International Journal of Electrical and Computer Engineering (IJECE)
Vol. 7, No. 6, December 2017, pp. 3515~3520
ISSN: 2088-8708, DOI: 10.11591/ijece.v7i6.pp3515-3520

A Reliable Peer-to-Peer Platform for Adding New Node Using Trust Based Model

Vimal S.[1], Srivatsa S K.[2]
[1]Research Scholar, Sathyabama University, Tamilnadu, Chennai
[2]Retired Professor, MIT, Anna University, Tamilnadu, Chennai

Article Info

Article history:

Received Mar 30, 2017
Revised Apr 25, 2017
Accepted May 25, 2017

Keyword:

Trust management
Security and reputation aggregation

ABSTRACT

In order to evaluate the trustworthiness of participating peers in unstructured peer-to-peer networks, Reputation aggregation methods are used in this method. Each and every peer of the network will collect the local scores of each transaction and will compute global scores by aggregating all the local scores with the help of global scores, each individual peer can interact with its suitable peers. But the existing method will not consider the score of the new peer. In this condition, requests are handled by existing peers who leads to failure in downloading process. To rectify this, NP-TRUST model is used to distribute the request to all peers including the newly joined peers. The proposed method is compared with gossip and DFR-TRUST model in Transaction Success rate and variation in file request.

Corresponding Author:

Vimal S,
Sathyabama University,
Tamilnadu, Chennai.
Email: vimalshan@gmail.com

1. INTRODUCTION

P2P networks are attaining more attention now by the way of file sharing. In file sharing, every peer can join the network and download files. Due to open nature and anonymous network an ideal environment for malicious peer to spread virus is offered by the system. Reputation aggregation methods are used to avoid downloading inauthentic files. The trust of the system will show the reliability and safety of peers and quantified trusts [1], [2] are known as reputation score by these trusts, individual peer will avoid transaction with malicious peers. The peer with high reputation score will provide safe files in high probability, thus every peer will select peer with High reputation score. Two types of reputation scores are; 1) Global score, 2) Local score.

In all the transaction, peer receives a file to evaluate its reliability with help of local score. By aggregating local scores, every peer will share a unique global score. Then each peer refers to global score and selects the transacting peer whose global score is high. If peer foes not send a file to others then local score is not calculated. Also if global score of peer is not enough, then peer is not selected as uploader. The main purpose of DFR-TRUST model is to distribute the file requests among peers to provide safe file with high probability. In DFR-TRUST model, local score calculation will not depend on number of file providing and also will select middle evaluated peers. In P2Pnetwork, departure and participation of peers [3], [4], [5] occur frequently, thus the number of high evaluated safe peer's decreases with peer's departure.

The purpose of NP-TRUST model is to distribute file requests among safe peers; this will include newly joined peers and initial peers. By giving chances new peers to be evaluated intentionally, file requests are distributed among all safe peers and new peers are utilized as up loader. By this way, NP-TRUST model avoids concentration of file requests on portion of safe peers.

2. RELATED WORKS

In this section, we explain about reputation aggregation method, its related work and their problem.

2.1. Method for Reputation Aggregation

This method is introduced to evaluate peers in P2P and thus it will avoid downloading inauthentic files. There are two values. One is local score which is the trustworthiness of peer and local score is calculated for all the transaction. Local score is defined with peer i, file downloaded evaluates peer j, as Lij [5], [6]. Peers who received the file evaluates sender by the quality of received file. Other value is global score which is aggregated score of local scores and it is used to decide which peer is reliable. Global score is defined with peer j by peer i as v_{ij}. By selecting the high global score peer; each peer can avoid transacting with malicious peers.

The Eigen Trust algorithm aggregates trust information by having peers, to perform a distributed calculation of vectors of trust matrix. Power Trust leverages the power law distribution of peer feedbacks to fast aggregate global reputations. e.g, Freenet, Gnutella, Kazan. Gossip Trust and ILGT were introduced for unstructured P2P. They support computation of aggregate functions. These mechanisms are adoptable to peer dynamics and robust to disturbance of malicious peers. Although problem that file request concentrate on existing high reliable peers. DFR-TRUST model was proposed to avoid file request concentration problem.

2.2. DFR-TRUST

This extends the reputation aggregation algorithm of Gossip Trust to combat malicious peers. All peers will hold local scores and will calculate global scores by exchanging local scores [1]-[3]. The purpose of DFR-TRUST model is to avoid transacting with malicious peers. It will deal with problem that file requests concentrate on portion of highly evaluated peers. To distribute file requests among safe peers, it is necessary to avoid variation of global scores because global scores are used as selection probability of up loader. The number of times that these peers are evaluated increases will lead to distribution of file request.

a. Peer Separation

In DFR-TRUST model, whenever each peer decides a transacting peer, peer refers to global scores. The peers are divided as high reliability peer, low reliability peer and middle reliability peer. The global scores of middle reliability peer are not polarized and are decided as malicious. The threshold between low and middle reliability peer are calculated by peer ias v_i and between middle and high reliability peer as v_{hi} as

$$\overline{v_i} = \frac{1}{N}\sum_{j=1}^{N} v_{ij}$$

Where N = Number of all peers in the network

$$\overline{v_{hi}} = \frac{1}{N_h}\sum_{j=1}^{N_h} v_{ij}$$

Where NA = Number of peers whose global score are higher than $v_{i.}$

b. Manipulating neighboring Scores

Whenever each peer downloads a file, downloader's will calculate local score of up loaders. Each peer will change the calculation method according to peer. Each peer will calculate $r_{ij}(x)$ when peer i downloads from peer j for x times, where $r_{ij}(x)$ is the reputation score that peer i has against j. Peer i normalizes all Rij which peer i calculates for peer j($1 \leq j \leq N$)

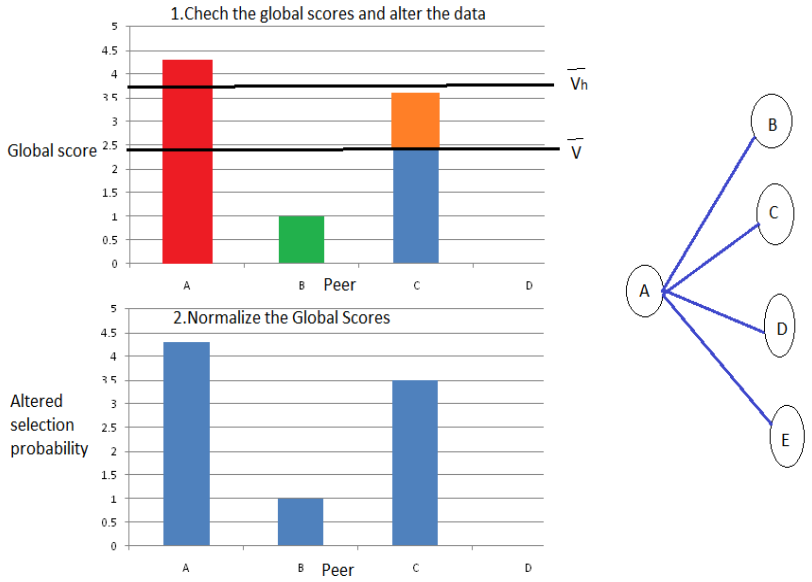

Figure 1. Selection probability in the alteration

To make middle reliability peers as transacting peer by Figure 1, each peer will alter the selection probability of transaction peer according to peer division when using global scores for selection probability. If there is a middle reliability peer among peers, downloader's alter the global score of middle reliability. After this alteration, downloader will normalize the global scores of reply peers including altered global scores of middle reliability peers and uses them as selection probability.

2.3. Related Work Problems

In P2P networks, due to frequent participation and departure of peers, the highly valuated safe peers decrease with peer's departure. Then, many file requests concentrate on a portion of safe peers participating from beginning which are defined as initial peers. However, reputation [7]-[9] system will not consider reputation scores of new peers. DFR-TRUST model is used to distribute file requests among safe peers does not cope with problem and fails to distribute the problems are: 1) New peer cannot reply to file requests since they do not have initial files to upload 2) New peer's global scores are set as 0 at the beginning 3) Calculation method of local scores stands on number of provision of files.

3. NP – TRUST MODEL

The NP- TRUST model will consider the reliability of new peers and will calculate global scores. The main purpose is to distribute files requests among safe peers (both initial and newly joined peers). NP-TRUST model has three phases. In this paper we will see about the phases of NP- TRUST model in the following chapters.

3.1. To Supply Initial Files to New Peers

In this phase, to deal with the lack of initial files for new peers, other peers will supply some initial files to it. The peer which is supplying initial files to new peers is called as supplier peer. The two main roles of supplier peers are 1) Low or middle reliability peer and 2) Newly joined peers. The low reliability peers are likely to be imposing download limitation by tit-for-tat mechanism. The new peer needs the chance for evaluation. For the first time, new peer will send requests for initial files. The peers which receive the request will calculate number of needed files and will supply it. The new participating peer will receive all supplied files because it does not know global score of each supplier. However, receiving an inauthentic file from supplier, the new peer will deny initial file supplied by same supplier.

3.2. New Peer Selection

This phase will deal with the problem of lack of evaluation chances of new peers. The global score of new peers are set to 0 when participating in the network. Thus they are not selected as uploaders. When downloader makes a query for file, reply peers as new peers if falling under both of following,

i) Global score of reply peer is 0

ii) Downloader have not downloaded and uploaded to reply peer.

If there were several new peers, a downloader will select one peer randomly. If there were no new peer, downloader selects uploader as usual. Once peers are treated as a new peer, downloader selects new peer in certain probability β_k.

$$\beta_k = \theta_k * E$$

Where E is the constant of selection probability.

3.3. Local Score Calculation

In this phase, the local score of peers are calculated shows in Figure 2. The local scores are set to low in comparison to initial peers, evaluation chances of new peers also get low. Receiving a file, each peer i calculates local scores against peer j L_{ij} where peer j is the sender of file. Local score is calculated as,

$$L_{ij} = \begin{cases} \dfrac{Rs_{ij} - Rv_{ij}}{Rs_{ij} + Rv_{ij}} & (Rs_{ij} \geq Rv_{ij}) \\ 0 & (\text{otherwise}) \end{cases}$$

Where R_{sij} denotes all provision times of safe files from j to i and R_{vij} denotes all provision time of inauthentic files from j to i.

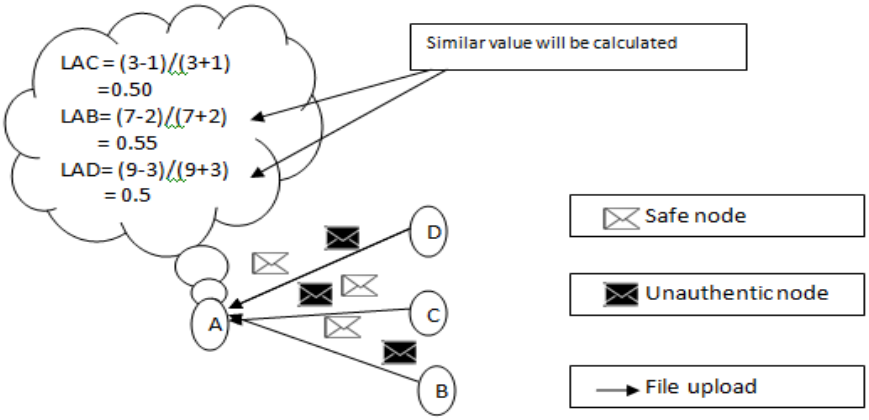

Figure 2. Local scores of NP-TRUST

4. PERFORMANCE EVALUATION

The effect of NP-TRUST is discussed by comparing with DFR and Gossip Trust. To compare, we simulate Gossip trust and DFR-TRUST at same time. Evaluated terms in global [10] safe peers score, success rate in the downloading of files and number of selected time as uploader.

4.1. Setting Up Simulation

Here the inauthentic file provision probability of safe peers is set to 0.05 because we consider that safe peers involuntarily provide downloaded inauthentic file. On other hand, inauthentic file provision probability of malicious peers is set to 0.5. The probability of providing inauthentic file by malicious peers gets highest when inauthentic file provision probability of malicious peers is set to 45%. Aggregation [11]-[13] cycle of global scores is 1000.

Participation and Departure Model: The number of participating and departing peers is set to same ratio 8% of all peers. Thus, as aggregation times increases, ratio of new peers decreases gradually. If departed peer participate to network again, peer is managed by new peer. Malicious Peer Model: This model provides inauthentic files at constant rate. And they do not run tactical attack the malicious peer attack which tries at exploit reputation aggregation method. The tactical attack is attack which malicious peers provide safe files until their global scores get high and provide inauthentic files.

4.2. Confirmation for Selecting New Participating peers as an Uploader

The ratio of malicious peers is 0.5N and the probability of providing inauthentic files of malicious peer of 60%. We confirm independent files to new peers. The average number of selected times as uploader is set to 0 when new peers are only supplied initial files and global scores are set to 0. As the aggregation cycle increases, average number of transaction of initial peers increases. Although number of new peers does not increase significantly which means that file requests concentrate on initial peers. Then, we should confirm the independent effect of global scores of new peers. These scores are set to average of global scores of all peers. We got almost same results. This means that file requests concentrate on initial peers. From these outcomes, we can say that utilizing tow countermeasures individually is not effective. Thus, we combine these countermeasures to diversify the file requests.

4.3. Number of Selected Times as Uploader

We use DFR and Gossip Trust to compare with NFR-Trust [14], [15] regarding number of selected times as uploader. This simulation is executed for investigating whether file requests are distributed among safe peers. The selected times of new peers are high while malicious peers are kept low in NP-Trust. This means file requests are distributed to new peers. Although in Gossip Trust, few of new peers are utilized as uploaders and requests have concentrated on portion of initial peers.

The standard variation of selected times as uploader of safe files in NP-TRUST model is one third of the DFR-TRUST model and one tenth of the Gossip Trust. Thus the selected times of safe peers are balanced in NP-Trust, file requests are distributed as expected. The reason that NP-Trust has accomplished the distribution is because NP-Trust gives chances to new peers to be evaluated. It supplies new files to new peers and global scores of new peers are valuated high. In Gossip Trust, it does not have mechanism to evaluate the new peers. Thus peers are rarely selected as uploaders.

4.4. Global Scores of Safe Peers

The three methods are compared in terms of global score. If the scores do not converge to that of critical peers, new peers are likely to be selected as uploader. The average of global scores within evaluates initial safe peers and new peers. We confirm how global scores change when aggregation [16], [17] cycle increases and ratio of initial peers decreases.

NP-Trust use calculation method of local scores which express radical reliability soon and thus the convergence is fast. DFR-Trust shows in Figure 3 needs some aggregation cycle to calculate local scores. Thus reliability of initial peers is high when compared to new peers. The global scores of initial peers get high. Therefore some aggregation times are needed to calculate global score of new peers. Thus the provision time of new peers is fewer than that of initial peers because participating times are different. Therefore global scores are kept low and do not converge on radical reliability.

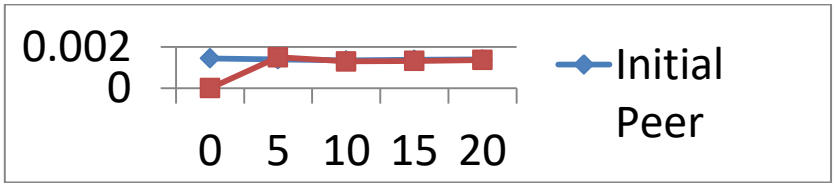

Figure 3. Aggregation cycle of NP-TRUST

4.5 Success Rate of Downloading Files

The success rate of downloading files is evaluated during three methods. The success rate of downloading files of NP-Trust is 8% higher than that of DFR trust and 10% higher than that of Gossip Trust. In NP-Trust, the global scores of new peers are calculated same as that of initial peers if their reliability is equal. Thus the number of download failure is avoided because there is no concentration of file requests to some safe peers. The number of downloaded inauthentic files gets higher than that of NP-Trust because global scores of initial malicious peers are relatively high compared to new peers.

5. CONCLUSION

Thus NP-Trust has been proposed whose purpose is to distribute file requests to safe peers which include initial peers and new peers as well. Chances are given to new peers to evaluate and create evaluating mechanism. Calculation method of local scores in NP-Trust does not rely on file provision times. Thus global

scores of new peers are high when compared to initial peers. As a future work, it is necessary to handle peer, which misapplied the preferential treatment for new peers and detect peers that repeatedly joins and leave for attack.

REFERENCES

[1] M. Hefeeda and O. Saleh, "Traffic modeling and proportional partial caching for peer-to-peer systems", IEEE/ACM trans.Networking 2008, Vol. 16, Issue. 6, pp. 1447–1460, December. 2008.
[2] R. Xiang, J. Neville, and M. Rogati. Modeling relationship strength in online social networks. In *Proc. of WWW*, 2010.
[3] G. Salton, A. Wong, and C. S. Yang. A vector space model for automatic indexing. *Communications of the ACM*, 1975.
[4] J. Erman, A. Mahanti, M. Arlitt, and C. Williamson, "Identifying and discriminating between web and peer-to-peer traffic in the network core", ACM WWW 2007, pp. 883–892, May. 2007.
[5] R. Zhou, K. Hwang, and M. Cai, "GossipTrust for Fast Reputation Aggregation in Peer-to-Peer Networks", IEEE Trans. on Knowledge and Data Engineering, vol. 20, Issue. 9, pp. 1282–1295, 2008.
[6] J. Meserve, "P2P traffic still dominates the Net," Network World, August 2005.
[7] B. Cha and J. Kim, "Handling Fake Multimedia Contents Threat with Collective Intelligence in P2P File Sharing Environments", P2P, Parallel, Grid, Cloud and Internet Computing, pp.258-263, November 2010.
[8] A. Matsumoto, Y. Mashimo, M. Yasutomi, and H. Shigeno, "ILGT: Group Reputation Aggregation Method for Unstructured Peer-to-Peer Networks", ICPADS 2010, pp. 197–204, December 2010.
[9] A. Matsumoto, M. Yasutomi, and H. Shigeno, "Distribution of File Requests Using Trust Aggregation Method for Unstructured P2P Networks", Information Processing Society of Japan, Vol.53, No.2, 2012.
[10] T. Yajima, A. Matsumoto, and H. Shigeno, "Hub Node Reinforcement against Forwarding Obstruction Attacks in Peer-to-Peer Networks", Network-Based Information Systems (NBiS2011), pp.388-393, September 2011.
[11] S. Kamber, M.Scholosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks", ACM WWW 03, pp. 640–651, May 2003.
[12] R. Zhou, and K. Hwang, "PowerTrust: A Robust and Scalable Reputation System for Trusted P2P Computing", IEEE Trans. on Parallel and Distributed Systems, pp.460-473, April 2007.
[13] K. Albrecht, R. Arnold, M. Gahwiler, and R. Wattenhofer, "Aggregating information in peer-to-peer systems for improved join and leave", IEEE P2P 2004, pp. 227–234, 2004.
[14] T. Yajima, A. Matsumoto, and H. Shigeno, "PTrust for Reputation Aggregation in Peer-to-Peer Networks", 1st International Symposium on Access Spaces (IEEE-ISAS 2011), pp. 180–185, June 2011.
[15] J. Mao, Y. Cui, j. Huang, and J. Zhang, "Modeling and Analysis of Resource's Load-Scale in P2P Network", CMC 2009, January 2009.
[16] K. Walsh and E. Sirer, "Experience with an object reputation system for peer-to-peer file-sharing", Symposium on Networked Systems Design and Implementation (NSDI 2006), May 2006.
[17] C. Binzel and D. Fehr. How Social Distance Affects Trust and Cooperation: Experimental Evidence from A Slum. In *Proc. of ERF*, 2009.

BIOGRAPHIES OF AUTHORS

Vimal S received his B.E degree in Computer Science and Engineering from Anna University and the M.Tech Degree in Information Technology from Sathyabama University Chennai. He is currently a Ph.D. student in the Department of Computer Science and Engineering at Sathyabama University, Chennai.

Srivatsa S K Retired Professor, MIT, Anna University, Chennai. He has published more than hundred and twenty National and International journals and Conferences. He also Guided many Research Scholar.