Volume 2, No. 8, September 2011
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

REPUTATION SYSTEM IN PEER-TO-PEER NETWORK: DESIGN AND CLASSIFICATION

Sandeep Kumar[1], Chander Diwaker[2], Amit Chaudhary[3]
[1, 2, 3] CSE Department, UIET, Kurukshetra University, Kurukshetra, INDIA
[1]sandeep167@gmail.com, [2]chander_cd@rediffmail.com, [3]amitch115@gmail.com

Abstract: Peer-to-Peer (P2P) applications have recently seen an enormous success and have reached millions of users. The main reason of this success is the anonymity the users enjoy. However, as recent experiences with P2P networks show, this anonymity offers an opportunity to exploit the network like free-rider, virus spread, malicious file spread etc. The problem of securing hosts on P2P network while keeping the openness of the system has been studied extensively over last couple of years but still there are various issues on it. Reputation and incentive are two traditional systems to deal various problems in the Peer-to-Peer network. In this paper we define reputation system and give reputation system's design consideration and classification used to create an efficient reputation system that can handle various P2P security issues like free-rider problem, DDoS attack.

Keywords: P2P; Reputation system; Trust; free-rider; selfish peer

INTRODUCTION

Peer-to-peer networks are networks in which peers cooperate to perform a critical work in a decentralized manner. All peers are both client and server of resources and can contact each other directly without intermediary peers. Compared with a centralized system, a peer-to-peer (P2P) system provides an easy way to aggregate large amounts of resources residing on the edge of Internet or in ad-hoc networks with a low cost of system maintenance. However, the difficulty in establishing direct relationships might reduce the participation of the nodes and the quality of the communication in systems formed by stranger nodes. The system might not function properly if non-cooperative (rational) behavior will be privileged and predominant in the network. This occurs because individual rational nodes are wants to maximize their own use of the resource while the costs of the service are shared between all those to whom the service is available. Selfish nodes do not share their services if they cannot increase their utility; these nodes are called free riders [1] [2].

Since there is no centralized node to provide as an authority to monitor and punish the peers that behave badly, malicious peers have an encouragement to provide poor quality services for their benefit because they can get away. Some traditional security techniques, such as service providers requiring access authorization, or consumers requiring server authentication, are used as protection from known malicious peers. However, they cannot prevent from peers providing variable-quality service, or peers that are unknown. One possible solution is to introduce a reputation scheme to the system. The interactions between peers affect their reputation in such a way that free-riders are not able or difficult to build up a high reputation. When a peer has a resource to spread, and there are several peers requesting this resource, the peers with higher reputation are given priority over peers having lower reputation value [3].

This use of reputation differs from the classic use of reputation to increase the quality of transactions in peer-to-peer systems such as eBay, or to marginalize untrustworthy peers as in the systems. If reputation is used to discourage free-riding then the choice to interact with a peer with high reputation is made in order to reward the peer for its previous behavior, rather than to enhance the expected quality of the immediate transaction. Mechanisms for trust and reputation can be used to help peers distinguish good from bad partners. This paper describes reliance and reputation mechanism that allows peers to discover partners who meet their individual requirements through individual experience and sharing experiences with other peers with similar preferences[4][5].

TRUST AND REPUTATION MANAGEMENT

First we categorize the peers in P2P into four classes: Honest Peer, Selfish Peer, Malicious Peer, and Evil Peer [6].
Honest Peer: These type Peers initiate's only good transactions. His ratings are always correct, good transactions are rated good, and bad transactions are rated bad by them.

Selfish Peer:

These type Peers is a so called free-rider. He blocks all inquiries by other agents and refuses to rate his transaction partners. He just initiates neutral to good transactions by himself.

Malicious Peer:

These type Peers initiates good, neutral and bad transactions by chance. He tries to damage the system with his rating behavior and rates every transaction negative.

Evil Peer:

These type Peers try to gather a high reputation by building a group in which they know each other. If an evil agent finds another evil agent to trade with, they always give each other a good rating. If an evil agent does not find another evil agent, after seeking for a while, he transacts neutral and rates neutral. 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. 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[7][8]. In this paper, we adopt the following definitions:

Trust:

A peer's belief in another peer's capabilities, honesty and reliability based on its own direct experiences

Reputation:

A peer's belief in another peer's capabilities, honesty and reliability based on recommendations received from other peers. Reputation can be centralized, computed by a trusted third party, like a Better Business Bureau; or it can be decentralized, computed independently by each peer after asking other peers for recommendations [7].

Trust and reputation models follow these four general steps:

1. Collecting information about a certain participant in the community by asking other users their opinions or recommendations about that peer.
2. Aggregating all the received information properly and somehow computing a score for every peer in the network.
3. Selecting the most reliable 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.
4. According to the satisfaction obtained, a last step of punishing or rewarding is carried out, adjusting consequently the global trust (or reputation) deposited in the selected service provider.

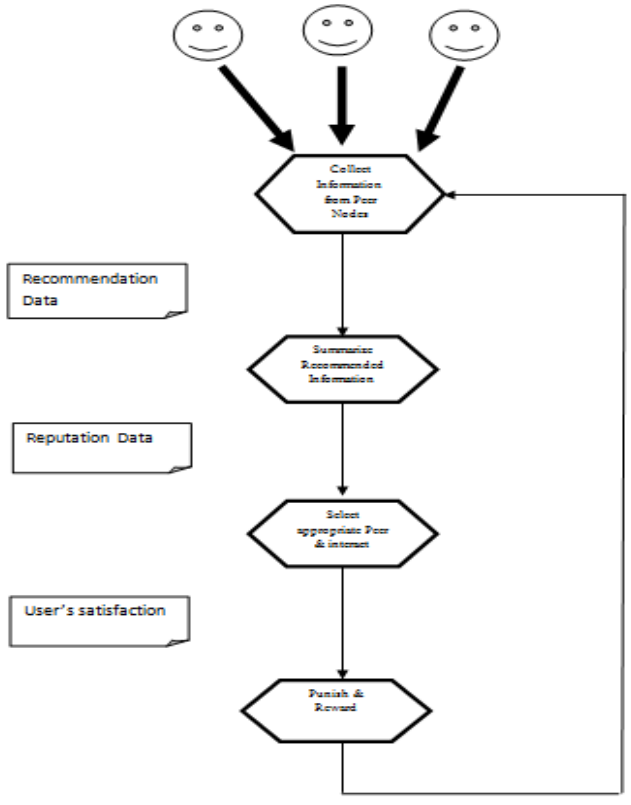

Figure 1: Steps in Trust and reputation model

DESIGN CONSIDERATIONS

There are five issues that are important to address in any P2P reputation system [9][10].

1. The system should be self-policing. That is, the shared ethics of the user population are defined and enforced by the peers themselves and not by some central authority.
2. The system should maintain anonymity. That is, a peer's reputation should be associated with an opaque identifier (such as the peer's Gnutella username) rather than with an externally associated identity (such as a peer's IP address).
3. The system should not assign any profit to newcomers. That is, reputation should be obtained by consistent good behavior through several transactions, and it should not be advantageous for malevolent peers with poor reputations to continuously change their opaque identifiers to obtain newcomers status.
4. The system should have negligible overhead in terms of computation, infrastructure, storage, and message complexity.
5. The system should be robust to malicious collectives of peers who know one another and attempt to collectively subvert the system.

CLASSIFICATION OF REPUTATION

Based on whether the reputation is obtained directly or indirectly we identify two types of reputation along this dimension

- Direct Reputation
- Indirect Reputation

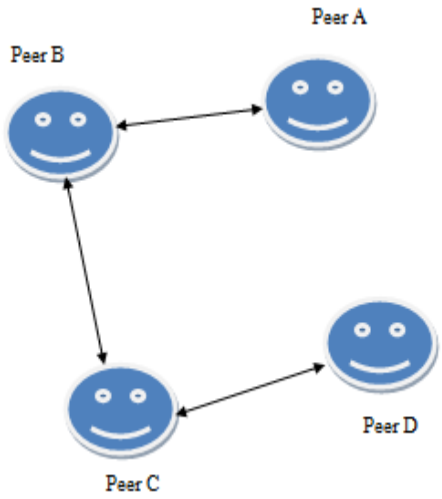

Figure 2: trust relationship between peers

We define a *direct reputation* as if a witness peer is queried directly by the reputation querying peer, then we call this reputation as direct reputation. Since Peer C had previously interacted with Peer D(let us assume that the interaction between Peer C and Peer D was in the same context as the one Peer B is querying for)it advises Peer A about its perceived trustworthiness of Peer D. We term this reputation that is passed by Peer C (witness peer) as Direct Reputation [11].

We define an *Indirect Reputation* as if a witness peer is queried by the intermediate peer/s, and not by the reputation

querying peer directly, then we call this reputation as indirect reputation. Peer A since it does not know the trustworthiness of Peer D, (since they have not interacted previously), it may pass on this query to other peers, whom it feels may know about Peer D's trustworthiness. Peer B becomes an intermediate peer. Let us assume that Peer B passes the reputation query of Peer D reputation to Peer C. Peer C since it knows the trustworthiness of Peer D, passes the information to Peer B, who in turn passes it back to Peer A. We term this reputation obtained from Peer B about Peer D, which was convey to Peer B by Peer C as Indirect Reputation.

Classification of reputation as a degree of trust as advised by the witness peer. The witness peer may advise that the reputation queried peer may be trusted, may not be trusted for that given context. We identify three main types of reputation along this case [12]

- Positive Reputation
- Negative Reputation
- Neutral Reputation

We define positive reputation as "Reputation of the reputation queried peer obtained from a witness peer that advises that the reputation queried peer be trusted"

We define negative reputation as "Reputation of the reputation queried peer obtained from a witness peer that advises that the reputation queried peer not to be trust"

We define neutral reputation as "Reputation of the reputation queried peer obtained from a witness peer that is unsure about the trustworthiness of the reputation queried peer".

CONCLUSION

Enabling peers to develop trust and reputation among themselves is important in a peer-to-peer system where resources (either computational, or files) of different quality are offered. It will become increasingly important in systems for peer-to-peer computation, where trust and reputation mechanisms can provide a way for protection of unreliable, buggy, infected or malicious peers. in this paper we present how trust and reputation managed in the network and give design consideration used for designing the reputation system and give classification of reputation that are calculated in the network in various ways ie. reputation may be positive or Negative from direct or indirect peer nodes.

REFERENCES

[1]. Tseng, T.-Y. Lee, R. Lin, S.-W. Han, T.Huafan Univ., Shihding "Mixed Client Server and Peer to Peer System for Internet Content Providers" 1-4244-0099-6 IEEE 2006

[2]. D. Liben-Nowell, H. Balakrishnan, and D. Karger, "Analysis of the evolution of peer-to-peer systems" in Proceedings of the Annual ACM Symposium on Principles of Distributed Computing, Monterey, California, USA, 2002.

[3]. Riidiger Schollmeier, Institute of Communication Networks, Technische Universitat "A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications" 0-7695-1503-7102 IEEE 2002 , pp.101-102

[4]. M. Ham and G. Agha, "ARA: a robust audit to prevent free-riding in P2P networks," in Peer-to-Peer Computing, 2005. P2P 2005. Fifth IEEE International Conference on, pp. 125–132, 31 Aug.-2 Sept. 2005.

[5]. D. J. Zage and C. Nita-Rotaru, "On the accuracy of decentralized network coordinates in adversarial networks," in CCS '07: Proceedings of the 14th ACM Conference on Computer and Communications Security, (New York, NY, USA), ACM Press, October 2007.

[6]. S. Marti and H. Garcia-Molina "Taxonomy of trust: Categorizing P2P reputation systems" Computer Networks, vol. 50, Mar. 2006, pp. 472-484.

[7]. Felix Gomez Marmol, Gregorio Martınez Perez "Security threats scenarios in trust and reputation models for distributed systems" available at www.sciencedirect.com, computers & s e c u rity 2 8, 2 0 0 9 , pp. 5 4 5 – 5 5 6

[8]. Sepandar D. Kamvar, Mario T. Schlosser, Hector GarciaMolina "The EigenTrust Algorithm for Reputation Management in P2P Networks" Budapest, Hungary.ACM, 2005

[9]. Shalendra Chhabra, Ernesto Damiani, Sabrina De Capitani di Vimercati "A Protocol for Reputation Management in Super-Peer Networks" Proceedings of the 15th International Workshop on Database and Expert Systems Applications (DEXA'04)1529-4188/04 IEEE, 2004

[10]. P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, "Reputation systems," Communications of the ACM, vol. 43, no. 12, pp. 45–48, 2000.

[11]. L. Xiong and L. Liu, "A reputation-based trust model for peer-to-peer ecommerce communities," in IEEE Conference on Electronic Commerce, June 2003.

[12]. K. Lin, H. Lu, T. Yu, and C. Tai, "A reputation and trust management broker framework for web applications," in Proceedings of the 2005IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE'05), pp. 262–269, IEEE Computer Society Washington, DC, USA, 200**5.**

