The Trust Model of Multiple Factors for Peer-to-Peer Networks

Yu-Wei Chen and Hsin-Fang Chang

***Abstract*—With internet boom, since more and more people share resource with each other through internet platform, peer-to-peer has become very popular in recent years. In the P2P environment, all nodes share resource with identities as anonymous users, and don't need to account file content they upload, as a result, some node does some malicious work through this leak, and reduce the service quality of internet, which makes security issue on internet very important. In this paper, we design "The Trust Model of Multiple Factors" to calculates the trust value of nodes with multiple factors, and node will choose its own provider through this. Many malicious behaviors may be avoided by this model, and we expected this model to increasedownload success rate and moreover, it may decrease the number of malicious behaviors on internet.**

***Index Terms*—Trust model, trust evaluation, peer-to-peer, network security.**

I. Introduction

In recent years, in order to solve P2P problem about network security, many scholars have been on the trust-model issues [1]-[9] to explore. Recent researches for trust model based on the reputation; such as EigenTrust[1] and CuboidTrust[2] decrease the number of downloads of inauthentic files. PeerTrust[3] and Reputation-based Trust [4] solve this kind of collusion. PowerTrust[5] is resilience to nodes abuse by global reputation evaluation.

In addition to above-mentioned reputation model, Zuo*et al.* proposed a novel multi-level trust model to improve the security of P2P network [6]. It avoids collusion, traitor and free-rider attack. And Li *et al.*propose a multi-dimensional trust evaluation model for large-scale P2P computing to avoid collusion like [7]. Now, artificial intelligence technology has been applied to the trust-model, e.g. fuzzy theory [8] and Bayesian network (also called belief network or directed acyclic graphical model) [9].

In this paper, we propose "The Trust Model of Multiple Factors" calculating the trust value of nodes with multiple factors. Let every single node choose its own provider. Many malicious behaviors are avoided by this model, and we expect this model to increase the download success rate, moreover, it may decrease number of malicious behaviors on internet.

II. Related Works

In order to solve the network security problem, some P2P trust models have been proposed. In EigenTrust[1], which to assign a unique global trust value, based on Power iteration. Chen *et al.* proposed CuboidTrust[2], which create a more general reputation-based trust model with three factors including contribution, trustworthiness and quality of resource. Li *et al.* proposed PeerTrust[3], which defines three parameters and two factors to calculate the trust value of node, namely, feedback, the total number of transactions, credibility of feedback, transactions context and community context. Zhou *et al.* proposed PowerTrust[5], to leverage the power-law feedback characteristics. The nodes are dynamically selected by a distributed ranking mechanism. By using look-ahead random walk strategy, the aggregation speed and the accuracy of global reputation to would be improved significantly.

III. The Trust Model of Multiple Factors

In the P2P environment, every node acts as a file's provider and also as a receiver. All nodes share resources with identity as anonymous user, some node may do malicious act during providing file. So the network security issue becomes important.

In order to overcome the network security problems, we propose "The trust model of multiple factors for peer-to-peer networks, called MFTM",it calculates trust value of the nodes through multiple factors. We set weights to different factors by various aspects of server, calculating the trust value of each provider,then let the every receiver choose theirown providers. Many malicious behaviors then will be avoided by this model, and we expect the model to increasedownload success rate and moreover, it may decrease the probabilities of malicious attacks.

A. Basic Architecture

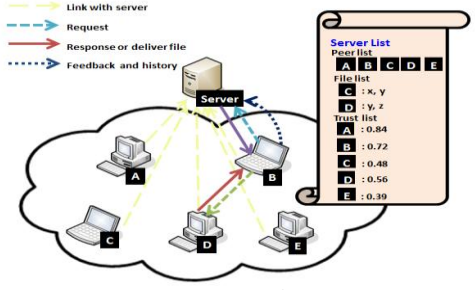

Fig. 1. The MFTM's framework.

Fig. 1 is the MFTM's framework, in this environment, there are five nodes A, B, C, D and E, if node B goes to download the file y, it sends a request to the server, and server return node C and D's data that shares the same file y. In this time node B is allowed to choose node D which is

Manuscript received March 15, 2012; revised May 10, 2012.

The authors are with Graduate Institute of Information and Logistics Management, National Taipei University of Technology, Taipei, Taiwan (email: zixfang@gmail.com).

with the highest trust value. After transaction finish, node D sends the historical evaluation and the feedback to the server, and the trust value of node B is modified with multiple factors based on transaction behavior, finally, the trust value is stored in the server.

B. Formal Function of the Factors

We propose MFTM, which calculates trust value of nodes with multiple factors, including the historical factor, the feedback factor, the contribution factor, the risk factor and the punishment factor. This section we introduce these factors. In table 1, indicates the meaning of each factor.

TABLE I: BASICNOTATIONS

Notation	Description
H	value of historical factor
h_i	i^{th}historicalevaluation
t	thetimewhilecalculating the value of history factor
t_i	i^{th}transaction timeof the nodewhile calculating the value of history factor
$\mathrm{w}(t_i)$	weight of the time of i^{th} transaction
T_i	trust value of i^{th}nodeduring transaction
d	time interval
N	the total number of transactions of the node
F	the value of feedback factor
m	amount ofthe file which the node provides
c_i	sum of feedback value of i^{th} file
k	the total number of feedback that the specific file obtained
f_j	feedback value of j^{th}transaction
θ	threshold value of feedback
pt	value of punishment
p	percentage of punishment
T_{ID}	the current trust value of the node
C	value of contribution factor
Sr	range of file size
S_i	contribution value of i^{th} file
R	value of risk factor
N_s	the total number of successful transactions of the node
w_i	weight ofi^{th} factor

1) History factor

History factor reflects to node's long-term behavior. The node estimates its nature by previous transaction. In the server there is the history list which records ID of the provider node, ID of the request node, file name, download time, trust value of request node and whether to recommendation.

In the P2P environment, each node chooses provider node through the third party's opinion, especially the provider node that untouched. Therefore, it ensures the quality of the transaction, so we will be recommend as the historical evaluation. The node may change its behavior anytime, so we consider the weight of time in our trust model, therefore the information that newly obtains higher weight.

Definition 1. The value of historical factor defined as the following equation:

$$H = \left[\sum_{i=1}^{N} h_i \times \mathrm{w}(t_i) \times T_i\right] \Big/ \sum_{i=1}^{N} \mathrm{w}(t_i) \qquad (1)$$

where h_i is the historical evaluation,(1 represent the recommended, 0 is not recommended.)

Definition 2. The weight of time defined as the following equation:

$$w(t_i) = \frac{1}{\log_2 d} \; where \; d = t - t_i + 2 \qquad (2)$$

As an example, the filea in the environment that node A uploaded, and node B, C and D downloaded it at the different time. Assuming that t is 11/10, download time is 11/1, 11/5 and 11/9,T_i is 0.5, 0.6 and 0.2 and $h_i$is 1, 1 and 0. Using Eq. (2)d is 11, 7 and 3, $\mathrm{w}(t_i)$ is 0.289, 0.356 and 0.631. From Eq. (1), wecalculate that thevalue of historical factor of node A is 0.28.

2) Feedback factor

Feedback factor used to estimate the satisfaction of transaction. Request node sends feedback value to the provider when finishing transaction. In the server there is the feedback list that records ID of the provider node, ID of the request node, file name, download time, trust value of request node and the value of feedback.

After the transaction finish, the request node sent the value of feedback to the server, and the trust value of node B is modified with feedback factor based on transaction behavior, finally, the trust value is stored in the server.

Definition 3. The value of feedback factor defined as the following equation:

Definition 4. The sum of feedback value of i^{th} file defined as the following equation:

$$F = \left(\sum_{i=1}^{m} c_i\right)/m \qquad (3)$$

$$c_i = \left(\sum_{j=1}^{k} f_j \times T_j\right) \Big/ \sum_{j=1}^{k} T_j \qquad (4)$$

where f_j is the feedback value of j^{th} transaction,(1 represent the file is correct and the quality of the file is good, 0.75 represent the file is correct but the quality of the file is bad, 0.25 represent the file is not correct but non-destructive, 0 represent the file is not correct and destructive.)

In the environment, some nodes provide the correct value of feedback based on transaction acts. Some nodes deliberately provide error value of feedback that to lead tocalculate the trust value is wrong.In this paper, when calculating the trust value, we add the punishment mechanism that decreases the error value of feedback.If receive the quantity of feedback in the same file over our set threshold value, request node's the value of feedback should to compare with the feedback value of other nodes.The situations of comparison are as follow:

- Majority of nodes sends value of feedback to the node that upload the file, that the value of feedback is 1 or 0.75. If the value of feedback of the request

node is 1 or 0.75, we using Eq. (4) to calculated the value of feedback, else starting the punishment mechanism which in 3.2.3 of the article.And vice versa.

As an example, file a, and file b in the environment that node A uploaded, and node B, C and D downloaded the file a at the different time. Assuming that T_j is 0.5, 0.6 and 0.2. The value of feedback is 1 that node B and C is given. Node D was send the value of feedback is 0.75, then using Eq. (4)to calculated the sum of feedback of the file a, we obtainc_a = (0.5 + 0.6 + 0.15) / 1.3= 0.962. Node B and E downloaded the file b, assuming the value of feedback are 1, T_E is 0.4,using Eq. (4), we obtain thec_b= (0.5 + 0.6) / 0.9 =1. Final, the value of feedback factor of node A is 0.981.

Corresponding to the above, if node D was sent the feedback value is 0, that the punishment mechanism is activated, and calculating the value of feedback factor to exclude node D's feedback value.As a result, the$c_a$is1, the c_b is1 and the value of feedback factor of node A is 1.

3) Punishmentfactor

Punishment factor used to punish the node which sent error value of feedback. It protects against node collusion, slander etc. In the server there is the punishment list that records ID of the provider node, ID of the request node, value of punishment and percentage of punishment. The conditions of punishment are as follows:

Parameter$f^{'}$, represent majority of nodes send value of feedback to the node that upload the file.

- When f′ is 1,the trust value of request node has to decrease 15% if feedback value is 0.25, andthe trust value of request node has to decrease 20% if feedback value is 0.
- When f′ is 0.75,the trust value of request node has to decrease 10% if feedback value is 0.25, and the trust value of request node has to decrease 15% if feedback value is 0.
- When f′ is 0.25, the trust value of request node has to decrease 10% if feedback value is 0.75, and the trust value of request node has to decrease 15% if feedback value is 1.
- When f′ is 0, the trust value of request node has to decrease 15% if feedback value is 0.75, andthe trust value of request node has to decrease 20% if feedback value is 1.

Definition 5. The value of punishment factor defined as the following equation:

$$pt = T_{ID} \times p \tag{5}$$

4) Contribution factor

The P2P environment is composed by different nodes that can share resources.When there are more and more nodes provide resources in the environment that can share more resources.Contribution factor reflects the contribution of nodes in the P2P environment.In the server there is the contribution list that records ID of the provider node, file name and size of file.Simultaneously, we consider the correctness of file uploaded, rather than raise the trust value by small transaction.In this paper, the file size is divided to five ranges, which Sr1, Sr2, Sr3, Sr4 and Sr5, and the different ranges has difference contribution value.

Definition 6. The value of contribution factor defined as the following equation:

$$C = \left(\sum_{i=1}^{m} S_i \times c_i\right)/m \quad where \quad S = \begin{cases} 0.2, & 0_{MB} < Sr1 \le 100_{MB} \\ 0.4, & 100_{MB} < Sr2 \le 300_{MB} \\ 0.6, & 300_{MB} < Sr3 \le 500_{MB} \\ 0.8, & 500_{MB} < Sr4 \le 1024_{MB} \\ 1, & 1024_{MB} < Sr5 \end{cases} \tag{6}$$

As an example, file a and b in the environment that node A has uploaded. Assuming that file a's and b's feedback value is 1, and file size is 150_{MB}, 7.184_{MB}, using Eq. (6), we obtain the C = (0.4 * 1 + 0.2 * 1) / 2 = 0.3.

5) Risk factor

Risk factor used to estimate the risk of transaction.In the server there is the risk list that records ID of the provider node, the total number of transactions of provider node, the total number of successful transactions of provider node.

Definition 7. The value of riskfactor defined as the following equation:

$$R = N_s/N \tag{7}$$

C. Formal Function of Trust Value

In this paper, it calculates the trust value of nodes with multiple factors. We set weights to different factors by various aspects of the server, calculating the trust value of each provider, letting the request node chooses the provider they want for raising the quality of service and success ratio on transaction.

Definition 8. The trust value of nodedefined as the following equation:

$$T_{ID} = H \times w_1 + F \times w_2 + C \times w_3 + R \times w_4 + pt \tag{8}$$

where $T_{ID}$is trust value of node, w_i, i=1, 2, 3 and 4, which representing weightof history factor, weightof feedback factor, weightof contribution factor and weightof risk factor.

It calculates trust value of provider node again while finishing each transaction, when punishment value of request node is changed, that calculating trust value of request node again, and the punishment value become zero.

Assuming that value of history factor of node A is 0.28, value of feedback factor of node A is 1, value of contribution factor of node A is 0.3, value of risk factor of node A is 1, value of punishment factor is 0 and weight of these factor is the same, we can get the trust value of node

A is 0.645.

IV. Conclusion

In this paper, we propose the trust model of multiple factors. It effectively restrains malicious nodes, improving transaction success rate and service quality. In the future, we will keep making efforts on establishment of simulate system of trust model through java language within multiple factors, and verifying the feasibility of this proposed method.

References

[1] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The EigenTrust algorithm for reputation management in P2P networks," in *Proceedings of the 12th International World Wide Web Conference*. 2003, pp. 640-651.

[2] R. Chen, X. Zhao, L. Tang, J. Hu, and Z. Chen, "CuboidTrust: a global reputation-based trust model in peer-to-peer networks," *Fourth Int. Conf. on autonomic and Trusted Computing*. 2007, pp. 203-215.

[3] X. Li and L. Liu, "PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities," *IEEE Transactions on Knowledge and Data Engineering*. 2004, Vol. 16, No. 7, pp. 843-857.

[4] S. Peng, J. He and Y. Meng, "Reputation-based trust update in network environment," in *2008 International Symposium on Electronic Commerce and Security*. 2008, pp. 118-123.

[5] R. Zhou and K. Hwang, "PowerTrust: A robust and scalable reputation system for trusted P2P computing," *IEEE Transactions on Parallel and Distributed Systems*. 2007, pp. 460-473.

[6] C. Zuo, J. Zhou, and H. Feng, "A novel multi-level trust model to improve the security of P2P networks," in *proc. 2010 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT).* 2010, pp.100-104.

[7] X. Li, F. Zhou, and X. Yang, "A multi-dimensional trust evaluation model for large-scale P2P computing," *Journal of Parallel and Distributed Computing.* 2011, pp. 188-193.

[8] Z. Hu, H. Lin and Y. Zhou, "A fuzzy reputation management system with punishment mechanism for P2Pnetwork," *Journal of Networks.* 2011, vol. 6, No. 2, pp. 190-197.

[9] Y. Wang and J. Vassileva, "Bayesian network trust model in peer-to-peer networks," in *Proc. Of the Workshop on "Deception, Fraud and Trust in Agent Societies" at the Autonomous Agents and Multi Agent Systems. LNCS 2872, Berlin: Springer-Verlag*.2003, pp. 23-34.