

Balanced Reputation Detective System (BREDS): Proposed Algorithm

Pallavi Bansal¹, Narender Singh²

^{1,2}Computer science & Engineering department, G.I.T.M, Bilaspur, Yamunanagar, Haryana

Abstract -In the past, many reputation systems tried to distinguish malicious peers from other honest peers. The reputation of a peer is calculated by summarizing complains of his neighbors who have interacted within. In P2P every peer must keep transaction records. If a peer wants to download a file from providers, he cloud review the transaction records and selects a best provider. After examined Peer-to-Peer network and problems in Peer-to-Peer network it is concluded that there must be a system that minimize these problems. A reputation system is a good choice for handling these types of problem. Because of the open nature of P2P models, the Selfish phenomenon is popular and degrades the system performance. Anonymity may exacerbate this problem since the Selfish cannot be located, and since selfish behaviors might be prevalent without any punishment. So objective of this paper is to design a reputation system for Peer-to-Peer network that can handle Selfish problem in this network efficiently with minimum network load.

Key Words: Peer-to-Peer Network, Reputation Management, BReDS

1. INTRODUCTION

Peer-to-Peer networking is mostly known under the brand of Napster. Within this application the Peer-to-Peer networking concept is used to share files, i.e. the exchange of MPEG Layer3 (mp3) compressed audio files. However Peer-to-Peer is not only about file sharing. it is also about establishing multimedia communication networks based on Peer-to-Peer concepts or resource sharing. A basic problem we often encountered is the multifaceted and confusing situation, concerning the terms related to Peer-to-Peer networking in publications and discussions. Often *Peer-to-Peer* is used without having clearly stated the meaning of *Peer-to-Peer*. Thus it may happen, that sometimes in discussions the term *Peer-to-Peer* is used with completely opposing meanings. The central theme of this poster therefore is to bring in a clear definition of *Peer-to-Peer* networking and its different facets, like e.g. "Hybrid" *Peer-to-Peer* networking. Further on we also give a definition of the classical *Client/Server* architectural concept, to make a distinctive delimitation to *Peer-to-Peer* network architectures possible. The emerging peer-to-peer model has

recently gained major attention due to its high potential of sharing huge amount of resources among millions of networked users, where each peer acts as both a resource provider and a consumer. A dilemma in P2P computing area is that when every participating peer tries to maximize its own utility, the overall utility of the collaboration might drop. In the worst case scenario, P2P resources are easily depleted due to selfish users take free rides without offering any sharing resource. Unfortunately, such "tragedy of the commons" phenomenon also happens in a number of existing peer-to-peer systems where cooperated scientific research systems emphasize on sharing resource voluntarily. Apparently, certain resource management scheme has to be implemented on P2P systems to ensure them working properly and growing healthily. In a P2P model, a resource to be searched in a P2P overlay network may take one or more hops to be found. Also, as the resources are decentralized and the location information of the resources is distributed, every peer has to participate in other peer's resource lookups. After a resource has been found, usually a direct connection between the two peers can be used. Thereby, peers are usually only helping in resource lookups, but the resource utilization like file download or a voice call is made directly between the corresponding peers. A fully decentralized P2P network is very difficult to shut down, as there are no central servers or other entities that the network is dependent of. In general, P2P networks potentially offer an efficient routing architecture that can be self-organizing, massively scalable and robust. They can also provide good fault-tolerance, load balancing and explicit notion of locality and wealthy peers are more trustful, is not always valid. Simply taking into consideration the bid price in resource allocation cannot satisfy the increasing security concerns from different participating organizations. [1, 2, 3, 9, 10]

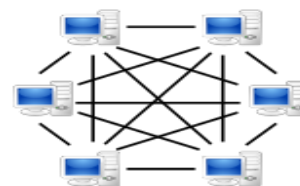


Figure1: Peer-to-Peer overlay Architecture.

1.1 Super nodes in a Peer-to-Peer Overlay Network

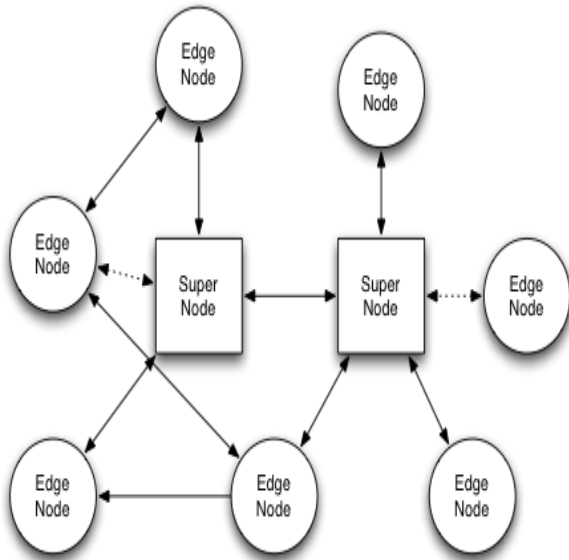


Figure2: Peer-to-Peer Supernode Architecture.

A super node is a well-known P2P node that has some guarantee of high availability, computing resources and available networking bandwidth. Accordingly, they can provide more resources for other peers and they are usually more stable than regular peers. A regular peer may also become a super node, if the requirements are fulfilled. Thereby, it does not necessarily need to have a static public IP address or DNS name for super node, if it is otherwise well-known and has sufficient bandwidth capacity. However, these are useful capacities especially if an operator provides super node functionalities for a network. The use of super nodes implies a hierarchical structure instead of a flat structure. However, a flat structure can also have super nodes, if the regular peers do not participate in the overlay signaling. Instead, the super nodes act on behalf of these regular peers in the P2P overlay. In this case, only the super nodes run the P2P algorithm. [4, 5, 11]

2. TRUST AND REPUTATION MANAGEMENT

Trust and reputation management has recently become a very useful and powerful tool in some specific environments where a lack of previous knowledge about the system can lead participants to undesired situations, specifically in virtual communities where users do not know each other at all or, at least, do not know everyone. It is in those cases where the application of trust and reputation mechanisms is more effective, helping a peer to find out which is the most trustworthy or reputable participant to have an interaction with, preventing thus the selection of a fraudulent or malicious one.[12]

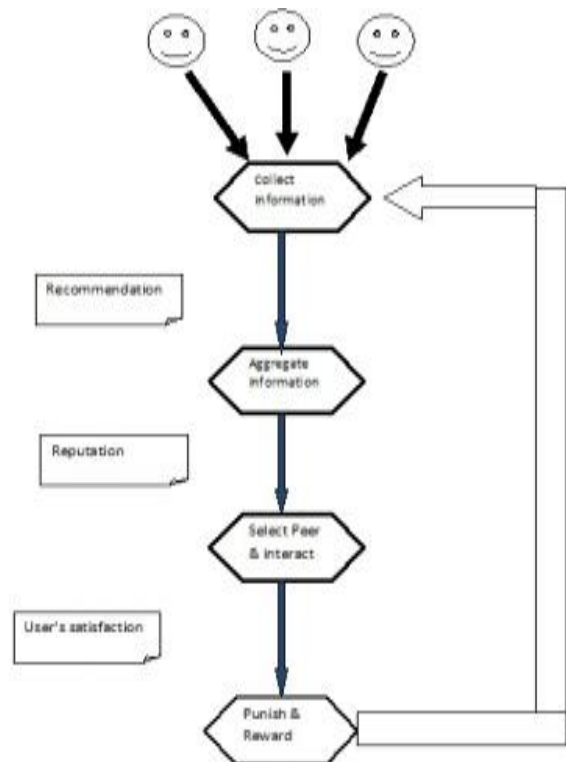


Figure3. Trust and Reputation Model steps

It has noticed that most of the current trust and reputation models follow these four general steps

- *Collecting information* about a certain participant in the community by asking other users their opinions or recommendations about that peer.
- *Aggregating* all the received information properly and somehow computing a score for every peer in the network.
- *Selecting* the most trustworthy or reputable entity in the community providing a certain service and effectively having an interaction with it, assessing a posteriori the satisfaction of the user with the received service.
- According to the *satisfaction* obtained, a last step of punishing or rewarding is carried out, adjusting consequently the global trust deposited in the selected service provider.[6,7,8]

This is an issue that should not be underestimated when designing and developing a new trust and reputation model over distributed and heterogeneous systems, since an inaccurate management of these threats could result in important security deficiencies and weaknesses. Reputation Systems Reputation systems are the most well known solution to build trust in P2P networks, through a social control using feedbacks from the community. Recommendations on the past experiences of peers help to make decisions about quality and reliability of transactions. After each transaction between two peers, the evaluator peer

gives a recommendation about the behavior of the evaluated peer during the transaction. Several solutions of reputations systems already exist for decentralized systems as, some of them are for structured and others for unstructured P2P networks.[13]

3. PROBLEM DOMAIN

In recent years, Peer-to-Peer (P2P) networks have soared in popularity in the form of file sharing applications. Large amounts of data and resources are being shared co-operatively among P2P users on a global-scale that is a good sign but with this popularity comes security implications and vulnerabilities. Some basic problems in peer-to-peer network are:

- P2P file sharing systems suffers from free-riders, who use others, resources without sharing their own cause system-wide performance degradation.
- File “poisoning” by injecting a massive number of distractions into the peer-to-peer network, to reduce the availability of the targeted item.
- A number of Users do not want to share files, data, or resources rather desire to free ride on others.
- A worst condition for open networks is when a group of malicious peers make collusive attempts to manipulate the ratings.
- Some participants consume more resources than they contribute.
- File pollution is also a main problem in P2P network that is, the accidental injection of unusable copies of files in the network, also decreases content availability.
- Networks are not completely secure.
- Some malicious behavior can't be punished due to open nature of P2P networks.
- A worst condition for open networks is when a group of malicious peers make collusive attempts to manipulate the ratings.
- Reputation building based feedback is difficult, due to dynamic changes in open networks.
- A malicious request responder, if selected as a service provider can attack on the system.
- Malicious raters, easily attack Reputation models based on subjective user rates.

4. ALGORITHM: BALANCED REPUTATION DETECTIVE SYSTEM (BREDS)

This paper proposes a Balanced Reputation Detective System including two transaction protocols for peer-to-peer file-sharing networks. In proposed system, it divides the whole P2P network into many groups with more than one group managers to decrease the traffic load of query messages. The proposed system offers the following properties. (1) Peers are classified into different reputation

levels according to the peer’s past transaction records and contributions. (2) Every peer could assign his own files to several authorized levels by himself according to his freedom. Thus, other requesting peers cannot download the files if their reputation levels are less than the authorized levels of files. (3) If a peer shares no files with other peers, his reputation would be degraded as time goes by. (4) If peers are not enthusiastic to share files to increase their reputation levels, they will not download the files because their reputation level is less than the authorized level of files. By the properties above, peers have incentive to share files with other peers in order to get good service from other peers.

4.1 System Structure

Figure 4 shows the structure of system having various groups and each group have more than one group manager to avoid any unwanted condition of group manager. Each group has many peer nodes connected to group manager for efficient use of network services.

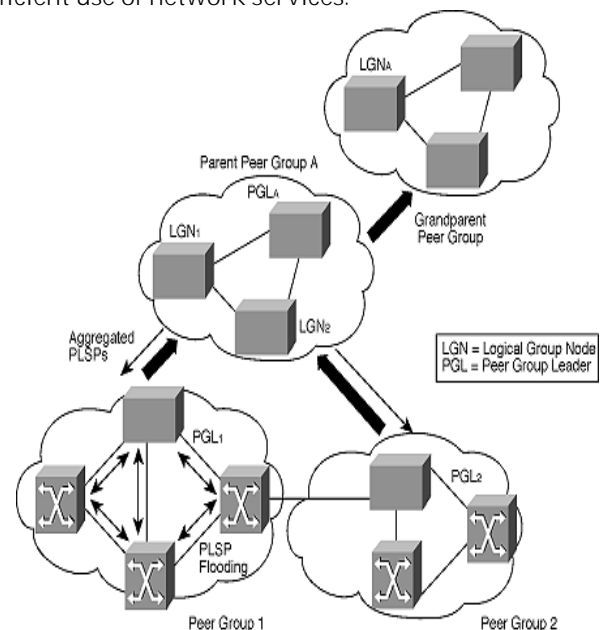


Figure 4: System Model for BREDS

5. SIMULATION ENVIRONMENT

In this section simulation environment used for model implementation is described. Network simulator version 2 is used, for the simulation purpose with ns2 version ns-2.29 was used with different network scenario. In the following section the details regarding to the NS2 simulator and their usage is given.

6. RESULTS

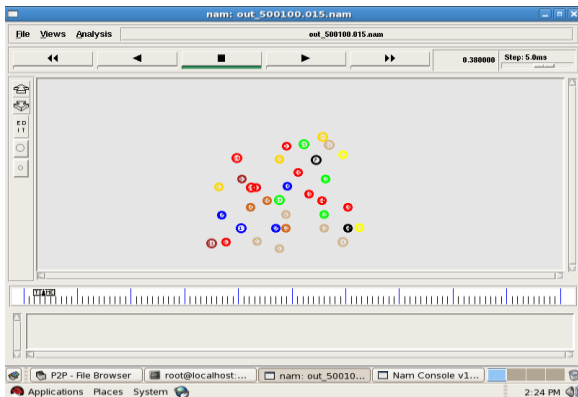


Figure 5: Simulation of BReDS

As per figure 6.1 shows the simulation of our model consists of 35 nodes.

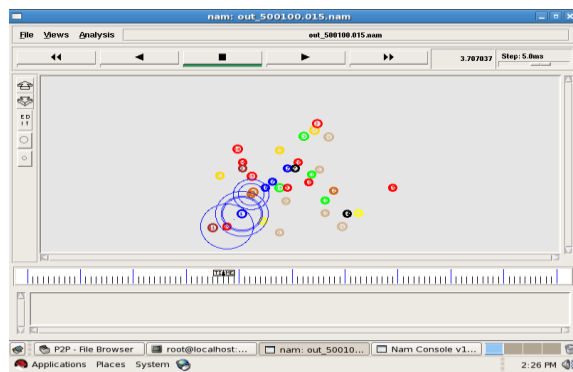


Figure 6: Delivery of Service Behaviors of BReDS

From the figure 6 it is analyzed that as soon as full network is established number of groups' increases to balance load between the groups. In this way maximum services are provides to the network. Surely it will be a flexible and robust model for Peer-to-Peer network.

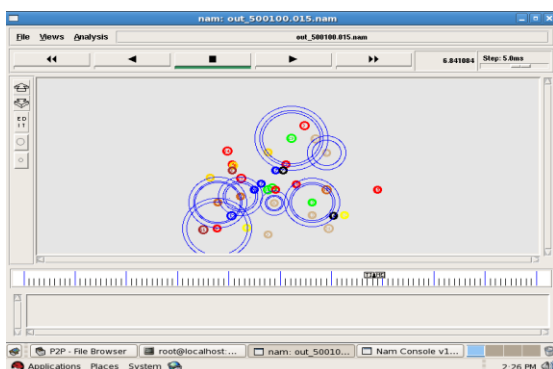


Figure7 : Packet drops

Figure 7 shows that groups are communicated for the services. It is not always possible that services are available in to a peer node in the same group so group manager extends the search to another group. So groups need to be

communicating other groups for better services. If any malicious node is detected then services are not proved to that node. In simulation packet drops represent that malicious node is eliminated from the network by not giving any service to that node based on their reputation in the network.

7. CONCLUSION

To probe further, it is suggested to keep two kinds of reputation scores on each peer node: one to measure the *quality-of-service* (QoS) and another for *quality-of-feedback* (QoF) by participating peers. Integrating these two scores together and address the tradeoffs between them in future research challenges. Further research is also encouraged to apply reputation systems to enforce copyright protection in P2P systems. With the help of object reputation, a client can validate the authenticity of an object before initiating parallel file download from multiple peers. This opens up a meaningful direction to extend BReDS systems for managing object reputations.

REFERENCES

- [1] E. Adar and B. Huberman. Free riding on Gnutella, Technical report, Xerox PARC, 10 Aug. 2010.FirstMonday.
- [2] Hughes, D., Coulson, G., and Walkerdine, J. (2011). Freeriding on gnutella revisited: The bell tolls? In Submitted to IEEE Distributed Systems Online.
- [3] Utah Division of Consumer Protection, Pyramid Schemes, available at: <http://www.commerce.utah.gov/dcp/education/pyramid.html>
- [4] Jia Zhao and Jian-De Lu, A Self-Organized and Searching-Improved Community Management Framework for Decentralized Unstructured Peer-to-Peer Networks, Technical Report TR-SCU-05001, Soochow University. Available at: <http://csts.suda.edu.cn/TR/TR-SCU-05001.pdf>
- [5] Philipp Obreiter and Jens Nimis, A Taxonomy of Incentive Patterns The Design Space of Incentives for Cooperation, Proceedings of the Second Intl. Workshop on Agents and P2P Computing (AP2PCy 13), Springer LNCS 2872, Melbourne, Australia (2013)
- [6] Michal Feldman, Christos Papadimitriou, John Chuang and Ion Stoica, Free-Riding and Whitewashing in Peer-to-Peer System, SIGCOMM'10 Workshop, Portland, Oregon, USA, 2010

- [7] Michal Feldman, Kevin Lai, Ion Stoica, John Chuang, Robust Incentive Techniques for Peer-to-Peer Networks, Proceedings of the 5th ACM conference on Electronic commerce (May 2012)
- [8] Cuihong Li a, Bin Yu b, Katia Sycara "An incentive mechanism for message relaying in unstructured peer-to-peer systems" Electronic Commerce Research and Applications 8 (2009) ScienceDirect, pp.315–326
- [9] Haribabu, K. Reddy, D. Hota, C. Ylä-Jaaski, A. Tarkoma, S. "Adaptive lookup for unstructured peer-to-peer overlays" 978-1-4244-1796-4 IEEE 2008, pp. 776 - 782
- [10] K. Haribabu, ChittaranjanHota, AnttiYlä-Jääski "Indexing through Querying in Unstructured Peer-to-Peer Overlay Networks" 978-3-540-88622-8 ACM 2008