RESEARCH ARTICLE OPEN ACCESS

Distributed Trust Management Model for Peer To Peer Systems

M. Anitha [1], R. Hemalatha [2]

M.Phil Scholar [1], HOD and Assistant Professor [2]
Department of Computer Science
Tiruppur Kumaran College for Women
Bharathiyar University
Tamil Nadu –India

ABSTRACT

In a file sharing peer-to peer system trust is essential to attain enhanced cooperation between peers. Reputation is utilized in reputation-based peer-to-peer systems to form trust between peers. Commonly in these systems, extremely reputable peers will be chosen to upload requested files and thus diminishing malicious uploads in the system considerably. Conversely, malicious peers should be encouraged to fund confidently by uploading authentic files rather than malicious ones. In this work, distributed algorithms is presented, which allow a peer to reason nearly trust worthiness of other peers depends on past interactions and recommendations using distributed trust management model. In this, peers build their own trust network in their vicinity with the use of local information available trust-reputation, trust-service, and recommendation metrics which are well-defined to measure trustworthiness in providing services and providing recommendations with the use of a trust management system. In addition to that, Credibility Behaviour is presented as the second dimension of the trust management framework. The Malicious Detector Algorithm (MDA) is utilized to discover liar peers. The new concept of suspicious transactions is presented to identify these liar peers. Performance evaluations show that the proposed scheme is able to detect and isolate malicious peers from the system, henceforth, giving higher peer satisfaction, improved network resource utilization and increasing peers' satisfaction.

Keywords:- Reputation System, Peer-To-Peer Networking, Distributed Trust Management, Malicious Detector Algorithm, Credibility Behaviour

I. INTRODUCTION

Earlier several reputation management systems have been proposed [1], [2], [3], [4], [5] and all of these have concentrated on the completely-decentralized P2P systems. There is no reputation management system has been projected for partially-decentralized P2P systems. MerelyKaZaA which is a proprietary partially-decentralized P2P system, has familiarized basic reputation metric which is called as "participation level" for rating peers. But the proposed reputation management schemes cannot be applied for completely decentralized P2P systems in the case of a partially-decentralized systems. The partially-decentralized P2P systems (e.g. KaZaA [6], Morpheus [7] and Gnutella2 [8]), have been projected to diminish the control overhead needed to run the P2P system. In these systems, several of the peers such as "super nodes" or "ultra peers", index the files shared by peers connected to them and proxy search demands in aid of these peers [9]. Therefore queries are directed to super nodes and not to other peers. Normally super node supports 300 to 500 peers based on available resources [8].

In [10], projected a reputation management system for partially-decentralized P2P systems and this reputation mechanism permits an additional clear-sighted management of peers and files. Through several transactions, good reputation is attained by having consistent good behaviour. The reputation standard is accustomed make a distinction between peers. The main aim is to exploit the user satisfaction and reduction the sharing of corrupted files. In the following, Real Behaviour Based Algorithm referred to the in [10] as the Inauthentic Detector Algorithm (IDA). This procedure detects malicious peers from whom inauthentic files received and separates them from the system. Ultimately the previously proposed feedback-based reputation management schemes for P2P systems, put emphasis on identifying and exhausting peers who are sending inauthentic files. Not at all special mechanism was projected to identify and punish peers that send wrong feedbacks. The peers can lie in their feedbacks definitely.

Even though some proposed feedback-based reputation schemes take this behaviour into concern, these schemes only rely on peers' reputation for their peer-selection progression. Such liar peers can challenge the reputation system through disturbing seriously the reputation of other peers that is whether it rises the reputation of malicious peers, or drop the reputation of good peers.

If they are not sending inauthentic files these malicious peers may not be detected and thus reputation of these methods can be extraordinary with effective trust model. It is utmost importance to sense liar peers and avoid them from disturbing the system. In this work, a new scheme called the Malicious Detector Algorithm (MDA) is proposed that as well as detecting and punishing inauthentic peers which is based on IDA, perceives liar peers and castigates them. Finally, the proposed scheme decreases significantly the amount of malicious uploads and protects the strength of the system.

The paper is organized as follows. In Section 2presents the related works. Section 3, presents an analysis of peers' behaviour with the reputation management scheme and the proposed approaches to detect malicious peers, while Section 4 presents the performance evaluation of the proposed scheme. Conclusion and future work is drawn in section 5.

II. RELATED WORK

Mekouar et al. planned a Malicious Detector algorithm in [11] to observe cheater peers that send wrong feedback to subvert reputation system. That is, when every group action between a combine of peers, each peers are needed to come up with feedback to explain the group action. If there is an apparent gap between the two items of feedback, each are regarded being suspicious. Ji et al. raised a group primarily based metric for safeguarding P2P network against Sybil attack and collusion by dividing the complete network into some trust teams supported international structure data that is tough to get [12]. In [13], Lian et al. suggested numerous collusion detection approaches as well as pair-wise detector and traffic concentration detector with information of Maze file sharing application supported trace analysis. So as to ensure the correctness of the name calculation, Despotic et al [14] compared the probabilistic estimation and social network strategies.

Besides, they additionally known four categories of collusive behaviour. Recently, Tehale et al used the false message idea for distinguishing and confirming the Sybil nodes within the network [15]. Selvaraj et al given a comprehensive survey of security problems in name Management Systems for P2P networks in [16]. Jin et al planned a peer primarily based monitoring technique in Peer-to-Peer streaming setting [17]. Koutrouli et al provided an intensive view of the assorted quality threats against a suburbanized name system and also the individual defense mechanisms [18]. Recently, an upload entropy theme is developed by Liu et al. to stop collusions and any enhance strength of personal trackers' sites [19]. However the threshold of this theme has to be settled manually.

Moreover, Lee et al. imply a simplified ingroupobserveion technique to detect the colluders [20], however their technique is restricted to colluders who form a circle. Ciccarelli et al [21] surveyed the literature on P2P systems security with specific attention to collusion, to seek out out however they resist to such attacks and what solutions may be used. On the one hand, they summarized five collusive categories, then investigated the influence of collusion on numerous applications. On the opposite hand, they mentioned the possible solutions that may be utilised to resist collusions, like theory of games then on. Liu et al [22] brought forward a replacement strategy supported trust worth and considers each the standard and also the variety of shared resources to avoid the development of free riding. Moreover, they additionally sketched collusion, slander and different misdeed throughout strategy style.

A MSPCA and Quality of Reconstruction primarily based technique Peer Mate was planned in our former work [23], it will with efficiency observe malicious peers for P2P systems. However, Peer Mate cannot decide malicious peers that initial Sybil attack to the system. Moreover, PeerMate wants a reconstruction threshold, which might remarkably impact its potency. Besides, several micropayment systems primarily based ways are planned to assist the P2P systems resist conniving behaviour, during this work, however, we have a tendency to primarily concentrate on the way to observe malicious peers below P2P systems with reputation management schemes.

III. PROPOSED DISTRIBUTED TRUST MANAGEMENT MODEL FOR PEER TO PEER SYSTEMS

a. Understanding Peer Behavior on lies

In a P2P system, smart peers are those who send authentic files and do not belong their feedbacks (Type T1 in Table-1). Malicious peers are often divided into three categories: 1) peers that send inauthentic files and do not exist their feedbacks (Type T2), 2) peers that which send authentic files and belong their feedbacks (Type T3), and 3) peers that send inauthentic files and belong their feedbacks (Type T4). A cheater peer is one that once receiving an authentic file, rather than giving an appreciation adequate one, the peer sends an appreciation adequate −1 to decrease the name of the peer uploading the file. Otherwise, it sends a positive appreciation to extend the name of alternative malicious peersif the peer receives an inauthentic file. Note that we tend to take into account the consistent behavior of peers. This implies that almost all of the time a peer behavior is in line with the class it belongs to (i.e., T1, T2, T3, or T4). For instance, a better peer will typically send inauthentic files by mistake. Note conjointly that peers will modify their behavior over time and thence will jump from one class to a different.

Table 1. Peer Behavior

Type	Peer	Authentic Behavior	Credibility Behavior
T1	Good	High	High
T2	Malicious: Inauthentic	Low	High
T3	Malicious: Liar	High	Low
T4	Malicious: Inauthentic & Liar	Low	Low

b. Effect on Reputation

As all know, peers could contains positive or negative reputations. Commonly the good peer has a positive reputation because the user behaving in a good manner. However, malicious peers can lie and thus the user's reputation will be decreased and even get negative in this situation. Reversely, if the user sending inauthentic files then the malicious peers will have negative reputation values. But, is some other malicious peers sending positive reputation then their reputation values can increase and even get positive where they even can receive inauthentic files as well. If it is happens where lair are not determined nor punished in the system.

c. Detecting Malicious Peers

Let's assume from peer P_j (Notations are given in Table 2)the peer P_i downloads file F. Since it is sending the file, it efforts on the Authentic Behavior (sending authentic or inauthentic files) of peer P_j, and the Credibility Behavior who are lying or not in the feedback of peer $P_i$from the time when it is sending the appreciation that will disturb the reputation of peer P_j. If the appropriate actions need to be taken after this transaction, then have to detect if peer P_j belongs to any of the categories T2 and T4, and if peer P_i belongs to any of the categories T3 and T4. Peer P_i requests a search service $ReqF_i$from its supernode $Sup(i)$. PeerP_i will choose peer P_j according to the Authentic Behavior of P_j when peer P_i obtains the result of the search request $ReqF_i$,. Peer P_i sends a request $ReqF_{ij}$ to download file F from peer P_j andsubsequently downloading this file, peer P_i sends feedback $A_{i,j}^F$. On the Authentic Behavior of peer P_j, the Credibility Behavior of peer P_i will have a important effect. Inauthentic Detector Algorithm (IDA)permits to discover peers sending inauthentic files. The main aimis to detect peers now and that direct wrong feedbacks and reduce their effect on the reputation based system.

Table 2: Notations and its Description

Notation	Description
P_i	peer i
$D_{i,j}$	The units of downloads performed by peer P_i from peerP_j
$D_{i,*}$	The units of downloads performed by peer P_i
$D_{*,j}$	The units of uploads by peer P_j
$A_{i,j}^F$	The appreciation of peer P_i after downloading the file F from peer P_j
$Sup(i)$	The super node of peer i

d. Reputation-based Approach

The reputation based approach is utilized to say that malicious peers have a low reputation than good peers. The idea to diminish the impact of peers which having a low reputation is taken into account when updating the reputation of other peers in the reputation based system.

If $A_{i,j}^F = 1$

then

$$D_{*,j}^{+} = D_{*,j}^{+} + \frac{(1 + AB_i)}{2} Size(F)$$

else

$$D^{-}_{*j} = D^{-}_{*j} + \frac{(1 + AB_i)}{2} Size(F)$$

In this approach, the impact of peer P_i on the Authentic Behavior of peer P_j is associated to the Authentic Behavior of peer P_i (i.e., AB_i). In case peer $P_i$has a good reputation (commonly above zero), it is reliable more and it will impact the reputation of peer P_j, on the other hand, In case its reputation is low, as a result decreasing the impact on the reputation of peer $P_j$merely a small fraction of the file size is considered. His reputation is null when peer P_i is new and since it is not known yet if it is a good or a malicious peer, merely half of the size of the uploaded file F is disturbing the reputation of the peer uploading the file that is peer P_j. The problem with this approach seems in the following example. Let assume that some peers be appropriate to category T3 and those peers continuously send authentic files, however send wrong appreciations besides. Those peers will have a high reputation most of the time along with above logic, subsequently they continuously send authentic files and henceforth will receive good feedbacks. The system be trusted those peers and will disturb seriously the reputations of other peers and may ultimately threaten the system.

e. Malicious Detector Algorithm (MDA)

Malicious Detector Algorithm is better approach utilized to identify peers that lie in their feedbacks is to detect suspicious transactions. A suspicious transaction is defined as one in which the appreciation is changed from the one predictable knowing the reputation of the sender. Otherwise, if $A^F_{i,j} = 1$ and $AB_j < 0$ or if $A^F_{i,j} = -1$ and $AB_j > 0$ then this transaction consideredas suspicious. Thesupernode $Sup(i)$ keeps track of the following values for each peer $P_i$toidentify peers that lie in their feedbacks:

- N_i : The total number of downloads accomplished by peer P_i
- N_{*i}: The number of downloads by peer P_i where the sign of the appreciation sent by peer P_i is different from the sign of the sender's reputation, i.e., AFi,j × ABj < 0 (i.e., through a suspicious transaction)
- T_{F_i}: The total size of all the files uploaded by P_i.

where$N_{*i} \leq N_i \forall i$, when receiving the appreciation (i.e., $A^F_{i,j}$) of peer P_i, its supernode $Sup(i)$ will modernize the values of N_i and N_{*i}as follows:

$N_i = N_i + 1$

$if\left(A^F_{i,j} \times AB_j\right) < 0$ then$N_{*i} = N_{*i} + 1$

Let $\alpha_i$be the ratio of $N_{*i}$and N_i:

$$\alpha_i = \frac{N_{*i}}{N_i}$$

where$0 \leq \alpha_i \leq 1 \ \forall i$, $\alpha_i$is denoted as the ratio of the number of suspicious feedbacks sent by peer P_i over the total number of feedbacks sent by peer P_i. $\alpha_i$is a good indicator of the liar behavior of peer P_i . Certainly, if peer P_i lies in its feedbacks, the number of times $A^F_{i,j}$ and the sender's reputation having different signs, and therefore the value of $N_{*i}$is high. Liar peers will incline to have values of α_i near whereasgood peers will tend to have values of $\alpha_i$near zero. The following update strategy is utilized for the sender's appreciationto diminish the effect of liar peers. The sender's supernode $Sup(j)$ performs the following algorithm subsequently getting the appreciation $A^F_{i,j}$,.

If $A^F_{i,j} = 1$

then

$D^{+}_{*j} = D^{+}_{*j} + (1 - \alpha_i)\ Size(F)$

else

$D^{-}_{*j} = D^{-}_{*j} + (1 - \alpha_i)\ Size(F)$

end if

$TF_j = TF_j + Size(F)$

From the time when liar peers (in categories T3 and T4) will have a high value of α_i and their consequence on the reputation of the peer sending the file is diminished. Then again, good peers will have a lower value of α_i and later will keep having an impact on the reputation of other peers.In this approach, the Authentic Behavior is calculated in this manner:

$$AB_j = \frac{D^{+}_{*j} - D^{-}_{*j}}{T_{F_j}} \quad if\ T_{F_j} \neq 0$$

$AB_j = 0\ otherwise$

WhereAB_j is updated after each upload of peer P_j and α_i is updated after each download of peer P_i . It denotes that liar peers will be identified even if they did not upload any file and though they did not perform any download inauthentic peers will be identified. If peer P_i changes its behavior, α_i will also change, and therefore its impact on the reputation of other peers. As, incase peer P_i changes its behavior from category T3 to T1, the number of suspicious

transactions N_{*i} involving this peer which is in comparison to the total number of transactions N_i will be less and in future the value of α_i will decrease, creating the impact of this peer more significant.

In this case, the Credibility Behavior of peer P_i is defined to be: $CB_i = 1 - \alpha_i$ .Here, the reputation of peer P_i is the couple (AB_i, CB_i) which describes the behavior of peer P_i in terms of Authentic Behavior who are sending authentic or inauthentic files and Credibility Behavior who lying or not in the feedback. Where a peer can yet download a file from a peer with low value of CB_iproviding the value of AB_i is high. As a result, the system can still yield benefit of a peer that delivers authentic files but lies in its feedbacks.

In this work, the new idea of contribution behavior that permits to differentiate between peers that contribute completely to the system (i.e. altruistic) and therefore the free riders (i.e. egoistic). In this reputation-based system with many users, the competition to transfer requested files is incredibly high. Since peers with higher name values are continuously chosen, these peers can have higher contribution values and can receive higher services. Peers that are still within the method of building their reputation cannot be elected to accomplish the transfer. These peers can receive lower services and cannot be able to increase their contribution values in this system.

If the Contribution Behavior of a peer is computed based mostly only on it's uploads and downloads, some peers might legally receive lower services. Therefore, need to acknowledge peers that are offered to transfer files and reward them. With the popularity of peers' handiness, peers with a null or a coffee contribution worth can have an opportunity to receive services, and build their name. Gradually these peers can, nonetheless certainly, have their requests handled by the system. These peers are going to be able to transfer files, have additional possibilities to share with others, and increase their name and contribution values step by step. During this work the Contribution Behavior of peers ought to be supported with the two criteria. First is Peers' Availability: being offered for uploading requested files. Second is Peers' Involvement: non-malicious uploads done versus downloads received by a peer. The Contribution Behavior of a peer signifies its contribution in terms of sharing files and completely contributing to the system.

f. Analysis Of Malicious Detection

Let take on(From figure 1) that a peer P_i downloads a file F from a peer P_j . It focus on the Authentic Behavior who sending authentic or inauthentic files of peer $P_j$from the time when he is sending the file and also the Credibility Behavior who dishonest or not in the feedback of peer P_i since he is sending the appreciation that will disturb the reputation of peer P_j. Letimagine that peer P_i and peer P_j are described by the following probabilities:

- P_i: (p_i, q_i)
- P_j: (p_i, q_i)

Where p and q denotes the probabilities of sending inauthentic files and wrong feedbacks correspondingly. Here, $AB_{nj} = \frac{X_{jn} - Y_{jn}}{X_{jn} + Y_{jn}}$, where the values of X_{jn} and Y_{jn} will be modernizedconsistent with the authenticity of the file sentby peer P_j and the credibility of peer P_i.

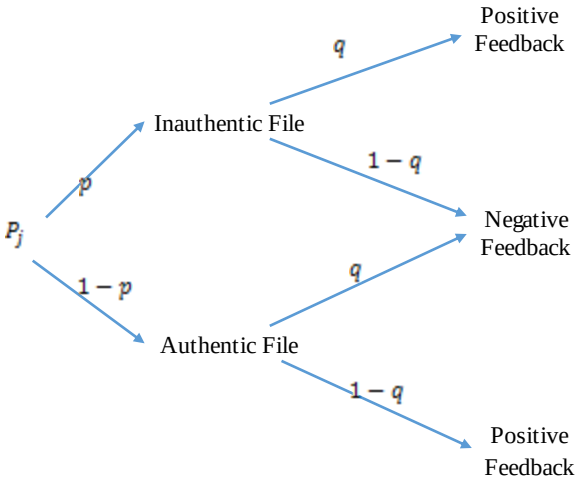

Figure 1.Authentic and Credibility Probabilities

Let's assume a scenario where all peers with the same probability sending wrong feedbacks. Where all peers have the same value of q and hence the following conditions should be noticed.

- Y_{jn} will rise by the size of the uploaded file F_n with probability $Q = (1 - p_j)q + p_j(1 - q)$
- The value of X_{jn} will rise by the size of the uploaded file F_n with probability $(1 - Q)$ $AB_j = 1 - 2Q = 1 - 2[(1 - p_j)q + p_j(1 - q)]$

$$= 1 - 2(q - qp_j + p_j - q)$$
$$= 1 - 2q + 4qp_j - 2p_j$$
$$= 1 - 2p_j - 2q(1 - 2p_j)$$

$= (1 - 2p_j)(1 - 2q)$

This means that the reputation of peer AB_j is based on the probability of sending inauthentic files p_j and the probability of lying in the feedback (i.e., q) of all peers that downloaded a file from peer P_j .If the probability of sending inauthentic files of peer P_j is nearly null and its reputation has to be close to 1. Still, its reputation can become −1 if q is close to 1 because of the lying behavior of peers who downloaded files from peer P_j.

In the subsequent case, deliberate that peers have diverse values of q. Let q_n be the probability of untruthful for the peer P_n who downloaded the file F_n from peer P_j at the nth upload of peer P_j.

Since peer P_j will send an inauthentic file with probability P_j, we obtain the followings:

- The value of Y_{jn} will increase by the size of the uploaded file F_n with probability $(p_j(1 - q_n) + (1 - p_j)q_n)$The value of X_{jn}will increase by the size of the uploaded file F_n with probability $\left((1 - p_j)(1 - q\_n) + p_j q_n\right)$

In this case, the reputation of peer p_j depends also on the probability q_k of all peers P_k that downloaded files from p_j.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

In this section, the system is stimulated under two criterias. One is service differentiation with static peer behavior and another one is service differentiation with rational peer behavior. The system is stimulated with 500 peers and 500 files. Here 500 peers have been chosenfrom the time when a supernode typically supports between 300-500 peers, based on availability of resources.

- Initially, each peer has as a maximum 15 randomly chosen files and each file has at least one owner.
- Every peer willrequest for a file with a Zipf distribution generally the files that the peer does not already have. Where theZipf distribution parameter is selected close to 1.
- Peers are separated into two categories such asContributors and Free Riders. The Free riders constitute 70% of the peers. Meanwhile 30% of peers are malicious peers that send inauthentic content from each category. Peers' behavior and distribution are summarized in table 3
- MinDownload is set to the average file size.
- Here 150, 000 requests are stimulated.

Table 3.Peers' Behavior and Distribution

Category	Percentage	Malicious	Non Malicious
Contributors	30%	0.9%	0.01
Free riders	70%	0.09%	0.01

Consistent with the table 3, peers with index from 1 to 350 be a member of the category of free riders (FR) and peers with index from 351 to 500 be a member of the group of Contributor Peers (CP).To show the effectiveness of the proposed scheme in identifying and handling free riders both good and malicious, a situation is considered where system having a high percentage of free riders.

a. Static Behavior

In this first set of simulations, we consider static peer behavior. This means that peers do not change their behavior over time. We will compare the following schemes:

1. The reputation management scheme with no service differentiation (NOSD). This is utilized to display the significance of service differentiation between the peers.
2. The reputation management scheme with the reputation value as a recommendation for service diversity which is named as Reputation-Based Service Differentiation (RBSD).
3. The reputation management scheme with the Contribution Behavior as a recommendation for service differentiation. This scheme is called as the Contribution-Based Service Differentiation (CBSD).

Free riders share files with a probability of 50. Additionally, 100 of the non-malicious free rider peers can settle for uploading the primary file to induce a high reputation.The following figure 2 depicts the normalized load supported by completely different peers when 150; 000 requests sent to the system within the case of the NOSD scheme. The X axis represents peers' id whereas the Y axis represents the normalized peer load share. From the figure, it's clear that the proposed reputation management scheme which is ready to discover, determine and

isolate malicious peers that is peer id 246 to 395, as they are not requested to transfer files, preventing the peers from receiving malicious content. This is often clearly unfair to the peers that contribute considerably to the system.

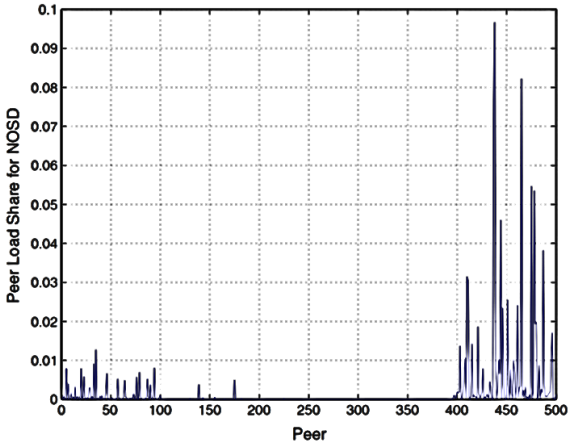

Figure 2. Peer Load Share for NOSD

The figure3 depicts the reputation values of the peers (i.e., the Authentic Behavior) within the case of the reputation based Service Differentiation (RBSD) theme. It is clear that the method is ready to spot malicious peers. However, the method is not ready to differentiate between free riders and contributor peers.

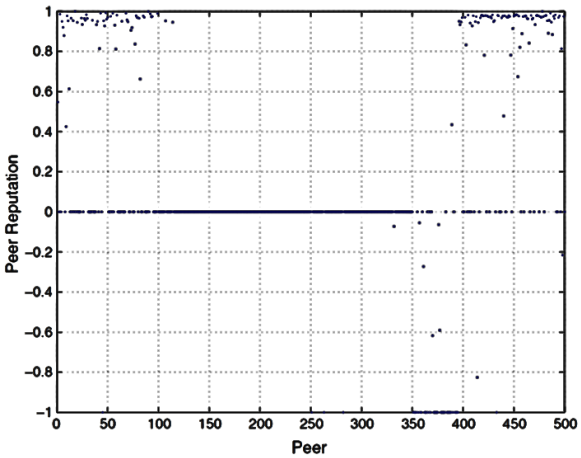

Figure 3. Peers Reputation in RBSD

Reputation is not an honest indicator of the contribution of the peer as are able to see from examination Figure 4, the Contribution Behavior value within the case of the Contribution based Service Differentiation (CBSD) technique. The Contribution Behavior value could be a smart indicator of the peer load share. In alternative words, a peer with a high contribution level is supporting additional load than a peer with a low contribution level. Note that the Contribution Behavior values of malicious peers that is peer id 246 to 395 area unit null. This is often as a result of malicious peers are harming the system by uploading malicious files. From this results, it is known that the Contribution Behavior price may be used for service differentiation which can effectively reward smart peers and penalize each free riders and malicious peers.

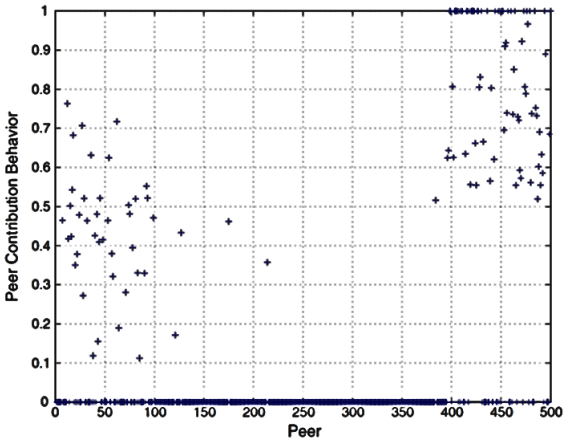

Figure 4. Peers contribution behavior in CBSD

The two figures (Figure 5& 6)shows the percentage of productive requests for RBSD and CBSD severally (i.e., accepted requests by the supernode). We have a tendency to additionally notice that free riders have concerning 500th probability to possess their request processed by the supernode. Free riders with high name values (i.e., peer id 1 to 100) have nearly identical proportion of productive requests as non-malicious contributor peers. However, free riders failed to contribute at identical level. The free riders with id from one to a hundred, have a lower proportion of productive requests since they uploaded solely few files compared to non-malicious contributor peers GCP. The latter peers are rewarded with a high level of service since they need supported the majority the load. They contributed considerably and completely to the system. The supernode processed their requests with a high probability. A number of the malicious peers' uploaded additional malicious content than smart one, therefore their proportion of productive requests is incredibly low.

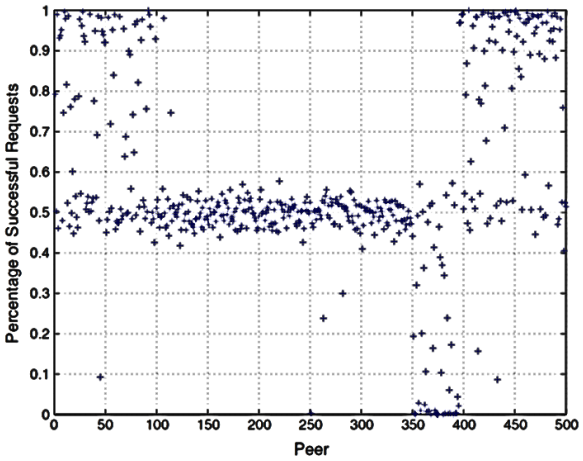

Figure 5.Percentage of successful requests for RBSD

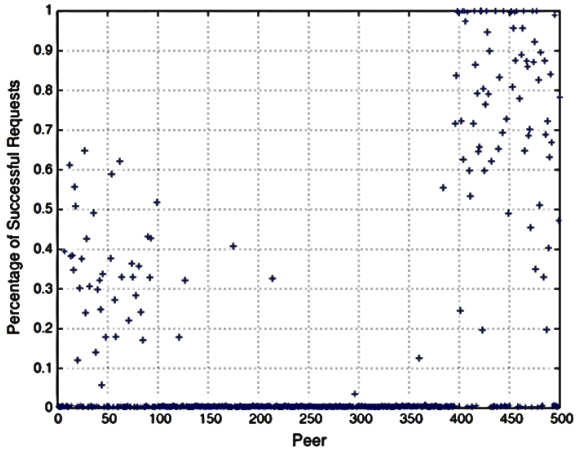

Figure 6.Percentage of successful requests for CBSD

Performance evaluations make sure the flexibility of the projected technique to effectively determine each free riders and malicious peers and cut back the amount of service provided to them. On Subsequently hand, good peers receive higher service. Forward a rational behavior, free riders tend to extend their contribution to urge higher service and indirectly reducing the load supported by smart contributor peers. Moreover, the projected technique generates a competitive surroundings wherever peers are forced to endlessly participate to learn from the system by reducing considerably.

V. CONCLUSION AND FUTURE WORK

Finally a distributed trust model for P2P networks is utilized, within which a peer will develop a trust network in its proximity. A peer will isolate malicious peers around itself because it develops trust relationships with smart peers. Two context of trust, service and recommendation contexts, are outlined to determine capabilities of peers in providing services and giving recommendations. Interactions and suggestions are thought of with satisfaction of super node. A recommendation contains the recommender's own expertise, data from its acquaintances, and level of confidence within the recommendation. These parameters provided from super node enable to user a stronger assessment of trait additionally to get rid of malicious nodes and suspected nodes. Individual, collaborative, and pseudonym ever-changing attackers are studied within the experiments to evaluate the damage of collaboration and pseudospoofing relies to attack behavior. Though recommendations are necessary in insincere and oscillating attackers, pseudospoofers, and collaborators, which are less helpful in naive and discriminatory attackers. Distributed Trust Management be each service and recommendation based mostly attacks in most experiments. However, in extraordinarily malicious environments like a 50 % malicious network, collaborators will still spread great amount of deceptive recommendations. This study have got not enclosed instances like a node leaves and joins another node within the same cluster within the same cycle. This sort of instances based mostly study will be enlarged as future work.

REFERENCES

[1] K. Aberer and Z. Despotovic, "Managing Trust in a Peer-2-Peer Information System," in The 9th International Conference on Information and Knowledge Management, Atlanta, USA, November 2001, pp. 310– 317.

[2] F. Cornelli, E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, and P. Samarati, "Choosing Reputable Servents in a P2P Network," in The 11th International World Wide Web Conference, Honolulu, USA, May 2002, pp. 376–386.

[3] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The EigenTrust Algorithm for Reputation Management in P2P Networks," in The 12th International World Wide Web Conference, Budapest, Hungary, May 2003, pp. 640–651.

[4] M. Gupta, P. Judge, and M. Ammar, "A Reputation System for Peerto-Peer Networks," in ACM 13th International Workshop on Network and Operating Systems Support for Digital Audio and Video, Monterey, USA, June 2003, pp. 144–152.

[5] L. Xiong and L. Liu, "Peertrust: Supporting reputation-based trust for peer-to-peer

electronic communities," IEEE Transactions on Knowledge and Data Engineering, vol. 16, no. 7, pp. 843–857, 2004.

[6] "Kazaa," http://www.kazaa.com/.

[7] "Morphus," http://www.morphus.com/morphus.htm.

[8] "Gnutella2 Specification," http://www.gnutella2.com/.

[9] S. Androutsellis-Theotokis, "A Survey of Peer-to-Peer File Sharing Technologies," Tech. Rep., ELTRUN, 2002.

[10] L. Mekouar, Y. Iraqi, and R. Boutaba, "A Reputation Management and Selection Advisor Schemes for Peer-to-Peer Systems," in The 15th IFIP/IEEE International Workshop on Distributed Systems: Operations & Management (DSOM), Davis, USA, November 2004

[11] L. Mekouar, Y. Iraqi and R. Boutaba, Peer-to-Peer's Most Wanted: Malicious Peers. Comp. Net., vol. 50, no. 4, Mar. 2006, pp. 545–62.

[12] W. Ji, S. Yang and B. Chen, A Group-Based Trust Metric for P2P Networks: Protection against Sybil Attack and Collusion. International Conference on Computer Science and Software Engineering, 2008 Volume: 3, Page(s): 90 - 93.

[13] Q. Lian, Z. Zhang, M. Yang, B. Y. Zhao, Dai Y. and X. Li, An empirical study of collusion behavior in the maze P2P file-sharing system. In IEEE ICDCS, June 2007.

[14] Z. Despotovic and K. Aberer, P2P reputation management: Probabilistic estimation vs. social networks, Computer Networks 50 (2006) 485–500.

[15] A. Tehale, A. Sadafule, S. Shirsat, R. Jadhav, S. Umbarje, and S. Shingade. Parental Control algorithm for Sybil detection in distributed P2P networks. International Journal of Scientific and Research Publications, Volume 2, Issue 5, May 2012.

[16] C. Selvaraj and S. Anand. A survey on Security Issues of Reputation Management Systems for Peer-to-Peer Networks. Computer Science Review, In press.

[17] X. Jin and S.-H. G. Chan. Detecting malicious nodes in peer-to-peer streaming by peer-based monitoring. ACM Trans. Multimedia Comput. Commun. Appl., vol. 6, no. 2, pp. 9:1–9:18, 2010.

[18] E. Koutrouli and A. Tsalgatidou. Taxonomy of attacks and defense mechanisms in P2P reputation systems—Lessons for reputation system designers. Computer Science Review, 2012.

[19] Z. Liu, P. Dhungel, D. Wu, C. Zhang and K. W. Ross, Understanding and Improving Incentives in Private P2P Communities. In ICDCS 2010, Italy, Jun. 2010.

[20] H. Lee, J. Kim and K. Shin, Simplified clique detection for collusion-resistant reputation management scheme in P2P networks. In 2010 International Symposium on Communications and Information Technologies (ISCIT), 2010, Page(s): 273 - 278.

[21] G. Ciccarelli and R. L. Cigno, Collusion in peer-to-peer systems, Computer Networks, Comp. Net., vol. 55, no. 15, Oct. 2011, pp. 3517–3532.

[22] Y. Liu, Y. Li, N. Xiong, J. H. Park and Y. S. Lee, The incentive secure mechanism based on quality of service in P2P network, Computers and Mathematics with Applications, 60 (2010) 224-233.

[23] X. Wei, T. Ahmed, M. Chen, and A.-S.K. Pathan, PeerMate: A malicious peer detection algorithm for P2P Systems based on MSPCA, in Proc. IEEE Int. Conf. on Computing, Networking and Communications (ICNC), Lahaina, HI, USA, Jan. 2012, pp.815-819.