Indian Journal of Research Communication Engineering (IJRCE)
Vol.2.No.1 2014 pp 37-41.
available at: www.goniv.com
Paper Received :08-03-2014
Paper Accepted:22-03-2013
Paper Reviewed by: 1. R. Venkatakrishnan 2. R. Marimuthu
Editor : Prof. P.Muthukumar

ENHANCED DISTRIBUTED TRUST BASED NETWORK MODEL FOR PEER-TO-PEER SYSTEM ARCHITECHTURE

R.Renuga[1] A.Rajesh[2] A.Kumaresan[3]
Dept. of CSE,
S.K.P Engineering College,
Tiruvannamalai, India
renurajeeva@gmail.com, svishnuraj@yahoo.co.in Kummaresan@gmail.com

ABSTRACT

Direct connection, peer-to-peer systems can use less bandwidth, encourage faster file transfers and facilitate users to connect directly with one another to share useful information. In peer-to-peer file sharing has more malicious activity. It will reduce the performance of file sharing. Avoid this effect by making the trust relationship between two different peers. In this paper, we propose a Trust relationship have three different context service, reputation and recommendation. The past interaction and recommendation are valid by recentness, peer satisfaction parameters and importance. The Global trust information is not used here only using the local trust information and use distributed algorithm. The past interaction and recommendation are considered with satisfaction, weight and fading effect parameter. Past interaction history is creating itself. This approach provides high efficient to choose good peer in a peer-to-peer network. It forms only good peer networks and avoid the malicious peer in the networks. Graphical result shows that this approach to mitigate the malicious attack and improve the performance file sharing.
Key words: Trust relation, recommendation, reputation, peer-to-peer, file sharing

1. INTRODUCTION

In peer-to peer systems, peer can communicate with other peer directly. The peer-to-peer systems have several categories. Centralized P2P and decentralized P2P,centralized P2P means the server control is centralized to manage the systems. Decentralized P2P systems used to distribute control to each peerso we are easy to perform in malicious activity. To reduce the malicious activity by creating long term trust relationship between each peer. It provides the secure environment to share the information from one to another. Most trust relationships are mainly based on global trust information. The peer get the past interaction history of another peer for identifying good peer.

The peer has two different network model. Structuredpeer-to-peer and Unstructured peer-to-peer network. Based on this concept the trust information is stored [1][2][4]. In structured peer-to-peer network store the trust information in the Distributed Hash Table. The DHT store the global trust information. Unstructured peer-to-peer network store trust information about the neighborhood or past interacted peer. It does not have the global trust information [3].
In this paper, we propose a trust model. The main aim is to decrease the malicious activity performance in peer-to-peer and improve the secure file sharing. Here peer do not try to collect the global information. Each and every peer develops its own local view of trust about the past interacted peer. So this method can form the good peer dynamic trust groups and separate the malicious peer [5].

At the beginning stage each peer should assume to be a stranger. After interaction or service provider to another peer the interacted peer is considered as acquaintance [3]. The peer always prefers the acquaintance peer for the easy and secure transaction. Past interaction is evaluated based on the recentness, weight and peer satisfaction parameter [3]. The recommendation is valid by recommender's

trustworthiness []. So we have two different methods for creating trust relationship. One is a service and another one is recommended. The Service is used to select the best service provider and the recommendation is used for requesting the recommendation to another peer. Another one method is reputation. It is calculated based on the recommendation and we add the other method trust overlay network to calculate the reputation. Using this method we make a secure peer-to-peer architecture for file sharing. Finally, it forms good peer and isolate malicious peer.

The outline of the paper as follows: section2 discuss the related work. Section3 describe proposed method. Section4 deals with the Experimental result and final section5 gives the conclusion of this paper.

2.RELATED WORK

Comparsion Of Trust Model In Peer-To-Peer System

This paper explains different trust model. Here identify the which models are used in previous methods. 1.

Global Trust model: This model is based on the binary trust model or other words the agent could be either trustworthy or untrustworthy. Here the agent can perform transaction to another agent. The Advantage of this method is, if one agent can perform cheating to another agent during the transaction. This information is distributed to all agents in global trust model. For example p and q interact with each other. During this transaction, both complaints about each other. That time r wants to know about the trustworthiness of p& q. Then p and s interact each other, here also complain about each other. So both the p & s and p & q transaction p is untrustworthy. To find out the untrustworthy peer using the below formula. T(P) is the high trustworthy value of peer p.

$$T(\quad |c(p, \ | \ \in p \quad |c(\ , p \ | \ \in p$$

Advantage: solve the data management problem using decentralized data. *2.NICE Model* : is used to identify the good peers and guard from the malicious peers. Fig. 1 explain how Transaction happen in NICE model.

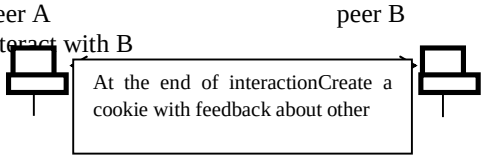

Figure. 1.NICE Model Transaction

Here to requestor want data from provider means, then show the signed cookie. Provider justify the validity of the cookie then it regarded as request peer trustworthiness. 3.*Eigen trust model*: It is designed for reputation management of P2P system. 4.*Trust in large scale P2P systems*: here builds the trust relationship without benefit of third parties. The trust model main aim is to distribute thereputation mechanism for P2P systems.

A Privacy Enhanced Peer-To-Peer Reputation System

This paper uses different technologies to make a secure transaction in P2P system. The three methods are Trust modeling, Reputation systems and TCPA technology. The trust model is used to develop the trust based on the experiences. The Reputation system calculates the reputation value of centralized, distributed and commercial apps method. The Distributed approach uses the poblano concept. It introduces a decentralized trust model with trust relationship. Finally TCPA Technology it stands for Trusted Computing Platform. TP must include the cost-effective security hardware that acts as the "root of trust" in a platform. This method have three different function protected storage, Integrity checking, TCPA Pseudonymous identity. These functions are used to enhance the security of P2P reputation system in a cost-effective and flexible manner.

Propagation of Trust and Distrust

The goal of this paper is to predict an unknown trust/ distrust value between any two users. This paper has different methods to propagate the trust. The methods are rounding, Iteration. Rounding have three different calculation, global, local, majority. These are all converting the continuous belief into discrete ones. This paper uses the matrix method concept. Assume n users are available partition into trust metrics T_{ij} and distrust matrix d_{ij}. Propagation of distrust has three models 1.Trust only B=T (B-belief, T-Trust matrix T_{ij}) 2.One-step Distrust, here distrust only a single step, while trust may propagate repeatedly. 3.Propagate distrust B=T-D (trust-distrust). It shows how trust is propagated.

Analysing Topologies Of Transitive Trust

This paper explains the concept of trust, trust property, transitivity and recommendation. Trust is a basic concept and trust property have three different type diversity, transitivity and combination. Trust diversity explains the possible trust in this method. It has three different type 1.Origin diversity 2.Purpose diversity 3.Target diversity. Transitive use the purpose diversity it defined by two trust variant. The trust variant is direct trust and indirect trust.

Trusted Peer-To-Peer Transcations With Fuzzy Reputation Aggregation

To build FuzzyTrust. A prototype peer-to-peer reputation systems that help mutual trust in P2P transaction. It uses the Fuzzy Logic inference rule to compute the local trust and aggregate the global reputation value. The system benefits are distinct advantages of fuzzy inference it can handle the imprecise linguistic termeffectively. This system uses the DHT overlay network to perform secure and speed transaction.

3.PROPOSED SYSTEM

Preliminary Notations

The P_x denotes the x^{th} peer. P_x gets service from another peer called interaction of P_x. Here interaction happened only unidirectional. For example the P_x downloads a file from the P_y. This interaction happened to P_x not to P_y because no one information is stored here. Once the P_x can interact by P_y means, then P_y is an acquaintance of the P_x. After finishing the interaction P_x evaluate the QoS and assign the satisfaction value. Then interaction is measured by the value of weight. It denoted by $0 \le w_{xy}^{k} \le 1$. The size of the file is calculated by the weight. The Importance of the old interaction value should decrease as any new interaction happens []. This issue is addressed by the fading effect parameter. It is denoted by $0 \le {}_{xy}^{k} \le 1$.

${}_{xy}^{k}$ $\frac{k}{s}$, $1 \le k \le$ $_{xy}$

The fading effect is defined as a function of time. It is recalculated when the new interaction happens. Trust metric notations are listed below in the Table1.

Table1 Trust metric notations

Notations	Description
${}_{xy}^{k}$	P_x satisfaction about k^{th} interaction with P_y
wt_{xy}^{k}	Weight of P_x k^{th} interaction with P_y
${}_{xy}^{k}$	Fading effect of P_x k^{th} interaction with P_y
rp_{xy}	P_x reputation value about the P_y
$_{xy}$	P_x trust value about P_y
rt_{xk}	P_x recommendation value about P_k
$_{xy}$	P_x service history size with P_y
A_i	A_i denotes set of acquaintance peer

Service Metric

This module is used to evaluate the acquaintance trustworthiness on the basis of service. Here calculate the competence belief and integrity belief using the service history. Competence belief represented the acquaintance satisfaction value in the past interacted. It is denoted as cb_{xy}. Competence belief is calculated by satisfaction, weight and fading effect.

cb_{xy} —$\sum_{k}^{s}$ (${}_{xy}^{k}$. wt_{xy}^{k} . $_{xy}$ Here Js the normalization co-efficient. $_{b}$ $\sum_{k}^{s}$ (wt_{xy}^{k} . $_{xy}$ .Integrity belief is denoted by $_{xy}$. The predictability of future interaction is called as integrity belief. It is calculated below.

$_{xy}$ —$\sum_{k}^{s}$ (${}_{xy}^{k}$. wt_{xy} . $_{xy}$ cb_{xy} ^{2}Here μrepresents the mean of the wt_{xy} ,fd_{xy}.

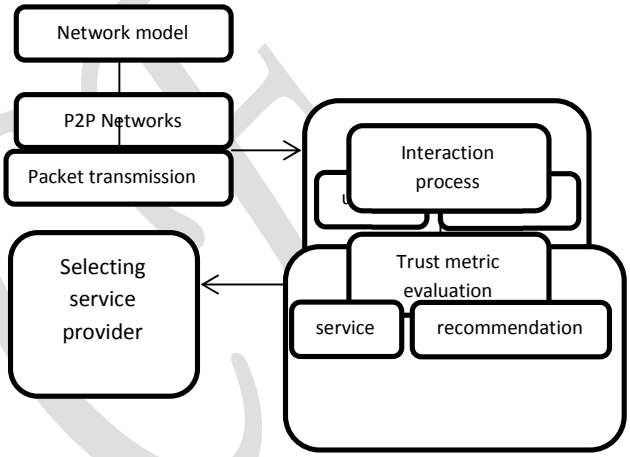

Figure. 2.Architecture diagram for P2P trust relationship

Recommendation Metric

Recommendation and reputation are used to measure the stranger's trustworthiness. The recommendation is calculated by the distributed algorithm. This algorithm shows how the P_x selects the trustworthy acquaintance and requests recommendation. Let λ_{max} denote the maximum number of recommendations. $P_x$sets a high threshold for recommendation value and request recommendation from high trusted acquaintance. After it reduce the threshold and repeats the same operations. The threshold drops under ($_{t}$ $_{t}$Value.

Algorithm1. Recommendation for P_y

1. $_{t} \Leftarrow \frac{\sum_{\in} rt_{xk}}{|\ |}$
2. $\Leftarrow \frac{\sum_{\in} (rt_{xk} \quad _{t}^{2}}{|\ |}$
3. $T \quad \Leftarrow$
4. $T_{low} \Leftarrow$ $_{t}$ $_{t}$
5. $rp_{set} \Leftarrow \emptyset$
6. While $_{t}$ $_{t}$ T_{low} $|rp_{set}|$ $_{ax}$do
7. For all $p_k \in$ do
8. If T_{low} rt_{xk} T t e

9. rec ⇐ request recommendation (p_k, p_y // calculate the recommendation value
10. $rp_{set} \Leftarrow rp_{set} \cup rec$
11. end if
12. end for
13. $T \Leftarrow T_{low}$
14. $T_{low} \Leftarrow T_{low}$ t
15. end while
16. return rp_{set}

3.4 REPUTATION METRIC

After collecting recommendation, we calculate the reputation value of P_y. P_x calculates a reputation of P_y by aggregating r_{ky} Values. Let er_{xy} denote P_x estimation about the reputation of P_y.

$$er_{xy} \quad \frac{}{e} \quad (rt_{xk} \cdot \ _{ky} \cdot rp_{ky}$$

e $\sum$ $\in$ $rt_{xk} \cdot \ _{ky}$ (Normalization co-efficient)

Then P Then P_x calculates estimations about the integrity and competence belief of P_y. It denoted by e dcb_{xy}.

$$ecb_{xy} \quad \frac{}{e \ b} \quad (rt_{xk} \cdot \ _{ky} \cdot cb_{ky}$$

$$e \quad \frac{}{e \ b} \quad rt_{xk} \cdot \ _{ky} \cdot$$

er_{xy} collected information from an acquaintance.

ecb_{xy} own experiences of P_x acquaintance with P_y.

Using the above formula calculates the reputation value.

$$rp_{xy} \quad \frac{| \ s \ |}{ax} \quad ecb_{xy} \quad e \quad 2 \quad \frac{| \ s \ |}{ax} \quad er_{xy}$$

3.5 SELECTING SERVICE PROVIDER

Selecting a service provider is based on service metric, competence belief, integrity belief and service history size. P_x download a file from an Uploader with high service trust. If service metric value is equal to select a large service history size peer.

4. EXPERIMENTAL EVALUATION

Simulation experiments show how much recommendations are used to identify the malicious peer, how much malicious attacks are mitigated. The simulation runs as cycles. The each cycle represents a particular period of time. Good peer always upload authentic files and gives good recommendation only. An attacker can perform both service and recommendation based attacks [3]. So we define four different attacker behavior 1.naive 2.discriminatory 3.oscillatory 4.hypocritical. A malicious peer network has both good and malicious peers. They don't know about each other, so they can perform attacks independently, the attacker behavior is given below.

1. *naïve:*The attacker always gives infected file and unfair recommendation about others.

2. *Discriminatory:* The attacker behaves malicious to groups of peers and attacker can perform good peer to remaining peers.

3. *Oscillatory* : The attacker can act as a good peer for long time period. Then it behaves like a naïve after it behave as a good peer again.

4. *Hypocritical*: The attacker behaves like a malicious peer for x percent probability.Another time it behaves as a good peer.

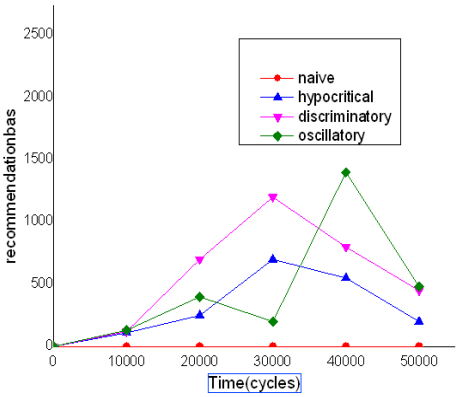

Figure. 3. Recommendation based attacker behavior

These are all the attacker behavior. It's common for both individual and collaborative attacks. Individual means malicious peers do not know about each other. Collaborators means they know about each other. It can perform good peer with each other and it perform malicious to non-malicious peer. The simulation results show the naïve performance is completely reduced and the remaining attacker performance are highly reduced better than existing methods. Figure 3 represents the attacker behavior in the proposed system. So the proposed system produces enhanced security to P2P file sharing.

5. CONCLUSION

In P2P networks, we make trust relationship between two different peers to isolate the malicious peer. This could be done by three different context service, reputation and recommendation. These contexts are defined to measure the service provider and recommendation capabilities of the peers. Past interaction and recommendation are calculated by weight, satisfaction and fading effect. These parameters provide better assessment of trustworthiness. The simulation performed individual and collaborative attack. It provides result in different attacker behavior. The proposed system completely reduces the naïve performance and enhance the P2P file sharing security.

REFERENCES

[1] L.Liu and L.Xiong, *"peertrust: supporting reputation based trust for P2P ecommerce communities," IEEE trans.* Vol .16, pp. 843-857, July 2004

[2] Z.Despotovic and K.Aberer, *"Managing trust in P2P information system,"10th Intl conf. Information and knowledge management.* 2001

[3] Bharat Bhargava and Ahmat Burak,*"A self organizing trust model for P2P systems"*, Jan 2013

[4] H.Garcia,S.Kamvar and M.Schlossaer,*" Eigen trust algorithm for reputation management in peer-to-peer metworks,"* Proc.12th www conf, 2005

[5] J. Kleinberg,*" the small world phenomenon: An algorithmic perspective", 32nd ACM symp*. Theory of computing, 2000