A Novel Trust Evaluation Model Based on Grey Clustering Theory for Routing Networks

Ting Han
Information Security Center Beijing University of Posts and Telecommunications, Beijing, China
hantin9@126.com

Shoushan Luo, Hongliang Zhu, Yang Xin
National Engineering Laboratory for Disaster Backup and Recovery, Beijing, China
{luoshoushan, zhuhongliang, yangxin}@safe-code.com

Yong Peng
China Information Technology Security Evaluation Center, Beijing, China
pengy@itsec.gov.cn

***Abstract*—The trust solutions to routing networks are faced with the evaluation of behavior trust and how to exactly evaluate the behaviors under the circumstance of existing recommend deceptive behavior such as providing fake or misleading recommendation. In this paper, by learning trust relationship from routing network, a trust evaluation model based on Grey Clustering Theory is proposed. The model adopts improved Bayes theory to evaluate the behavior trust. By introducing Grey Clustering Theory, the model clusters the recommend node to different trust classes according to recommend credibility and calculates the recommend weight to resistance the fraud recommends information from the deceptive node. Simulation results show that trust evaluation model based on Grey Clustering Theory cannot only effectively evaluate the routing node behavior but also has better anti-attack performance, anti-deception performance and higher attack node detection rate.**

***Index Terms*—routing node trust, routing node direct trust, routing node recommend trusts, grey clustering theory.**

I. INTRODUCTION

In routing network, trust relationship between routing nodes are often established dynamically and routing nodes have to manage the risk involved with the interactions without prior knowledge about credibility of cooperative nodes. The solution to this problem is adopting trust strategies to make routing nodes only interact with trustworthy nodes.

Some trust strategies which is based on cryptology have been presented to evaluate the routing node identity trust [1-4]. But these trust strategies cannot prevent the attack caused by the legal node and hijacked node. Trust evaluation models are proposed to solve this problem. Trust evaluation in routing network is predominantly based on the routing behavior regardless of the fact that behavior is normal or not. A number of trust evaluation models have been proposed to protect routing networks against the increasing malicious behaviors of nodes. Peng [5] proposed a trust evaluation scheme to evaluate the routing node behaviors by Bayes theory. SUN and YU [6-7] proposed a trust evaluation model by behavior evaluation. The model proposed by Wang [8] analyses the interaction behavior between routing nodes and evaluates the risk and network gain. Buchegger [9] provided a CONFIDANT routing protocol which punish the malicious node by evaluating the behavior trust. Momani [10] adopted Bayes theory to evaluate the communication behavior. But without considering recommend node trust evaluation, there are a lot of malicious recommended problem caused by fraud recommendation behavior in routing network. The conclusion of routing node trust solutions is shown in Table I.

TABLE I.
THE CONCLUSION OF ROUTING NODE TRUST SOLUTIONS

Solution	Advantage	Defect
The cryptology solution	The solution solves the issue of identity credibility.	The solution cannot prevent cannot prevent the attack caused by the legal node and hijacked node.
The trust evaluation solution	The solution evaluates the behavior of the routing node	The solution cannot restrain the strategy fraud recommendation behavior.

This paper presents Grey Clustering Trust model (GCT-Trust) to solve the routing node fraud recommendation and restrain the strategy fraud behavior. Our contributions include three folds: (1) GCT-Trust

© 2013 ACADEMY PUBLISHER
doi:10.4304/jcp.8.11.2743-2749

evaluates the routing node behavior by improving Bayes theory. (2) By introducing Grey Clustering theory, GCT-Trust clusters the recommend node to different trust classes to restrain the malicious fraud attack in trust recommendation. (3) In simulation, we validate GCT-Trust in OSPF protocol. The rest of this paper is organized as follows. Section II presents the GCT-Trust model. The related algorithm realization is described in Section III. The simulations and their analysis are presented in Section IV. The conclusion is drawn in section V.

II. Trust Model Based on Grey Clustering Theory

Routing node trust (RT) can be interpreted as the gradual and dynamic evaluation by one node on other nodes in the process of continuous interactions. This evaluation provides guidance on the behaviors of the routing node. *RT* can be classified into two categories [11]: routing node direct trust (RDT) and routing node recommend Trust (RRT). In routing network, *RDT* originates from the information collection by direct interactions and *RRT* is an integrated evaluation on the target routing node which is recommended by recommendation node [12-15].

A. Routing Node Direct Trust Calculation

RDT is calculated by improving Bayes model [16-18]. Let *s* shows the regular behavior judgment and *a* shows the malicious behavior judgment. Γ function of β function is chosen as the probability density function and the routing node directed trust probability density function is *RDTrust* () as in

$$RDTrust(s,a)=\frac{\Gamma(s+a)}{\Gamma(s)\Gamma(a)}p^{s}(1-p)^{a} \tag{1}$$

where $0\le p\le 1$.

According to probability theory, the mathematical expectation of β function is

$$E[P]=\frac{s}{s+a} \tag{2}$$

Let *x* represent the regular behavior appearance number and y represent the malicious behavior appearance number. The mathematical expectation of *x* and *y* is

$$\begin{cases} s=x+1, x\ge 0 \\ a=y+1, y\ge 0 \end{cases} \tag{3}$$

According to Equation (2) and Equation (3), the mathematical expectation of *RDTrust* () is as in

$$E[RDTrust(p\mid x,y)]=\frac{x+1}{x+y+2} \tag{4}$$

and the routing node direct trust of node *m* to node *n* (RDT_{mn}) is given by

$$RDT(m,n)=\left|E[RDTrust(p\mid x_n^m,y_n^m)]-0.5\right| \tag{5}$$

where $RDT_{mn}\in[0,1]$.

B. Routing Recommend Node Trust Calculation

The deceptive node can recommend strategy fraud trust information to rise up the trust level of some attack nodes or slander some normal nodes. More deceptive nodes can form a collusion-attack to threaten the whole routing network [19]. Through grey clustering theory, this paper solves above problem by clustering the recommend node to different trust classes and calculating recommend weight (RW) according to recommend credibility (RC) [20-21].

Let set (*m*, *i*) represents the set of public nodes. The difference of the evaluations on the public nodes between node *m* and node *i* ($diff_{mi}$) is given by

$$diff_{mi}=\left|\frac{\sum_{r\in set(m,i)}\left(RDT_{mr}-RDT_{ir}\right)}{set(m,i)}\right| \tag{6}$$

Let $diff_{mi}$'s upper limit is θ. The recommend credibility that node *m* evaluates node *i* (RC_{mi}) is given by $diff_{mi}$ as

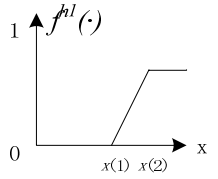
$$RC_{mi}=\begin{cases} 1-\dfrac{\theta}{diff_{mi}}\left(\theta<diff_{mi}\right) \\ 1-\dfrac{diff_{mi}}{\theta}\left(diff_{mi}<\theta\right) \end{cases} \tag{7}$$

To measure *RW* of different recommend nodes, we cluster the recommend node to different grey class by grey fixed weight clustering theory from the grey clustering theory[22].

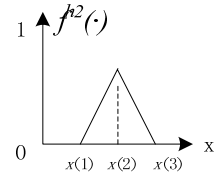
Let the grey class set is $H=\{h_1, h_2, h_3\}$, h_1 is trust class, h_2 is general trust class and h_3 is distrust class.

At the time frame *t*, we take *k* recommend nodes as clustering object and *RC* from *t* frames as the clustering indicator. For each grey class, clustering indicator has same whiten weight function and the weight of each clustering indicator is equal. Let three whiten weight functions are $f^{h1}(\cdot)$, $f^{h2}(\cdot)$ and $f^{h3}(\cdot)$ shown in Fig. 1[22].

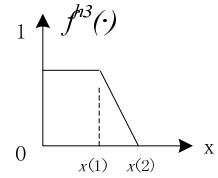
© 2013 ACADEMY PUBLISHER



(a) Whiten weight function of h_1, $f^{h1}(\cdot)$



(b)Whiten weight function of h_2, $f^{h2}(\cdot)$



(c) Whiten weight function of h_3, $f^{h3}(\cdot)$

Figure 1. Whiten weight function of grey class[22].

We calculate the grey clustering coefficient (η) of recommend node i to h_k (k=1, 2, 3) as in

$$\eta_i^k = \frac{\sum_{j=1}^{t} f^k(RC_{mi})}{t} \tag{8}$$

And then η's matrix is as in (7).

$$[\eta_i^k] = \begin{bmatrix} \eta_1^1 & \eta_1^2 & \eta_1^3 \\ \eta_2^1 & \eta_2^2 & \eta_2^3 \\ \cdots & \cdots & \cdots \\ \eta_k^1 & \eta_k^2 & \eta_k^3 \end{bmatrix} \tag{9}$$

If $\max\left\{\eta_i^1, \eta_i^2, \eta_i^3\right\} = \eta_i^k$, recommend node i belongs to grey class h_k (k=1, 2, 3).

If recommend node i (i=1, 2, n) is clustered to trust grey class (h_1), RW_i =1. If recommend node i is clustered to general trust grey class (h_2), RW_i =0.5. If recommend node i is clustered to distrust grey class (h_3), RW_i = 0. If node i is clustered to h_3, the recommend information from i will be discarded to avoid the negative effect. The value of RW is shown in TableII.

TABLEII
THE VALUE OF RW

Gray class	Value of RW	Description
Trust class(h_1)	1	The recommend information from the node is highly credible.
General trust class(h_2)	0.5	The recommend information from the node is general credible. Part of recommend information has large difference from direct trust information.
Distrust class(h_3)	0	The recommend information from the node is incredible.

Based on RW, the routing nodes recommend Trust of node m to node n (RRT_{mn}) is given by

$$RRT_{mn} = \frac{\sum_{i \in G} RDT_{in} RW_{mi}}{\sum_{i \in G} RDT_{in}} \tag{10}$$

where G is the set of the recommend node.

C. Routing Node Trust Calculation and Update

RT integrates from the RDT and RRT. We introduce the confidence factor λ to specify the impact of RDT on RT as

$$RT_{mn} = \lambda \times RDT_{mn} + (1-\lambda) \times RRT_{mn} \tag{11}$$

where 0≤λ≤1. λ also represents the confidence degree of routing node. So Equation (9) not only reflects the confidence degree of the routing node but also consider the RRT from other recommend nodes.

In Equation (10), we introduce the exponential decay factor (forgetting factor) to reflect the time-sensitive of RT and reduce old trust information's impact on the current trust evaluation. Let c represent the exponential decay factor.

$$RT_{mn}^{new} = RT_{mn}^{old} \times e^{-c \triangle t} \tag{12}$$

III. RELATED ALGORITHM REALIZATION

The routing node evaluates the trust of interaction nodes and updates the RT, RC and RW of interaction node after the end of every time frame. The algorithm by which routing node calculates and updates RT of interaction node is as Algorithm 1.

Algorithm 1. *RT calculation and update algorithm*

Input: node m, node n

Output: RT_{mn}

(1)If (interaction behavior happened) then

(2) Calculate RDT_{mn};

(3) *recommendset* (n) = {get the recommendation node set of the node n by Algorithm 2};

(4) For (node $i \in$ *recommendset* (n))

© 2013 ACADEMY PUBLISHER

(5) Get RT_{in}; /* RT_{in} is recommended by node i */
(6) Update RC_{mi}; /*update the RC of node i */
(7) Update RW_{mi}; /* update the RW of node i */
(8) Calculate RRT_{mn};
(9) Calculate RT_{mn};
(10) Return RT_{mn};
(11) Else
(12) Update RT_{mn};
(13) Return RT_{mn};
(14) END

We used the recommendation set searching algorithm (Algorithm 2) to obtain recommendation nodes and limit the scope of recommendation nodes.

Algorithm 2. *Recommendation set searching algorithm*

Input: node m, node n

Output: *recommendset* (n)

(1) If (hop (i) $<\eta$) then /* $hop(i)$ is the hop numbers between recommendation node i and node m. η is the maximum search depth to control the search depth of Algorithm 2*/

(2) For (node $i \in nset(m)$) Do /*$nset(i)$ is the set of all neighbor node of m*/

(3) If ($RT_{in} < \xi$) *then* /*if $RT_{in} > \xi$, the node i is not adopted as the recommendation node */

(4) *recommendset* (n)= *recommendset* (n)+{i};

(5) Return *recommendset* (n);

(6) END.

IV. THE SIMULATION AND ANALYSIS

In this section, simulation results are presented to demonstrate the proposed GCT-Trust by introducing GCT-Trust into OSPF protocol. We use OPNET to simulate the OSPF protocol with GCT-Trust (GCT-OSPF). The main goal in the simulation is to compare GCT-OSPF with the OSPF protocol introduced Bayes trust model (Bayes-OSPF) which does not consider the recommend credibility evaluating.

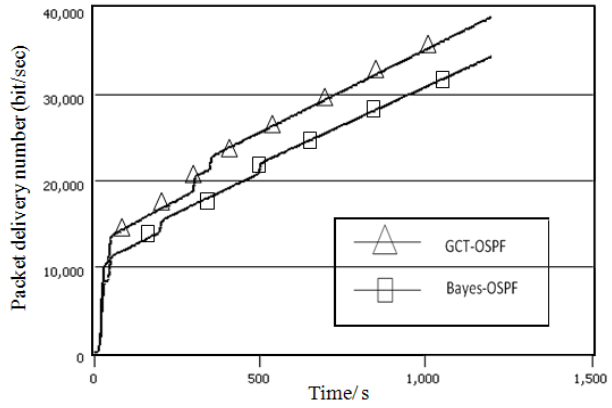
In Scenario 1, we compare GCT-OSPF with Bayes-OSPF under the circumstance of no recommend deceptive node. The simulation parameters are shown in Table III. We simulate the black-hole attack node as the attack node.

TABLE III
SIMULATION PARAMETERS OF SCENARIO 1

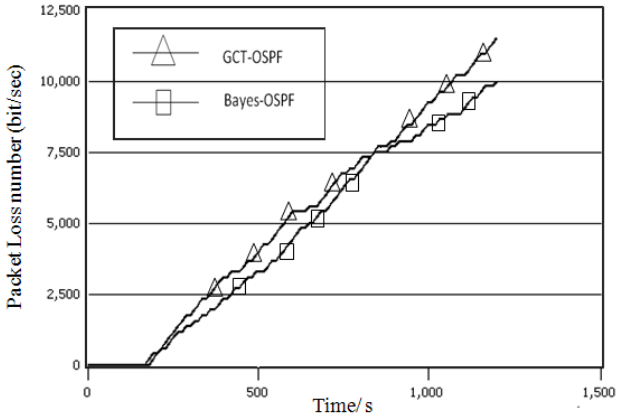
Simulation Parameters	Value
Node number	30
Attack node number	0-10
Simulation duration	1200s
Simulation scope	500×500

Fig.2 shows simulation results of Scenario 1. From the Fig.2 (a) and Fig. 2(b), it is shown that GCT-OSPF and Bayes-OSPF are almost same on the number of packet delivery and packet loss for both of them shield the attack node by trust evaluation theory. We analysis the routing overhead by OSPF Traffic Sent Average (bits/sec). With regards to OSPF Traffic Sent Average shown in Fig.2(c), GCT-OSPF and Bayes-OSPF have subtle routing overhead gap. It is due to both GCT-OSPF and Bayes-OSPF need to evaluate the node trust and transport the recommend trust information. So GCT-OSPF and Bayes-OSPF have similar routing performance under the circumstance of no recommend deceptive node. In summary, above simulation analyses can be attributed to the fact that GCT-OSPF and Bayes-OSPF have similar packet delivery numbers, packet loss numbers and routing performance under the circumstance of no recommend deceptive node.

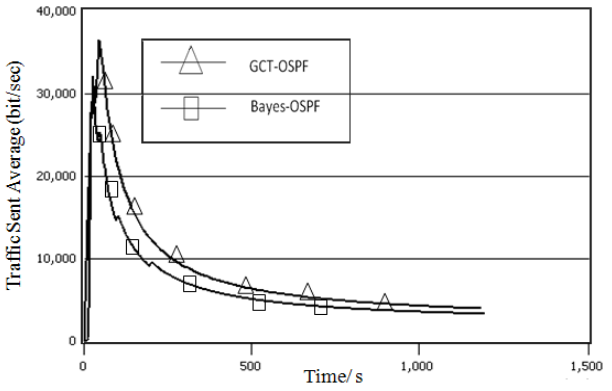
© 2013 ACADEMY PUBLISHER



(a) Packet delivery number



(b) Packet loss number



(c) Routing overhead

Figure 2. Simulation results of Scenario 1

In Scenario 2, we compare GCT-OSPF with Bayes-OSPF under the circumstance of existing deceptive nodes. The simulation parameters are shown in Table IV.

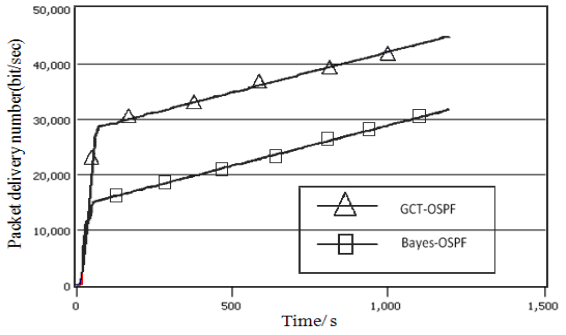
TABLE IV
SIMULATION PARAMETERS OF SCENARIO 2

Simulation Parameters	Value
Node number	30
Attack node number	0-10
Recommend deceptive nodes number	0-10
Simulation duration	1200s
Simulation scope	500×500

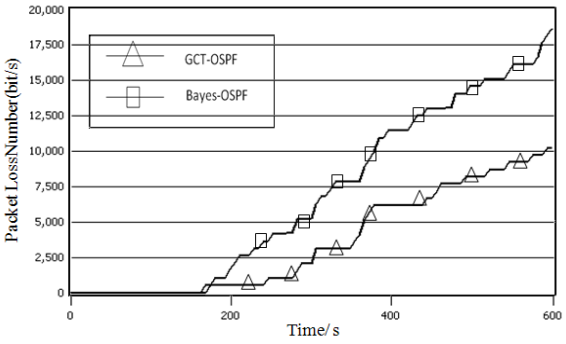
With the increase of the proportion of deceptive nodes, more malicious node cannot be detected. From Fig.3(a) and Fig.3(b), it is shown that both GCT-OSPF and Bayes-OSPF are influenced by the appearance of the attack node. But GCT-OSPF has more packet delivery numbers and less packet loss numbers than Bayes-OSPF. This is because GCT-OSPF can resistance the fraud recommends information from the deceptive node and detects the attack nodes correctly by introducing *RW*. GCT-OSPF has higher attack node detection rate than Bayes-OSPF according to Fig.3(c). In the simulation duration period, the attack node detection rate of GCT-OSPF almost reaches 100%. When there is a high rate of deceptive nodes, Bayes-OSPF keeps a lower attack node detection rate. GCT-OSPF has more routing overhead than Bayes-OSPF as Fig.3(d). This is because GCT-OSPF has to calculate and update *RW*. In summary, GCT-OSPF has better anti-attack performance, anti-deception performance and higher attack node detection rate than Bayes-OSPF under the circumstance of existing deceptive nodes.

The result of the simulation experiment shows the GCT-Trust can effectively building trust relationship between routing nodes, the routing network with large scale malicious node can still provide higher packet transaction rate.

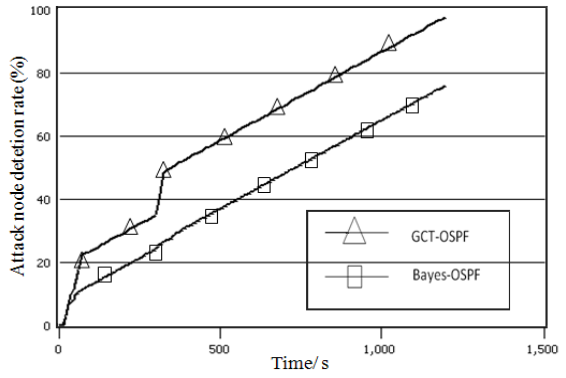
© 2013 ACADEMY PUBLISHER



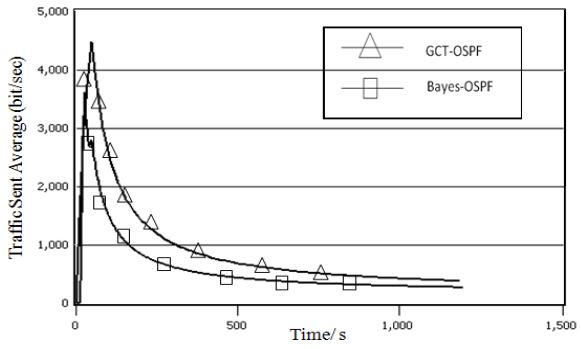
(a) Packet delivery number



(b) Packet loss number



(c) Attack node detection rate %



(d) Routing overhead

Figure 3. Simulation results of Scenario 2

V. CONCLUSION

This paper has presented GCT-Trust as a new trust evaluating model focusing on exact trust evaluation. In direct trust calculation, GCT-Trust has adopted the improved Bayes theory to evaluate the routing node behavior. GCT-Trust has clustered and analyzed the recommend node by introducing the grey clustering theory to avoid the fraud recommendation from the deceptive node. The simulation results shows that GCT-Trust has better anti-attack performance, anti-deception performance and higher attack node detection rate under the circumstance of existing deceptive nodes. Further work can be pursued in accommodating GCT-Trust to other routing protocols.

ACKNOWLEDGMENT

This work was supported in part by a grant from the National Natural Science Foundation of China (No. 61121061), National Natural Science Foundation of China (No. 61161140320) and National Key Technology R&D Program of China (2012BAH38B02).

REFERENCES

[1] S. Murphy, M. R. Badger, B. Wellington, "OSPF with digital signatures," http: // www.faqs.org /rfcs /rfc2154. html, 2013.

[2] S. Murphy, M. R. Badger, "Digital Signature Protection of the OSPF Routing Protocol", *in Proc. of Symposium on Network and Distributed System Security,* pp. 93-102, 1996.

[3] D. F. Li, Y. X. Yang and L. Z. Gu, "Secure Protection Mechanism for OSPF Protocol with Sinitizable Signature Scheme," *Journal of Beijing University of Posts and Telecommunications*, vol.34,no.3, pp.79-83,JUN.2011.

[4] S. Kent, C. Lynn and K. Seo, "Secure Border Gateway Protocol (SBGP)," *in Proc.of IEEE Journal on Selected Areas in Communications*, Vol. 18, No 4, pp 582-592, 2000.

[5] SC. Peng and W. J. Jia, "Voting-based clustering algorithm with subjective trust and stability in mobile ad-hoc networks," *in Proc. of IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, pp.3-9,2008.

[6] Y. X. Sun, S. H. Huang and L. J. Chen, "Bayesian Decision-Making Based Recommendation Trust Revision Model in AdHoc Networks," *Journal of Software*, vol.20, no. 9, pp.2574-2586, 2009.

[7] L. Yu, J. R. Ji and Z. H. Liu, "Semiring Trust Model Based on Adaptive Forgetting Scheme," *Journal of Electronics & Information Technology*, vol.33, no.1, pp. 175-179, 2011.

[8] L. N. Wang, L. Zhao and C. Guo, "A Network Connection and Routing Model Based on Trust Theory," *Geomatics and Information Science of Wuhan University*, vol.10, no.10, pp.999-1002, 2008.

[9] S. Buchegger, "Performance analysis of the confidant protocol," *in Proc. of the 3rd ACM international symposium on Mobile ad hoc networking & computing, MobiHoc*, pp. 226–236, 2002.

[10] Mohammad Momani, "Bayesian Fusion Algorithm for Inferring Trust in Wireless Sensor Networks," *Journal of Networks*, vol.5, no.7, pp. 815-822, 2010.

[11] B.Cai and Z. Li, "Computing and Routing for Trust in Structured P2P Network," *Journal of Networks*, vol.4, no.7, pp.667-674, 2009.

© 2013 ACADEMY PUBLISHER

[12] F. Cornelli, E. Damiani and D. C. Vimercati, "Choosing reputable servants in a P2P network," *in Proc.of the 11th International Conference of WWW*, pp.441-449, 2002.
[13] Z. Q. Liang and W. S. Liang, "A personalized trust model with reputation and risk evaluation for p2p resource sharing," *in Proc. of the 38th International Conference on System Science*, pp.256-264,2005.
[14] B. Yu and M. P. Singh, "An evidential model of distributed reputation management," *in Proc. of the First Joint Conference on Autonomous Agents & Multiagent Systems (AAMAS)*, pp.254-301, 2002.
[15] S. S. Song, K. Hwang and R. F. Zhou, "Trusted P2P transactions with fuzzy reputation aggregation," *IEEE Internet Computing Magazine*, vol.9, no.6, pp.24-34, 2005.
[16] J. Du and W. H. Li, "Security trust model formulti hop wireless ad hoc networks," *Journal of Jilin University (Engineering and Technology Edition)*, vol.9, no.5, pp. 1421-1425, 2011.
[17] A. Josang and R. Ismail, "The beta reputation system," *in Proc. of the 15th Bled Electronic Commerce Conference*, Bled, Slovenia, 2002.
[18] Y. F. Hwang, J. Y. Wang and J. Q. Zhang, "Bayesian Inference of Genetic Regulatory Networks from Time Series Microarray Data Using Dynamic Bayesian Networks," *Journal of Multimedia*, vol.2, no. 3, pp.46-55, 2007
[19] G. Wang and X. L. Gui, "DRTEMBB: Dynamic Recommendation Trust Evaluation Model Based on Bidding," *Journal of Multimedia*, vol.7, no.4, pp. 279-288, AUGUST 2012.
[20] L. F. Xu, H. G. Hu and Z. X. Sang, "A prestige reporting mechanism based on gray system theory," *Journal of Software*, vol .18, no.7, pp.1730-1737, 2007.
[21] L. F. Xu, D. S. Zhang and F. M. Xu, "Subjective trust model based on gray system theory," *Journal of Chinese Computer Systems,* vol.28, no.5, pp.801-804, 2007.
[22] L. J. He, "A distributed trust model based on grey system theory," Journal of Bei Jing Jiao Tong University, vol.35, no.3, pp. 26-32, 2011

Ting Han was born in Jinlin, P.R. China, 1984. He received the BS and MS degrees of computer science from XiDian University, China in 2004 and 2011 respectively, and now is a Ph.D candidate in Beijing University of Posts and Telecommunications. His research interests include information security, trusted computing and network security etc.

Shoushan Luo was born in Anhui, P.R. China, 1962. He is a professor and Ph.D supervisor of Information Security Center Beijing University of Posts and Telecommunications. His research interests include information security, network security and SecureMulti-PartyComputation etc.

Yang Xin was born in Shandong, P.R. China, 1977. He is an Associate professor of of Information Security Center Beijing University of Posts and Telecommunications. His research interests include information security, network security and trusted computing etc.

Hongliang Zhu was born in Henan P.R. China, 1982. He is a lecturer of Information Security Center Beijing University of Posts and Telecommunications. His research interests include information security, network security and trusted computing etc.

Yong Peng was born in Hunan P.R. China, 1974. He is a associate professor of China Information Technology Security Evaluation Center. His research interests include information security and network security etc.

© 2013 ACADEMY PUBLISHER