MJRET
Open Access
Multidisciplinary Journal of Research in Engineering and Technology
Journal homepage: www.mjret.in
ISSN:2348 - 6953

TRUST MANAGEMENT IN P2P SYSTEMS USING SORT MODEL

Vaibhav Naik, Amol Gangawane, Sujit Mendhe, Vikas Kapre
Computer Department, Imperial College of Engg. & Research,
S.P. Pune University, Pune, India
naik.vaibhav101@gmail.com, sujitmendhe@gmail.com,
amolgangawane007@gmail.com, vikaskapre007@gmail.com

Abstract: *This paper is use to solve the problem of the open nature of Peer to Peer system in a Network. The Main problem in P2P system is that every system is treated equally and possess equal rights to every resource in Network. Here the Security of Data or resources is not stated. Hence the trust problem arises in the Network. This Paper presents the solution to the Problem mentioned above by creating a Trusted Environment among the Peer, present in the Network. The trusted environment is created with the use of Distributed Algorithm which satisfies the trustworthiness of other peer to the peer on which it is calculated on the information available to the current peer, this calculation requires two parameters known as Past Interaction and Recommendations received from others. After applying the SORT the proposed system is able to prevent attacks from different malicious behavior model. In SORT, Every peers calculate its own set of parameters based on trustworthiness in relation of other peers in the Network. The Trust environment is required for the purposes like Communication, File Sharing or Resource Sharing. In this system the Algorithm will separate the trusted peers and the malicious peer from one another and will create a secure Environment.*

Keywords *– Peer to Peer System, Trust Environment, Reputation, recommendation, Security, Services*

1. INTRODUCTION

In P2P networks, Clients both provide and use resources. This means that unlike Client-Server System, the content serving capacity of Peer to Peer Network can actually increase as more users begin to access the content. Unlike Client-Server the peer have equal privileges, it means that every peer is able to provide services to other peers and at the same time it is able to use the services provided by another peers in the network.

The Problem arises mainly in this types of model is that, a peer can share infected file to other peers or there is no mechanism to guarantee the provided service is safe or malicious, So there is need to create a trusted environment which will help to perform secure communication and data sharing in the further transactions. In normal P2P model to maintain the trust between the peers is not easy, because the trust is an entity which cannot be expressed in numerical form and hence the SORT model introduces some metrics which will help to calculate the trust among the peers in the Network. Distinguishing the trusted and untrusted peers is not sufficient generally. Metrics should have appropriateness to rank the trusted peers according to their interaction and the feedbacks provided after interaction.

Communication with a peer may provide some certain information about the peer, but the feedbacks might contain misleading information Central Server is a concept which is use to prevent the malicious attacks or fake request and provides security but in Peer to Peer system there is no server concept which will rectify the malicious activities, so this system is being built which will provide the security from malicious activity [2] [3]. Managing the information related to the trust is directly proportional on the structure of the P2P Model. Peers communicate with each other and calculate the metric of trust with respect to other, each metric is different from each other i.e. metric is built by its own view and thus isolating trust and malicious peers [4]. In the beginning all peers are stranger to each other, when a peer provides to any other peer a service e.g. file operation so the peers considered as an acquaintance. At the time of communication, the first preference is given to acquaintance and if not present then stranger are preferred for communication. All peer has more than one acquaintance, so the preference is based on the basis of importance of peer, Recentness of communication and satisfaction of the requestor. The stranger is considered on the feedback of an acquaintance i.e. recommendation, which is calculated with the help of two parameter, Recommender's trust about stranger and knowledge gained from the recommender's acquaintance, and the level of confidence of the recommender. The SORT model considers service and recommendation two different things. This Model provides three metrics, Reputation, Service trust and Recommendation. Metrics parameters include peer's bandwidth, number of shared files, peer behavior (online/offline, session time) and last resource distribution this will result in the approximated conclusion [5], [6], [7]. With the help of these metrics SORT model mitigate the two type of attack Service based and recommendation.

2. WORKING OF SYSTEM

In proposed system, each peer plays a dual role of an admin and a user. Both the roles has different functions, Admin has the full authority of its own files and User role is for requesting for the files from other peer.

When a peer wants to communicate with any other peer for service then first its checks if the user is acquaintance or a stranger. If the peer is a stranger then, it will check communicate with its acquaintance for getting the trust information, if information is not available then it simply allows the stranger to communicate on trial basis. After the trial basis it develops the trust information of the stranger, and if the level of trust is up to the level then the stranger is considered as an acquaintance or else it considered as malicious peer and the future request from that peer are prohibited. If the requestor is an acquaintance then the trust information is checked from the metrics and the permission is allotted for the query passed by requestor. If two or more acquaintance are requesting for the same resource then the preference is calculated with the help of metrics, the trust information in the metrics is directly proportional to the priority of acquaintance, higher the trust value higher the priority. When peer login as an admin, he can upload, request check, recommendation, and assigning permission or else as an user he can request to any acquaintances, get recommendation from its acquaintances and download files.

3. METRICS

All peers present in the network are equal in computational power and responsibility. There is no Privileged, centralized or trusted peers to manage the information. A peer provide and use services.

Talking about an interaction it is a File Download.

3.1 Preliminary Notations

A peer is denoted p, i^{th} peer is denoted as $p_{i.}$ Interactions are always unidirectional because when peer p_i downloads a file from peer p_j any of information of interaction is not stored on p_j. If two peer, suppose p_i and p_j had an interaction then the both peer is considered as acquaintance. Every peer stores a record of past interaction known as service history, sh_{ij} denotes service history of p_i with p_i.

After an interaction completed the node downloading the file evaluates quality of service and sets a satisfaction value for the interaction. The importance of an interaction is called weight value, it means the importance of the file according to us. There is one important parameter known as fading effect it means that old interaction must lose its importance as soon as new interaction takes place.

- Satisfaction is denoted as 's'
- Weight is denoted as 'w'
- Fading Effect is denoted as 'f'

3.2 Service Trust Metrics

Evaluation of acquaintance's trustworthiness in the service context, two belief are calculated i.e. integrity belief and competence belief on the basis of information in its service history. Competence belief symbolizes how well an acquaintance satisfies the need of past interaction [8,9,10].

Let cb_{ij} represent the competence belief of p_i about p_j in the service context. In short competence is the average behavior in the past interaction. Evaluation of competence belief the instruction are consider on their recentness and weight.

Competence Belief:

$$cb_{ij} = \frac{1}{\beta_{ij}} \sum_{k=1}^{sh_{ij}} (s_{ij}^{k}.w_{ij}^{k}.f_{ij}^{k}) \tag{1}$$

Integrity Belief:

$$ib_{ij} = \sqrt{\frac{1}{sh_{ij}} \sum_{k=1}^{sh_{ij}} (s_{ij}^{k}.w_{ij}^{k}.f_{ij}^{k} - cb_{ij})} \tag{2}$$

Fading Effect:

$$f_{ij=}^{\mu} \frac{1}{sh_{ij}} \sum_{k=1}^{sh_{ij}} f_{ij}^{k} = \frac{sh_{ij}+1}{2sh_{ij}} \approx \frac{1}{2} \tag{3}$$

Service Trust Metrics calculation:

$$st_{ij} = cb_{ij} + ib_{ij}/2 \tag{4}$$

$$\mathrm{st_{ij}} = \frac{\mathrm{sh_{ij}}}{\mathrm{sh_{max}}}\left(\mathrm{cb_{ij}} + \mathrm{ib_{ij}}/2\right) + (1 - \left(\frac{\mathrm{sh_{ij}}}{\mathrm{sh_{max}}}\right) \mathrm{r_{ij}} \tag{5}$$

3.3 Reputation Metrics

To measure stranger's trustworthiness Reputation metric is used. There are two sections, we assumed that p_j is stranger to p_i and p_k is an acquaintance of p_i. If p_i wants to calculate Reputation metric between p_i & $p_{j,}$ it starts Reputation query to collect Recommendation from its acquaintances.

Estimation about reputation:

$$er_{ij} = \frac{1}{\beta_{er}} \sum_{p_{k \in T_i}} \left(rt_{ik}.\eta_{kj}.r_{kj}\right) \tag{6}$$

Estimation about Competence Belief:

$$ecb_{ij} = \frac{1}{\beta_{ecb}} \sum_{p_{k \in T_i}} \left(rt_{ik}.sh_{kj}.cb_{kj}\right) \tag{7}$$

Estimation about Integrity Belief:

$$eib_{ij} = \frac{1}{\beta_{ecb}} \sum_{p_{k \in T_i}} \left(rt_{ik}.sh_{kj}.ib_{kj}\right) \tag{8}$$

Reputation Metrics calculation:

$$r_{ij} = \frac{[\mu_{sh}]}{sh_{max}}\left(ecb_{ij} - eib_{ij}/2\right) + \left(1 - \frac{[\mu_{sh}]}{sh_{max}}\right)er_{ij} \tag{9}$$

3.4 Recommendation Metrics

After calculating the Reputation metric between p_i and p_j the recommendation trust values based on accuracy of their recommendations is updated by p_i. The Reputation trust metric explains how p_i updates rt_{ik} according to p_k's recommendation.

The following are the three parameters which are calculated about recommendations are satisfaction, weight and fading effect.

Recommendation satisfaction evaluation:

$$rs_{ik}^{z} = \left(\begin{array}{c} \left(1 - \frac{\left|r_{kj} - er_{ij}\right|}{er_{ij}}\right) \\ + \left(1 - \frac{\left|cb_{kj} - ecb_{ij}\right|}{ecb_{ij}}\right) \\ + \left(1 - \frac{\left|ib_{kj} - eib_{ij}\right|}{eib_{ij}}\right) \end{array} \middle/ 3 \right) \tag{10}$$

Recommendation weight evaluation:

$$rw_{ik}^{z} = \frac{[\mu_{sh}]}{sh_{max}}\frac{sh_{kj}}{sh_{max}} + \left(1 - \frac{[\mu_{sh}]}{sh_{max}}\right)\frac{\eta_{kj}}{\eta_{max}} \tag{11}$$

Competence and Integrity beliefs in recommendation

$$rcb_{ik} = \frac{1}{\beta_{rcb}}\sum_{z=1}^{rh_{ik}}(rs_{ik}^{z}.rw_{ik}^{z}.rf_{ik}^{z}) \tag{12}$$

$$rib_{ik} = \sqrt{\frac{1}{rh_{ij}}\sum_{z=1}^{rh_{ik}}\left(rs_{ik}^{z}.rw_{ik}^{\mu}.f_{ik}^{\mu} - rcb_{ik}\right)^{2}} \tag{13}$$

Evaluation of Recommendation Trust Metric

$$rt_{ik} = \frac{rh_{ik}}{rh_{max}}\left(rcb_{ij} - rib_{ij}/2\right) + \left(\frac{rh_{max} - rh_{ik}}{rh_{max}}\right) \tag{14}$$

4. CONCLUSION

In this paper we are presenting a trust model for p2p networks, in which trust information is developed on every single peer. With the help of this information the peer can isolate the trusted and malicious peer in its proximity. The two measures of trust is service and recommendation are used to define capability of providing service by a peer. An Interaction is one side download of a file, and recommendation contains the recommender's own experience about the peer with the parameter known as satisfaction, weight and fading effect. Parameters are provided for better assessment of trustworthiness of a peer.

The SORT model helps to mitigate the attacks based on service and recommendation in most of the experiments. The main problem in the SORT model is that if a peer changes it access to network the trust information calculated using SORT is affected because the same node is attached newly to an network and thus making it a stranger to the other peers in the network. Using the information about the trust does not solves all the problem related the security in P2P systems but it can enhance security and effectiveness of systems.

REFERENCES

[1] "SORT: A Self ORganizing Trust Model for P2P Systems" Ahmet BurakCan , Member, IEEE, and Bharat Bhargava, Fellow, IEEE.

[2] K. Aberer and Z. Despotovic, "Managing Trust in a Peer-2-Peer Information System" Proc. 10th Int'l Conf. Information and Knowledge Management (CIKM), 2001.

[3] F. Cornelli, E. Damiani, S.D.C. diVimercati, S. Paraboschi, and P. Samarati, "Choosing Reputable Servents in a P2P Network," Proc.11th World Wide Web Conf. (WWW), 2002

[4] P. Druschel and A. Rowstron. Past: A large-scale, persistent peer-to-peer storage utility. In Proceedings of the 18th ACM Symposium on Operating Systems Principles (SOSP'01), October 2001.

[5] Gnutella. Gnutella protocol specification v0.4.http://www.clip2.com/GnutellaProtocol04.pdf,2001

[6] J. Heidemann, F. Silva, C. Intanagonwiwat, R. Govindan, D. Estrin, and D. Ganesan. Building efficient wireless sensor networks with low-level naming. In Proceedings of the 18th ACM Symposium on Operating Systems Principles (SOSP'01), October 2001.

[7] J. Kubiatowicz, D. Bindel, Y. Chen, P. Eaton, D. Geels, R. Gummadi, S. Rhea, H. Weatherspoon, W. Weimer, C. Wells, and B. Zhao. Oceanstore: An architecture for global-scale persistent storage. In Proceedings of ACM ASPLOS.ACM, November 2000

[8] D.H. McKnight, "Conceptualizing Trust: A Typology and E-Commerce Customer Relationships Model," Proc. 34th Ann. Hawaii Int'l Conf. System Sciences (HICSS), 2001

[9] Y. Zhong, "Formalization of Dynamic Trust and Uncertain Evidence for User Authorization," PhD thesis, Dept. of Computer Science, Purdue Univ., 2004.

[10] S. Xiao and I. Benbasat, "The Formation of Trust and Distrust in Recommendation Agents in Repeated Interactions: A Process- Tracing Analysis," Proc. Fifth ACM Conf. Electronic Commerce (EC), 2003.