IMPROVING HYBRID REPUTATION MODEL THROUGH DYNAMIC REGROUPING

Sreenu G [1] and Dhanya P M [2]

[1] Department of Computer Science, RSET, Rajagiri valley, Cochin, India
gsreenug@gmail.com
[2] Department of Computer Science, RSET, Rajagiri valley, Cochin, India
dhanya.rajeshks@gmail.com

ABSTRACT

Peer-to-Peer (P2P) systems have the ability to bond with millions of clients in business and knowledge scenario. The mechanism that leads users to distribute files without the need of centralized servers has achieved wide recognition among internet users. This also permits for a range of applications further than simple file sharing. he main problem lies in the fact that peers have to customarily intermingle with mysterious peers in the absence of trusted third parties. Usually the lack of incentives often makes these strange peers to act as freeriders and thus reduce the system performance. The trustworthiness among peers is portrayed by applying the knowledge obtained as a result of reputation mechanisms. This paper endows with a new reputation model in association with a detailed survey of diverse reputation models. The proposed model suggests a hybrid reputation model through dynamic regrouping..

KEYWORDS

Hybrid Reputation, Compatibility Coefficient, Group splitting

1. INTRODUCTION

Presently the thought of P2P system has been fascinated plenty of curiosity in the network field. The sophisticated features like decentralized processing, independent nature of nodes and scalability makes the system more advantageous. One of the prevailing features that differentiate P2P system is the overlay network. Overlay network allows the P2P systems to connect diverse systems on top of existing network configurations.

Overlay network supports an open environment which in turn supports participation of all types of nodes. The presence of malicious nodes cannot be easily detected in the case of an open network and it raises a severe problem to the security of the network. On the better side the open nature of P2P network can be used to share the computing resources but the open nature itself creates a hazardous state through the inclusion of malicious peers. These malicious peers can diminish the system popularity by degrading the performance through malicious behavior like altering the message when it is passing through the transmission medium and denial of services of other peers.

To increase the number of participants the system must be competitive to provide good quality of service. As the number of participants increases the performance of the system will increase. On hand techniques to address these security issues include reputation mechanism, cryptographic techniques, and access control and data integrity mechanisms.

DOI : 10.5121/ijp2p.2012.3301

This paper summarizes features of different reputation models along with proposed hybrid reputation model. Hybrid reputation model suggests a new reputation model for finding the reputation score of each peer through group formation. It demonstrates the different procedures involved in the formation of groups, trust calculation and behavior judgment. Furthermore, the paper discusses the main advantages and issues identified in the model. Finally the projected result analyses the possible outcome of the project.

2. EXISTING SOLUTIONS

The P2P systems are facing the main problem of communication with strangers. So the whole thing is based on mutual trust among communicating peers. Trust value calculation can take input from reputation systems in the form of predictions on peer behavior in future founded on past behavior. Reputation value can also be extracted in the form of recommendations from other participating peers. A detailed survey of various reputation mechanisms includes the following methods.

1. eBAY [1]: This is a centralized reputation system as a solution to identify reputed peers involved in the transaction. The participating peers uses an online feedback system to rate other peers after each transaction and overall reputation of a participating peer is calculated as the sum of ratings over previous six months.
2. Xrep [2]: The main procedures involved in resource searching are vote polling and vote clustering. The peer will post the required service and collect the responses from all participating peers. In vote polling phase the participating peers will record their opinion about the peer. In vote clustering phase the recorded opinions will be aggregated. The peer behaviour is predicted based on the total votes collected.
3. TrustMe [3] : A bootstrap server will assign the trust value of participating peers to certain trust holding peers. These THA peers will give the trust values in response to the broadcasted queries from requesting peers. Security, anonymity and use of cryptographic keys are the main feature identified in the method.
4. NICE [4] : Cooperative distributed applications can be effectively implemented in a NICE platform. The service provider can check the reputation of the peer by considering the signed set of certificates. Moreover the service provider also conducts a search about the reputation of the peer. So finally the reputation value will be a considered as a combination of the certificates and referenced search.
5. EigenTrust [5]: EigenTrust uses concept of global trust value .Each peer is having a trust value about the peer that is globally accepted inside the network. By considering the global reputation the peer behavior can be determined as malicious or normal peer.
6. PeerTrust [6]:System architecture of PeerTrust has no central database. The trust data is distributes across the network. The trust manager associated with each peer will perform the functions of feedback submission and trust computation.
7. PowerTrust [7] : Trust overlay network is built on top of all peers in the network. Highly reputed power nodes will be selected using a distributed ranking mechanism. The PowerTrust system will take its input in the form of local trust scores send by peers after each transaction. The global reputation value of each peer will be calculated by the PowerTrust system by aggregating all the local trust scores.
8. FuzzyTrust [8]: Approximated reasoning is highly supported by FuzzyTrust. Uncertainty, fuzziness and incomplete information is better handled by FuzzyTrust. FuzzyTrust applies fuzzy inference on local trust value calculation and uses fuzzy inference to obtain global reputation aggregation weights.
9. GossipTrust [9]: Suggests a reputation aggregation scheme for unstructured networks.The process itself includes different steps and cycles. The peers are exchanging local scores

with randomly chosen neighbours and update the peers trust value. This repeats and finally the trust value congregates in one cycle. The next cycle will use the previous cycle congregated value and again find the new congregated value.The main feature is the method aggregate the reputation values in a completely distributed and scalable way.

10. Dual-EigenRep [10]: The method considers the recommended and recommending roles of each peer. The unified association between these two behaviors finally forms different trust communities which categorize different types of peers.
11. Three-Dimensional Based Trust Management Scheme for Virus Control in P2P Networks [11]: The method reflects on the trust values of peers and infection values of both the peers and content. A three dimensional normalization is used in ratio based normalization models to enhance the efficiency on the trust value computation.

2.1. Assessment of assorted active Methods

The above methods can be analysed in different ways. The main advantages and disadvantages analysed in different methods can be illustrated in the following way.

1. eBAY: A central server is present to manage the reputation values. The advantage is that users can put their feedback in an online feedback form. It is an actually used reputation system. The feedback can be recorded using numeric values. The main disadvantage is the lack of security.
2. Xrep: The main advantage is that the method combines the peer based reputation and resource based reputation. The disadvantage is that increase in the number of resources compared to number of peers will create astorage overhead problems.
3. TrustMe: The anonymous nature of storage of reputation values will create a secure environment. The performance will be affected if the network size is very large. As result of this method lots of messages will be generated. Furthermore the large network size will result a delay in time taken to transfer the global reputation value among peers.
4. NICE: The search and inference performance of the system will be enhanced if the users store added information. One drawback is the method not describing about the speed of transactions.
5. EigenTrust: Use of power iteration provides a distributed and secure method to compute global trust value. The inference that the peers which exchange trusted files will report sincere trust values is one disadvantage.
6. PeerTrust: The method will deal with the deceitful feedbacks and also handle the lack of incentives problem. The problem identified in this method is that it is not easy to implement in large scale P2P networks.
7. PowerTrust: The functioning competence can be achieved through the presence of power nodes. Since the power nodes can act as hotspots there is a chance congestion in the network.
8. FuzzyTrust: The malicious peers can be detected in a fast manner. The problem identified is that the method is not handling the collusion attack and freeriding .
9. GossipTrust: The application of bloom filters can be used for efficient reputation storage and identity based cryptography is used for secure communication. The drawback identified is that there is no method is defined to punish the malicious nodes.
10. Dual-EigenRep: The method is very efficient against different types of security issues like collusion,disguise and exaggeration.The method is not mentioning about the speed of transactions.
11. Three-Dimensional Based Trust Management Scheme for Virus Control in P2P Networks: The propagation of virus can be limited to a small number of peers. The main feature is that these activities will not affect the file downloading process. The method is not mentioning about the transaction speed.

An assessment of above listed methods shows that some of them are efficient in detecting malicious peers. Some methods are efficient in efficient storage of reputation scores, and others are useful in efficient computation of trust values. This paper suggests a hybrid reputation model which brings together all these factors to provide an efficient reputation model.

3. Proposed Solution

The proposed model focuses on the group formation based on the similarity of functions. All the participating peers will have a set of services and requirements. The requirements and services are needed to be shared among other participating peers. Functions are the combinations of services and requirements. Mutually complementing functions will share same group. The functional similarity is evaluated with the help of Compatibility Coefficient (CC). The CC computation is done through prefixed threshold values.

Different peers can communicate within their group through intra group communication and different groups can communicate through inter group communication. In order to analyse the peer behaviour the trust value is evaluated. The peers with a trust value below the fixed threshold will consider as malicious and are prohibited from further communication. Furthermore based on the transmission rate the groups will be regrouped. The necessity of group splitting and precise behaviour forecasting will be explained in later sections. Figure 1 represents a model of the proposed hybrid reputation model.

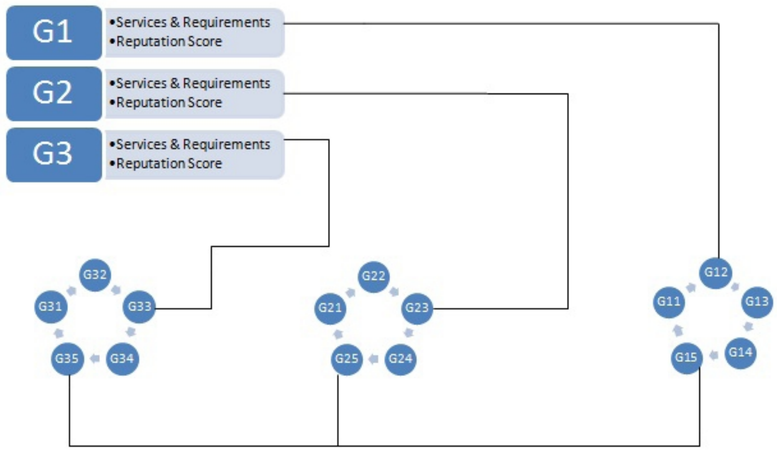

Figure 1. Model of the proposed system [12]

The detailed procedure of Hybrid Reputation Model is explained in following divisions.

3.1. Node Registration at central coordinator

The initial procedure of the system is node registration. This procedure is done at the entry point of the system that is the central coordinator. During registration the nodes will list their services and requirements.

3.2. Compatibility Coefficient (CC)

The central coordinator will calculate the CC value. The function of central coordinator is the computation of CC value and group peers according to CC value.

3.3. Calculation of CC

Based on the calculated CC value the participating peers are categorized into different groups. Each group should have a coordinator. The peer which led to the formation of a new group will act as the coordinator for that group. The CC value calculation is done by fixing two threshold values t1 and t2. Initially the opening node will act as the coordinator for the first group. All the arriving nodes will send their services and requirements with already existing group coordinators. The group coordinators will calculate the CC value between their group and arriving node. The central coordinator will compare the CC value calculated in all coordinators.

The CC value will be incremented by 1 if there is a match in between the services of arriving node i and requirements of coordinator node j and vice versa. Finally the CC values will be aggregated and compared with threshold values.

3.4. Group Formation

The central coordinator will compare the CC value of different group coordinators and initiate the group formation.

1. If the CC value between arriving node i and coordinator j is above threshold t1 then node i will join with coordinator j.
2. If the CC value is below threshold t2 the arriving node will form a new group.
3. If the CC value between arriving node and different coordinators is between t1 and t2 a regrouping will be performed.
4. If there is more than one group having threshold value greater than t1 then the group with highest CC value will be selected for group formation.

Figure 2 shows the diagram of peers in a group. Each peer is associated with reputation table.

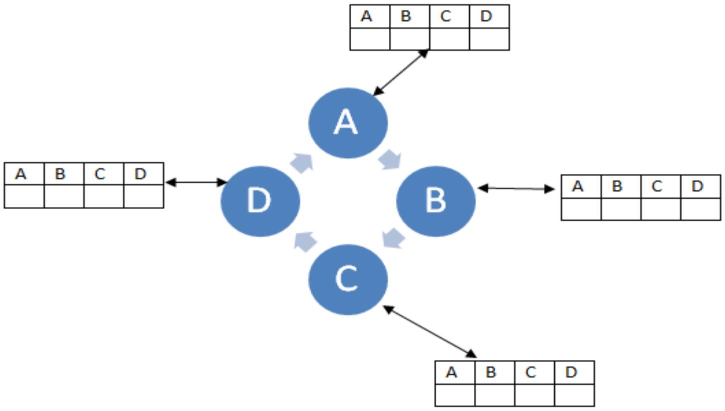

Figure 2. Group of peers allocated with reputation table[12]

3.5. Intra group Communication

Different peers in a group can communicate within their group. Each peer can satisfy other peers requirements. Since the group formation is based on similarity of functions the time taken to complete each request will be reduced.

3.6. Response Gathering

After the completion of each transaction the service requesting peers have to record their feedback about service provider. All the peers will be associated with a reputation table. The feedback about service provider should be recorded in the corresponding column of reputation table of service requestor. The reputation table contains space for all participating nodes in their group. After each local update the feedback scores will be globally updated using GossipTrust algorithm.

3.7. Appraisal of aggregated response values

The feedback recorded will represent the corresponding trust value. Each successful transaction will record a positive feedback. The positive feedback will be added by 1 and negative feedback will be decremented by 1. Before each transaction the peers will verify the reputation table. If the feedback (trust value) recorded for a node is below a fixed threshold the node will be consider as malicious and avoid from the remaining communication.

3.8. Intergroup Communication

If the requests for a peer will not satisfied within their group the request will be forwarded to other group coordinators. The group coordinators will check within their group and send a reply to the requestor coordinator if the requested service is available with required trust value.

3.9. Dynamic Regrouping

The size of each group is fixed based on the transmission rate within their group. After the joining of a new peer each group will be examined for its transmission criteria. The transmission criterion is evaluated using following parameters.

1. Number of packets per second
2. The available bandwidth

If the number of packets per second exceeds the available bandwidth the group will be divided.

3.10. Group splitting

At regular intervals of time the central coordinator will split the groups and reorder the groups. This reordering will help to avoid the malicious nodes from appearing to the next level. This will also reorder the nodes based on the changes in services and requests.

4. IDENTIFIED ISSUES AND RECOGNIZED SOLUTION IN PROPOSED MODEL

The chance of failure of central coordinator and group coordinator should be handled effectively. The failure of central coordinator can be handled by applying election algorithm [13] among the existing group coordinators. The group coordinator failure can be handled by applying election algorithm within the group itself.

5. GUARANTEED QUALITIES OF THE SYSTEM

5.1. Less Flooding

Since the peers are arranged in different groups most of the requests will be satisfied within the group. So unnecessary flooding can be avoided.

5.2. Small Sized Reputation Table

Each peer has to store a reputation table which containe entries for the peers in the same group. So the size of reputation table can be reduced.

5.3. Fast access

Less flooding will naturally reduce the access time.

5.4. Enhanced quality

The grouping of peers will limit the number of peers in each groups and that in turn reduce the traffic in each group. Reduced traffic will avoid congestion and loss of packets. All the services will be provided with less delay and high quality.

6. RESULT ANALYSIS

The proposed model suggests a less delayed high quality reputation model. The inclusion of regrouping will increase the transmission quality and the inclusion of group splitting will reduce the chance of malicious peers. The application of group splitting will not allow malicious peers from past transactions to enter into new transactions. So the reduction of malicious peers can be seen in each step after group splitting. The quality of a transmission consists of the reduction in transmission delay, fast detection of malicious peers and the large number of successful requests. The expected outcome of the project as plotted in Figure3, 4and 5 shown the above discussed three factors.

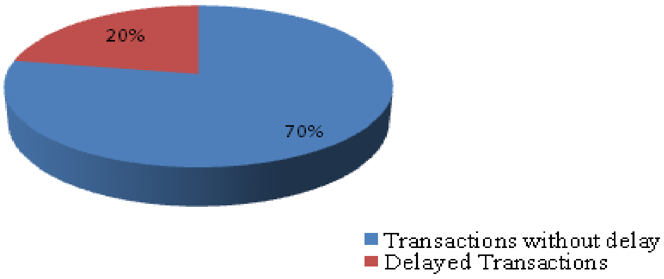

Figure 3. Transaction delay

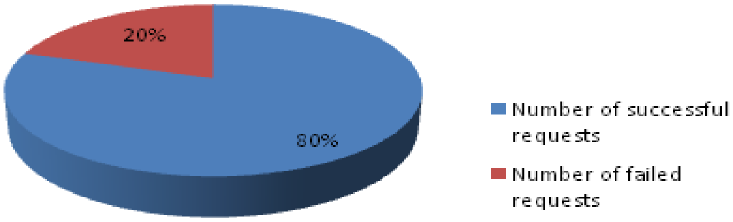

Figure 4. Number of Successful Requests

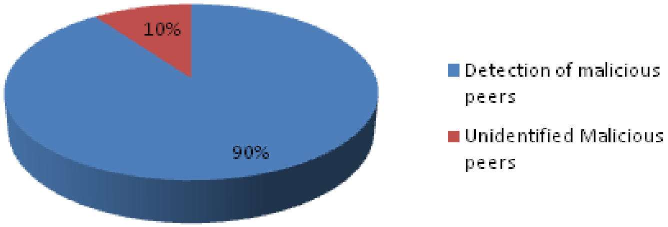

Figure 5. Detection of Malicious peers

7. CONCLUSION

A detailed study of existing reputation models is presented with a good analysis. The proposed model is a solution to the identified deficiencies in the existing methods. The entire working is illustrated in different steps including group formation, trust calculation and behavior determination. The paper also discusses the merits and demerits of the proposal. The identified solutions for these drawbacks are also presented. Finally the expected result is explained with the help of different pie charts.

REFERENCES

[1] eBay. eBay home page, (2009) http://www.ebay.com..

[2] E. Damiani, S. Vimercati, S. Paraboschi, P. Samarati, and F. Violante, (2002) ”A Reputation-based Approach for Choosing Reliable Resources in Peer-to-Peer Networks”, ACM Symposium on Computer Communication Security, pp.207 -216.

[3] A. Singh and L. Liu, (2003) “TrustMe: Anonymous Management of Trust Relationships in Decentralized P2P Systems”, IEEE IntI. Conf. on Peer-to-Peer Computing, pp.142-149.

[4] S. Lee, R. Sherwood, and B. Bhattacharjee, (2003) Cooperative peer groups in NICE.

[5] D. Kamvar, M. Schlosser, and H. Garcis-Molina, (2003) "The EigenTrust Algorithm for Reputation Management in P2P Networks," Proc.Word Wide Web Conf. (WWW2003), ACM Press, pp. 640-651.

[6] L. Xiong and L. Liu, (2004) “PeerTrust: Supporting Reputation-Based Trust for peer-to-peer Electronic Communities”, IEEE Transactions on Knowledge and Data Engineering,16(7):843–857,Second International Conference on Availability, Reliability and Security (ARES'07)

[7] R. Zhou and K. Hwang, (2006) "PowerTrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing" IEEE Trans. Parallel and Distributed Systems., vol. 18, no4 , ppA60-473.

[8] S. Song, K. Hwang, R. Zhou and YK. Kwok, (2005) ”Trusted P2P Transactions with Fuzzy Reputation Aggregation”, IEEE Internet Computing, Vol. 9, No. 6, pp.24-34.

[9] R Zhou and K. Hwang, (2007) "Gossip-based reputation aggregation for unstructured peer-to-peer networks," in Proceedings of IEEE International Conference Parallel and Distributed Processing Symposium, pp. 1-10. V3-23.

[10] Xinxin Fan, Mingchu Li, Yizhi Ren and Jianhua Ma, (2010) “Dual-EigenRep: A Reputation-based Trust Model for P2P File-Sharing Networks”uic-atc,pp.358-363, Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing.

[11] Lin Cai and Roberto Rojas-Cessa, (2010) "Three-Dimensional Based Trust Management Scheme for Virus Control in P2P Networks," Proc. IEEE ICC 2010, 5 pp., Cape Town, South Africa, May 23-27.

[12] Sreenu G, Dhanya P.M,(2012) “ A Hybrid Reputation Model through Federation of Peers Having Analogous Function “ , Advances in Computer Science , eng.& Appl., AISC 166,pp.837-846.springerlink.com

[13] Andrew S. Tanenbaum , (1994) Distributed Operating Systems, Prentice Hall; 1 edition

Authors

1. Sreenu G is a post graduate student in M.Tech CSESIS, Department of Computer Science and Engineering, RSET, Kochi, INDIA. Her interested areas are reputation models in P2P security and Distributed computing. She has been working as a lecturer in the same department.

2. Dhanya P.M is working as Assistant professor in the Department of Computer Science and Engineering, RSET, Kochi, INDIA. Her areas of interest are P2P networking, Distributed Computing and natural language processing. She is now a research scholar in CUSAT, KOCHI.