A Trust Model for Identifying Malicious Behavior in P2P Networks

Swapna H
Sree Chitra Thirunal College of Engineering
Trivandrum

Jayasudha J.S
Sree Chitra Thirunal College of Engineering
Trivandrum

Sabu M Thampi
School of Computer Science
Indian Institute of Information Technology and Management-Kerala

ABSTRACT
Peer-to-Peer (P2P) systems allow all peers to communicate and share resources with equal responsibility thereby eliminating the need for central authorities. These networks have gained wide popularity in providing services ranging from file sharing to distributed computing applications. In P2P networks the peers can join or leave the system dynamically and so the network topology changes due to this behavior. These features of a P2P make it vulnerable to different types of attacks. Trust and Reputation models can be used to minimize the impact of such threats. This paper proposes a trust model to identify malicious nodes in a P2P network. The main aim of the paper is to deploy a trust model for determining the trust value of peers with the notion of avoiding malicious ones. In this paper the global trust of a base peer is computed by only those set of peers that are reliable to the base peer. This can greatly help to reduce the computation and communication overhead associated with other trust and reputation based models where all the interacted peers have to respond to compute the global trust of the base peer. The proposed model takes the responsibility to detect malicious nodes and eliminates them from the system.

General Terms
Algorithms, Reliability, Security.

Keywords
Peer to Peer, Reputation, Trust, DDoS attack.

1. INTRODUCTION
P2P networks have gained wide popularity as a medium for sharing huge amounts of data. These types of networks allow users to share files and data located on their own computers and share resources found on other computers. All the peers in a P2P network are considered equal and they possess same abilities to effectively utilize available resources on the network.

The peers in such a network can join or leave the system in a random manner and so the network topology changes due to this dynamic behavior [1]. These features of a P2P make it vulnerable to different types of attacks such as Distributed Denial of Service attack (DDoS attack). A DDoS attack is an attempt to make a resource unavailable to others who intend to use it. The most common form of such an attack is flooding of invalid queries into the system. This prevents valid queries for files or queries for parts of file from being delivered. Hosts in a P2P network should be able to identify reliable or trust worthy peers to protect themselves from malicious entities.

Security mechanisms can be used to offer protection against the malicious agents. The traditional mechanisms used for such security protect resources from malicious users, by restricting access only to authorized users. But in some cases the providers of resources themselves can provide false or misleading information, in such cases the traditional security mechanisms fail. These mechanisms are called hard security measures such as authentication and access control based on cryptography. In such situations we have to use soft security measures like trust and reputation based mechanisms [2, 3].

Identification of reliable peers is a challenging task for a dynamic network like a P2P network [4]. To address this, several solutions have been proposed based on trust and reputation [5-10].

In this paper we propose a trust model to identify malicious peers in a P2P network. We identify the malicious peers which inject invalid queries to the network based on the computed trust values. Most of the existing models on trust and reputation compute global trust value of a peer by considering response from all interacted peers in the network. Thus the computation and communication overhead is very high since all peers in the network are engaged in the trust computation. The computation of global trust of a peer say $peer_i$ can also involve responses from peers which $peer_i$ may consider malicious. Hence in our proposed method we restrict the global trust computation of peer with only those peers that $peer_i$ treats benevolent peers i.e., peers reliable to the former.

The rest of paper is organized as follows. Section 2 discusses the related works. Section 3 is the proposed scheme. Section 4 discusses the simulation set up. Section 5 is the result and analysis section. Section 6 concludes the paper with future work.

2. RELATED WORKS
To achieve better cooperation between peers and to reduce the number of malicious file uploads by peers, trust management is very essential in a P2P file sharing system. In a reputation based P2P system, reputation is used to build trust among peers based on the peer's history of transactions and uploads. In such systems usually reputed peers will be selected to upload requested files, thereby decreasing significant malicious uploads in the system [11].Trust management is very difficult in peer to peer networks because a peer cannot know all other peers in that network. Efficient trust management model is necessary to manage and distribute trust on peers to distinguish good and bad peers [12].

To counter the problem of spreading inauthentic files in a P2P networks several trust and reputation models have been proposed such as Eigen Trust[13],Peer Trust[14],Cuboid Trust[15], AntRep[16] and many others[17-22].

Eigen Trust is one of the most cited trust and reputation based model used in P2P systems [13]. It is a method that can fight against malicious peers and allow P2P file sharing to remain feasible. This model assigns each peer a local trust value with every other peer with which it had interacted. Also the model

assigns each peer a global trust value computed by all the peers that had interacted with the peer based on the local trust values. The algorithm converges only if all peers respond with their local and global trust values. Thus, the algorithm assigns each peer with a unique global trust value based on the peer's history of uploads thereby achieving a decrease in the number of inauthentic file downloads. The algorithm introduces the concept of pre trusted peers that help fast convergence of the algorithm and avoid the interaction with malicious collectives to certain extent .The global trust value is used to determine the probability of a peer in being selected as the download source. The algorithm does not discuss about the case where some set of peers does not respond with their trust values.

Peer Trust[14] is a reputation based trust supporting system that includes a coherent adaptive trust model for quantifying and comparing the trust worthiness of the peers. The trust values are compared based on a transaction based feedback mechanism. This model possesses two important features. One feature is that it introduces three basic trust parameters and two adaptive factors in computing the trustworthiness of peers. The basic trust parameters are feedback a peer receives from others, the total number of transactions a peer performs and the credibility of the feedback sources. The adaptive factors include transaction context factor and community context factor. The second important feature is that it defines a general metric to combine these parameters. The way it measures the credibility of a peer does not distinguish between the confidence placed on a peer when supplying a service or carrying out a task, and when giving recommendations about other peers.

CuboidTrust[15] is a global reputation based trust model which builds four relations among the three trust factors contribution of the peer to the system, trustworthiness of the peer in reporting feedbacks and the resource quality. The model applies power iteration in order to compute the global trust value for each peer in the network. Here, direct trust values are not given a differentiated treatment and the score takes discrete values in the set {1,-1} instead of continuous values in the interval [-1, 1] which cannot be well interpreted. Like Eigen Trust algorithm this algorithm also maintains the concept of pre trusted peers.

AntRep[16] is a reputation model where the reputation evidences are distributed over the P2P network, based on a swarm intelligence paradigm. In this model, each peer has a reputation table which is very similar to distance routing table. The model differs from the distance vector routing table in two aspects (i) each peer in a routing table corresponds to a single reputation content (ii) the metric used is the probability of choosing each neighbor as the next hop instead of the hop count to destinations. AntRep has the ability to easily adapt to the dynamic topologies of P2P networks.

Eigen Trust makes use of transitive trust which means a peer trusts those peers that possess a high reputation in the opinion of trust worthy peers. Researchers proposed a negative trust metric in [17] that combines negative opinions like Badness, Positive Dishonesty and Negative Dishonesty with Eigen Trust in a single reputation algorithm. The resulting framework is very effective in reducing the number of inauthentic downloads from malicious peers. Also the model is found very effective against a number of threat attacks from the coalition of malicious peers. The model detects most of the malicious peers using an improved K means Clustering algorithm.

3. PROPOSED WORK

One drawback of the distributed Eigen Trust algorithm [13] is that the algorithm will not converge unless all peers respond with their global and local values. Even if one of the peers fails to report their trust value the algorithm will not converge. This requirement does not seem to be a reasonable since in a P2P network; one cannot expect peers to respond with a query always. If a peer say $peer_i$ has got a very good past reputation then definitely it will have many number of nodes having downloaded from it. Also the trust value of $peer_i$ is computed by all peers in Set A (set of peers interacted with peer i) which may also contain peers that $peer_i$ treats malicious. So the proposed mechanism will not consider all peers in Set A, but a subset of peers in A say A' which is the set of peers in A that are benevolent to $peer_i$. In the proposed mechanism we filter the nodes in A into a set A' which contains peers benevolent to $peer_i$ i.e. the set of reliable peers to $peer_i$. Peers that are benevolent to peer i should satisfy the minimum criteria being specified by peer i. The experiments conducted prove that the proposed work provide results faster than the existing algorithm.

3.1 Modified Global Trust Calculation algorithm

The network model consists of two types of peers: normal or good peers and bad or malicious peers. Normal peers participate in the network to download resources/files, always share authentic information and give exact rating to each resource it has consumed. But the malicious peers on the other hand upload inauthentic or pirated resources having the main notion of subverting the system. In our network set up we assume the existence of small fraction of pre trusted peers which are normal peers which will never act malicious or upload any wrong information. These peers are included in the network mainly for reducing the impact of malicious collectives. In existing scheme to calculate the global trust value of a peer all peers having interacted with it have to respond. But in the proposed scheme to compute the global trust of a peer, we consider only those peers that are benevolent to the former. We assume that the peers that satisfy the minimum criteria specified by the former are benevolent to it. Let $peer_i$ be the peer whose global trust value need to be computed. A is the set of peers having downloaded files from $peer_i$. Only those peers that satisfy the following conditions take part in the global computation of $peer_i$ in the algorithm proposed in [13]. The conditions that peers *benevolent* to $peer_i$ should possess include the following:

1. Minimum number of successful transactions with $peer_i$.
2. Contribution score of the peers in the network is always greater than one.
3. Peers possessing local trust score above the threshold set by $peer_i$.
4. Number of requests for the same file (before the actual downloading finishes) is less than minimum number of requests.

The peers that satisfy the above conditions are said to be benevolent to $peer_i$. Each peer has a contribution score based on the quality and the amount of files it shares. It is a number that tells about the upload and download rate of the peers. It is computed as ratio of number of files uploaded by a peer (along with its upload file quality parameter) to the number of files downloaded by a peer. A selfish peer will always have a

value near to zero for this contribution score. For a malicious peer even if the value of number of uploaded files outnumber the number of downloaded files, this score value will be less than 1, since the quality of files uploaded value will be very feeble. This file quality parameter is obtained by collecting feedback from other peers having interacted with it regarding its upload file contents.

We filter the nodes in A into the set A' which is the set of benevolent nodes to $peer_i$. Using the new approach if all peers in A' respond with their trust values then we can easily compute the global trust value of $peer_i$. Moreover this approach also minimizes the computational overhead in considering the trust values of all peers in A in cases if $peer_i$ had transactions with majority of nodes in the network. The last criteria can be used as a good indicator of a malicious peer since such a peer will always ask for the same file before the actual downloading finishes with the sole purpose of subverting the network.

Table 1: Notations used in the Algorithm

No	Notation	Meaning
1	N(i,e)	Number of Transactions between peers i and e
2	MIN_TRANSACT	Minimum number of transactions between two peers
3	S(i,e)	Local trust score of e with i
4	TR_THRES	The threshold local trust value
5	CS(e)	Contribution score of peer e
6	REQ_FILE	Request for the same file before the actual downloading finishes
7	TS	Tracker Server
8	NS(i)	Neighbors of peer i
9	E(i)	Cardinality of NS(i)
10	Π	Maximum number of connections for each peer
11	threshold_trust	Global trust threshold
12	MIN_R	Minimum number of requests for the same file

Case 1: New Peer Joining the Network

1. Peer p is joining the network for the first time.
2. p contacts the tracker server TS to get the list of currently active peers.
3. p randomly selects peer Pr if and only if the following conditions hold.
   If E(Pr)< π and S(Pr,i)=0 then
   connect(Pr,p)=1.
4. Otherwise p picks another peer from TS.

Case 2: Connection to be established between two peers j and k already transacted and disconnected later.

1. Peer j requests for a file say F.
2. j contacts tracker server which responds with set of peers possessing F , the list also contains k.
3. j first sends out a connection request to peer k.
4. Peer k on receiving the request establishes connection with j only if the following conditions hold.
   If E(k) < π and S(j,k)> TR_THRES then
   connect(k,j)=1
   E(k)=E(k)+1.
   Else if If E(k) < π and S(j,k)< TR_THRES then
   connect(k, j)=0.
   Then j selects another peer from T

Case 3: No prior transaction occured between j and k. k on receiving request from j, retrieves the transaction list of j, N(j) from which it takes the recommendation ratings of peer j.

1. If E(k)< π and S(j,k)=0 then
   K retrieves the list NS(j).
2. For every peer m in NS(j) do
   Aggregate the recommendations S(m,j) to get the global trust value of peer j, G(j).
3. If G>threshold_trust then
   Connect(k,j)=1 and
   E(k)=E(k)+1.
4. Else Connect(k,j)=0.

Case 4: Updation of Ratings for every transaction between j and k.

[1] Having established connection with peer k, peer j may rate k based on the file download from k.
S(k,j)=S(k,j)+β for every successful file transfer from k

[2] If the file downloaded is not the desired one or is of poor quality then
S(k,j)=S(k,j)-β
where β is the trust update parameter 0< β<1.

Algorithm: Global Trust Calculation of Peers

1. Assume that we have a set of pre trusted peers which never behave maliciously and always provide good files. In the initial set up only the pre trusted peers have trust value greater than 0 and all other peers have their initial global trust value equal to zero.
2. When peer 'a' transacts with peer 'b' it will access the quality of transaction as the function g(a,b) defined as

   g(a,b) = 1 if transacted file is of desired quality.
   = 0 if not the desired file.
3. Based on the above function, the local trust score value is defined as

$$S(a,b) = \sum_{k=1}^{num} g(a,b) / num$$

   where *num* is the number of transactions between a and b. If num=0 then S(a,b)=0.

4. To find the global trust of a peer say i, select the set of peers that have interacted with peer i say the set A.
5. For every element e in A do the following

   If N(i,e) > MIN_TRANSACT && S(i,e)> TR_THRES && CS(e)>1 && REQ_FILE<MIN_R then

   Add e to the new set A'.

6. The global trust computation of a peer i will include only those peers in set A'.
7. For every peer i
   i) Ask every peer j in A' about its opinion about i.
   ii) Repeat until trust values do not change
      (1) Compute global trust value by aggregating the opinions and trust values.

$$T_i(k+1) = \sum_{i=1}^{|A'|} S\ (i, j) * T_i(k)$$

      (2) Repeat the above two steps until all peers in A' respond, we will get the global trust value of peers.
8. If the global trust value of peer is below the trust threshold then that peer is treated malicious and can be removed from the network.

Existing algorithms take into account all peers in the global trust computation. In the proposed scheme we consider only those peers in the set A'. Thus the complexity reduces to O (nm) where n is the total number of peers and m is the number of peers satisfying the criteria, and always m<n. Thus the algorithm is better than existing algorithm that takes complexity of the form O (n^2).Thus the proposed scheme is better than the existing ones.

4. EXPERIMENTAL SET UP

We have conducted the experiments in Java. In our experiments, each peer is capable of both downloading and uploading files. Each peer is identified using a unique identifier say its IP address. As the dynamic network grows in size, a peer is elected as the supervisor (dynamic in nature). This supervisor has the role of a tracker server that keeps track of the peer list and resources. Whenever a peer wants a particular file, it requests it to the supervisor which will direct it to the appropriate peer holding the file. If the same file fragment is located at more than one machine then the supervisor initiates a load balancing algorithm where the file is accessed from the machine from where it was least accessed. The supervisor selection is dynamic in the sense, each time the network is set up; the supervisor is elected (as the one possessing the highest IP). The supervisor keeps the record of all listing of files and other resources of peers in that network.

The network model consists of nodes transacting with fixed number of neighbors. Each peer maintains the history of all nodes it has transacted with. Every peer in the network is capable of providing both authentic and inauthentic files to other peers in the network. The node parameters include neighbor list and for every neighbor, the number of transactions, number of requests for the same file, the time stamp of the request etc. Based on the history of transactions, each peer is assigned a global trust score as its reputation in the network.

The assumption that malicious peers upload inauthentic files in most of the cases hold true and eventually they can inject invalid queries into the system. Based on the history of transactions the trust value corresponding to the peers may vary. If the peers upload good files and possess a good resource sharing capability in the network, then they can achieve a high trust value. Eventually if at any time it is exhibits an inauthentic behavior, it gets a low trust rating from other peers in the network. Finally those peers whose trust value is below the threshold trust value are treated malicious and removed from the system since such malicious peers are capable of producing a DDoS attack. The results show that peers with low global score are capable of providing a higher fraction of inauthentic files than authentic files and are to be removed from the network.

We have simulated a Peer to Peer network with 100 nodes. The network consists of a sizeable population of malicious peers uploading inauthentic files and good peers providing authentic files. We also assume the presence of pre trusted peers which never upload wrong or inauthentic files. The result section discusses the global trust values with the existing approach where all peers engage in trust computation and our proposed scheme where only benevolent peers take part in trust computation. The graphs prove that malicious peers upload a higher fraction of inauthentic files than authentic files. The algorithm efficiently identifies the peers that possess global trust values below the trust threshold and are removed from the network.

5. RESULTS AND ANALYSIS

The following section discusses how trust values of peers are computed using both existing and proposed algorithms. In existing algorithm all peers engage in trust computation. Here we simulate the experiment using 100 peers. Figure 1 shows graph representing the global trust values of the 100 peers using Eigen Trust algorithm calculated based on its history of transactions with other peers. Our main objective is to identify the malicious peers uploading more inauthentic files than authentic files based on the notion of trust. These malicious peers have the main intention of subverting the system and thereby can induce a DDoS attack in a P2P file sharing system. These malicious peers will possess a global trust value less than the threshold and can be easily identified as in Figure 1 and Figure 2.

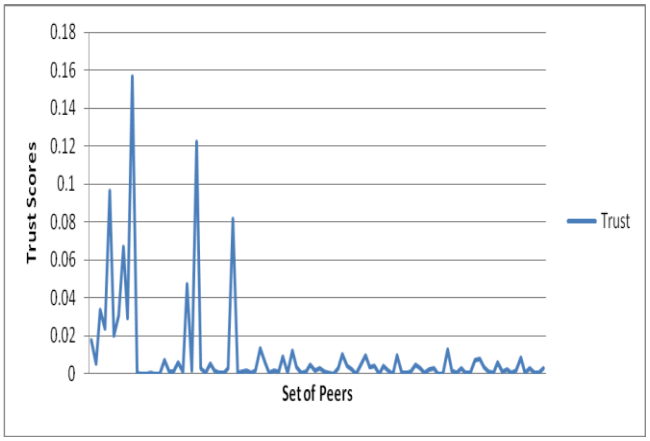

Figure 1: Global Trust Values using Eigen Trust Algorithm

Figure 2 shows the trust values generated using the modified trust computation algorithm where only those peers reliable to a peer will take part in its trust computation.

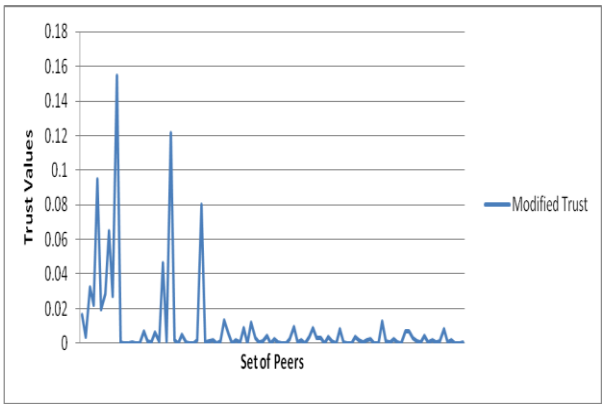

Figure 2: Global Trust Values using Modified Trust Algorithm

The computed global trust values obtained using the improved approach is less than the existing Eigen Trust algorithm. This is because not all peers engage in trust computation, only reliable peers engage in trust computation. The main aim of our approach is not to maximize the peer's global trust values but to compute the global trust values of peers by only those peers that are benevolent to it. The resulting trust value of a peer is reliable since they are computed by only those peers that the peer finds trustable thereby preventing opinion from peers that it finds malicious. In existing approach only if all peers respond with their opinions, we are able to compute the global trust values. If any one of the peers does not respond, then the algorithm will not converge. In the proposed work, it is required that only benevolent peers respond with their opinions to compute the global trust value.

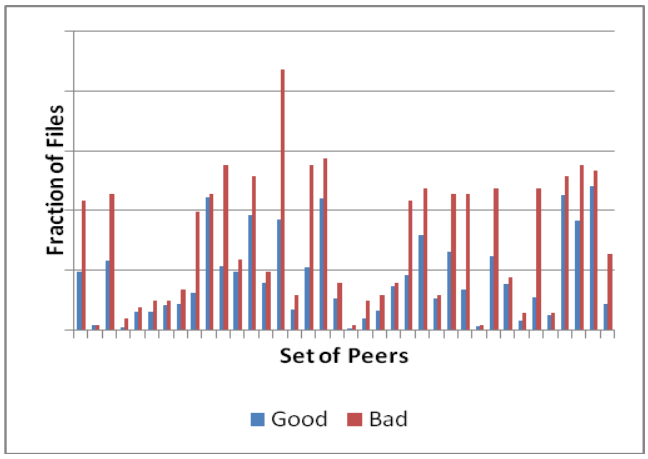

Figure 3: Fraction of files uploaded by malicious peers

In our experiment, we get 38 peers out of 100 possessing a trust value below the threshold trust.

The malicious peers upload a higher fraction of inauthentic files than authentic files. Figure 3 shows the fraction of files both authentic and inauthentic files uploaded by all the identified malicious peers. From the graph it is very clear that these peers upload greater fraction of inauthentic files than authentic files. Also the experimental set up shows that the proposed algorithm converges with the final trust values faster than the existing approach since in the new approach only benevolent peers engage in trust computation. Convergence is defined as that point where the global trust value does not change in further iterations. To justify the convergence of the trust values we considered a 10 peer (p1 to p10) network. Figure 4 and Figure 5 show the convergence of the global trust values using existing approach and proposed approach. The graphs show that the proposed algorithm converges in fewer numbers of iterations than the existing algorithm.

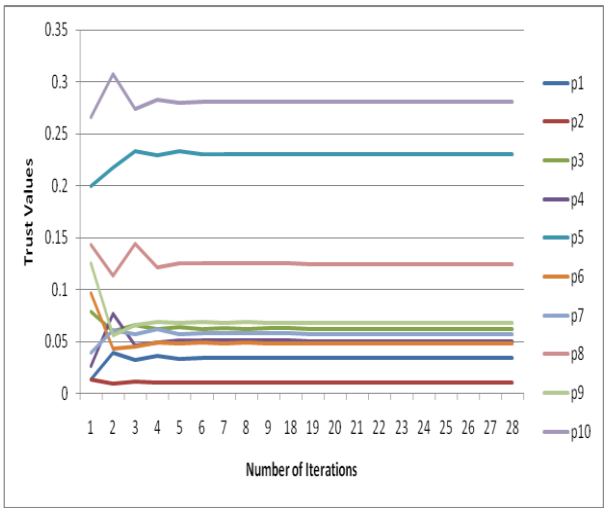

Figure 4: Convergence of Trust Values using Existing algorithm

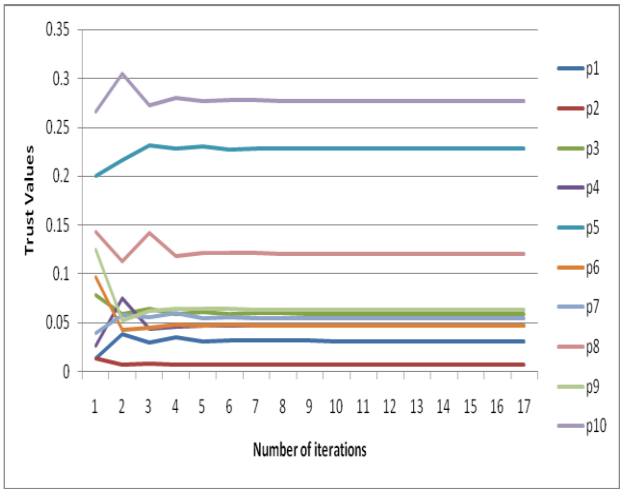

Figure 5: Convergence of Trust Values using proposed algorithm

In the proposed algorithm since only benevolent peers engage in trust computation, the algorithm converges in fewer number of iterations than the existing one. Figure 5 shows the convergence of peers to their final values using proposed method.

6. CONCLUSION

This paper proposes a trust based model to identify malicious peers in a P2P file sharing environment. Using the Eigen Trust algorithm, a unique global trust value is assigned to each peer in the network based on local trust score of peers, moreover all nodes take part in the global trust computation. In this paper the trust score of a peer is computed by only those peers that the former treats benevolent. Benevolent peers are those peers that satisfy the minimum criteria specified by the base peer. The resulting framework is found very effective in reducing the number of inauthentic file downloads in the system. This is because the peers providing more inauthentic files are identified based on its low trust rating and are removed from the network. This framework can improve resistibility against DDoS attacks in a Peer to Peer file sharing system, since the malicious nodes are identified and removed.

7. REFERENCES

[1] Lin Wang. 2006. Attacks against Peer to Peer Networksand Countermeasures. Seminar on Network Security,TKK T-110.

[2] Audun Jøsang, Roslan Ismail and Colin Boyd, "A Survey of Trust and Reputation Systems for Online Service Provision". Journal Decision Support Systems, 2007, Vol 43, Issue 2, pp 618-644.

[3] Xiaoliang Wang,Lincong Yang,Xingming Sun,Jinsong Han,Wei Liang and Lihong Huang, "Survey of Anonymity and Authentication in P2P Networks". Information Technology Journal, 2010, 9:1165-1171.

[4] Natalia Stakhanova,Sergio Ferreri, Johnny S.Wong and Ying Cai,2006.A Reputation based Trust Management in Peer to Peer Network. Proceedings of ISCA,pp 510-515.

[5] Selpk. A.A., Uzun,E. and Pariente, A., 2004.Reputation-Based Trust Management System for P2P Networks.IEEE International Symposium on Cluster Computing and Grid,pp 251-258.

[6] Kim,Y., Mazzocchi, D. and Tsudik,G. 2003. Admission Control in Peer Groups .Second IEEE International Symposium on Network Computing and Applications,pp 131.

[7] Huu Tran, Michael Hitchens, Vijay Varadharajan and Paul Watters 2005. A Trust based Access Control Framework for P2P File-Sharing. Proceedings of Annual Hawaii International Conference on System Sciences,pp 302c.

[8] Park, J.S., An, G. and Chandra, D. 2007. Trusted P2P computing environments with role based access control. Information Security, IET Volume 1, Issue 1,pp 27-35.

[9] Gaspary, L. P., Barcellos,M. P., Detsch, A. and Antunes, R. S., " Flexible Security in Peer to Peer Applications: Enabling new opportunities beyond File sharing", International Journal of Computer and Telecommunications Networking, 2007,Vol 51.

[10] A.Gupta, D.Malhotra and L.K. Awasthi, 2008.NeighborTrust: A trust based scheme for countering Distributed Denial of Service attacks in P2P Networks. Proceedings of 16 th IEEE International Conference on Networks, pp 1-6.

[11] Loubna Mekouar, 2010. Reputation Based Trust Management in Peer to Peer File Sharing Systems. Thesis Report. University of Waterloo.

[12] Moalla, S., Hamdi, S. and Defude, B., 2010. A New Trust Management Model in P2P Systems. Proceedings of International Conference on Signal Image Technology and Internet Based Systems,pp 241-246.

[13] Sepandar ,D. Kamvar, Mario, T. Schlosser and Hector Garcia-Molina, 2003. The Eigen Trust Algorithm for Reputation Management in Peer to Peer Networks. Proceedings of International Conference on World Wide Web, pp 640-651.

[14] L.Xiong and L. Liu,2004.PeerTrust:Supporting Reputation Based Trust for Peer to Peer Electronic Communities.IEEE Transactions on Knowledge and Data Engineering, Vol 16,pp 843-857.

[15] Chen, X. Zhao, L. Tang, J. Hu, and Z. Chen, 2007. CuboidTrust: A Global Reputation based Trust Model in Peer to Peer Networks. Autonomic and Trusted Computing, Lecture Notes in Computer Science, Vol 4610, pp 203-215.

[16] W. Wang, G. Zeng and L.Yuan, 2006.Ant-Based Reputation Evidence Distribution in P2P Networks. Proceedings of International Conference on Grid and Cooperative Computing, pp 129-132.

[17] Debora Donato, Stefano Leonardi and Mario Paniccia, 2008. Combining Transitive Trust and Negative Opinion for better Reputation Management. Workshop on Social Network Mining and Analysis.

[18] Han Yu, Zhiqi Shen, Chunyan Miao, C. Leung and D.Niyato, 2010. A Survey of trust and reputation management in wireless communications. Proceedings of the IEEE, 98(10):1755-1772.

[19] Chun-Ling Cheng, Xiao-Long Xu and Bing-Zhen Gao, "MEtrust: A Mutual Evaluation Based Trust Model for

P2P Networks". International Journal of Automation and Computing, 2012, V9 (1):63-71.

[20] Y. Wang, Y. Tao, P. Yu and F. Xu, 2007. A Trust Evolution Model for P2P Networks. International Conference in Autonomic and Trusted Computing, pp 216-225.

[21] F. Yu,H. Zhang, F.Yan and S.Gao,2006. An Improved Global Trust Value Computing Method in P2P System. Autonomic and Trusted Computing, Lecture Notes in Computer Science, Vol 4158, pp 258-267.

[22] Chunqi Tian, Baijian Yang, "R2Trust - a reputation and risk based trust management framework for large –scale, fully decentralized overlay networks". Journal Future Generation Computer Systems, 2011, Vol 27, Issue 8, pp 1135-1141.