R. (eds) HHInformation and Communication TechnologiesHH, HHCommunications in Computer and Information ScienceHH, vol. 101, pp. 148--156. Springer, Heidelberg (2010)
[6] HHHe, L.J.,HH HHHuang, H.K.HH: A distributed trust model based on grey system theory. Journal of Beijing Jiaotong university (Natural Science Edition). 35(3), 6--32 (2011)
[7] Onolaja, O., Bahsoon, R., Theodoropoulos, G.: Trust dynamics: a data-driven simulation approach. Trust Management V, 358, 323-334 (2011).
[8] Zhang, F., Jia, Z.P., Xia, H., Sha, E.: HHNode trust evaluation in mobile ad hoc networks based on multi-dimensional fuzzy and Markov SCGM(1,1) model. HHComputer Communications. 35(5), 589-596 (2012)
[9] HHYahyaoui, HHH., HHZhioua, SHH.: Bootstrapping trust of web services based on trust patterns and hidden Markov models. Knowledge and Information Systems. 37(2), 389-416 (2013)
[10] HHKayacan, EHH., HHUlutas, BHH., HHKaynak, OHH.: Grey system theory-based models in time series prediction. Expert Systems with Applications, 37(2), 1784-1789 (2010)
[11] Wu, Gin-Der, Zhu, Zhen-Wei.: HHAn enhanced discriminability recurrent fuzzy neural network for temporal classification problems. HHFuzzy Sets and Systems, 237, 47-62 (2014)

[12] HHXie, YHH.H., HHHu, J.KHH., HHXiang, YHH.H., HHYu, SHH., HHTang, S.SHH., HHWang, YHH.: HHModeling Oscillation Behavior of Network Traffic by Nested Hidden Markov Model with Variable State-Duration. HHIEEE Transactions on Parallel and Distributed Systems, 24(9), 1807-1817 (2013)
[13] NS-2.35 simulator, http://www.isi.edu/nsnam/ns/

Authors

Shaojie Zhou, born in 1960, is currently a Lecture in the School of Measurement-Control Technology and Communications Engineering, Harbin University of Science and Technology, China. His research interests focus on network and information security, trust computing. (*zhoushaojie1001@163.com*)

Hui Xia, born in 1986, is currently a Lecture in the College of Information Engineering at Qingdao University, China. His research interests focus on network and information security, trust computing, mobile computing, embedded system and cryptology. (*xiahui@sdu.edu.cn*)