ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

# Self - Organizing Trust with Predictability Trust for Reputation Management in Peer to Peer File Sharing

[I]Aswani Ashok, [II]Jayakumar T.V
[I,II]Dept. of CSE, Vidya Academy of Science & Technology, Thrissur, India

**Abstract**
*Peer to Peer (P2P) file sharing systems are endangered by different security threats. In this type of network, security established by using trust models. Self-Organizing and predictability trust model aims to decrease malicious activities in P2P file sharing systems. This method uses centralized P2P network model, where some functionalities are centralized ( indexing is centralized and file sharing is distributed). Two context of trust is used to measure trustworthiness of peers from which files are downloaded - trust metric evaluation using Self Organizing Trust model and Predictability Trust. Parameters used for trust value calculations are based on peer capabilities, behaviour and resource distribution. Predictability Trust works with Self Organizing Trust method give a second chance to a peer, which has been evaluated as malicious, by recovering a trust value based on time. The performance of the system can be measured by, the ratio of number of successful transaction by peers with the total number of transactions.*

**Keywords**
*Trust, File sharing, Trust recovery, security, Trust models.*

## I. Introduction

Peer to Peer(P2P) networking is mainly used for sharing of files and applications among internet users. Trust and reputation methods are used to improve the quality of services provided in P2P file sharing. The distributed peers have equal roles or capabilities for sharing information's directly with each other. A peer plays the role of a client and a server at the same time ie, the peer can initiate requests to other peers, and at the same time respond to incoming requests from other peers on the network. Trust management systems were introduced to solve the security problems in peer to peer file sharing systems. Trust and reputation values are used to build trust among peers based on their past transactions and feedbacks from other peers that are explicitly set by the users. Reputation systems are based on collecting information about peer's past transactions and computing a reputation value for these peers. Trust management systems assign to each peer a trust score that can be used by other peers to decide whether or not to interact with that peer. Therefore, many trust and reputation management systems have been proposed to prevent attacks on P2P file sharing systems.

Recognizing and isolating malicious peers is significant in all P2P environments, otherwise peers will not have the initiative to share their resources and will hesitate to send requests to other peers in fear of receiving corrupted or inauthentic files or being exposed to malware. Different security issues related with peer to peer file sharing are free riding, Malicious Peer interaction, Sybil attacks etc[1]. Peer to peer systems have recently gained an enormous influence in social, Academic and commercial communities.

BitTorrent [5] is an internet based peer-to-peer file sharing protocol that works in decentralized manner and it is one of the most commonly used protocols for transferring very large files. It doesn't overload web servers that provide downloads, and is much more efficient than downloading from a single server. Peers have optimized the upload and download rates in order to improve efficiency. An indexer compiles a list of torrents and their descriptions and is a place where users form a community around BitTorrent content. To share, download, or request files, indexer site has to be accessed. A tracker is a server that assists in directing peers, initiated downloads, and maintains statistics. Trackers route little pieces of data, or packets, to downloader's and assist them in connecting to their respective peers.

The proposed method uses centralized P2P[2] networking model, and uses a central server to store and manage trust information in P2P file sharing. Indexing of peers done by the central server based on their trustworthiness. The trustworthiness evaluated by service trust metric of self organizing trust model[3] and the consistency of performance of peers are calculated by predictability trust model[4]. Service trust metric evaluation done by different parameters based on the peer capabilities - bandwidth, number of shared files, peer behaviour- online and offline periods, waiting time for sessions, and resource distribution - file sizes, popularity of files[3].Trust is not a static value that keeps on changing based on the transactions. Predictability trust of peers are computed to identify whether the current trust value can accurately predict the peers future behaviour and whether the behaviour is consistent with its past behaviour.

This paper is organized as follows. In Section 2, the related works are presented. Then Section 3 describes proposed self-organizing and predictability trust model. And Section 4 provides experimental evaluations and finally conclusion of work.

## II. Related Research

Several surveys have addressed the problem of incorporating trust on peer to peer file sharing systems. Different ways of incorporating trust in P2P file sharing done by different parameters.

### A. P2P File Sharing Architectures

In general,P2P systems are categorized into two broad categories, centralized vs. decentralized, based on the availability of one or more servers, and to what extent the peers depend on the services provided by those servers. Besides these two main categories, there are also hybrid P2P systems that combine both centralized and decentralized architectures to leverage the advantages of both architectures[2].

### 1. Centralized P2P Systems

Centralized P2P systems combine the features of both centralized (e.g., client-server) and decentralized architectures. Like a client-server system, there are one or more central servers, which help peers to locate their desired resources or act as task scheduler to

coordinate actions among them. To locate resources, a peer sends messages to the central server to determine the addresses of peers that contain the desired resources (e.g., Napster[6]).

### 2. Decentralized P2P Systems

In a decentralized P2P system, peers have equal rights and responsibilities. Each peer has only a partial view of the P2P network and offers data and services that may be relevant to only some peers. As such, locating peers offering services and data quickly is a critical and challenging issue(eg. Gnutella [7]) . Currently, decentralized P2P networks file query method is based on either flooding where the query is propagated to all the node's neighbors, or random walkers where the query is forwarded to randomly chosen neighbors until the file is found.

### 3. Hybrid P2P Systems

Hybrid P2P systems have been introduced to take advantages of both centralized and decentralized architectures. To maintain the scalability, similar to decentralized P2P systems, there are no servers in hybrid P2P systems. However, peer nodes that are more powerful than others can be selected to act as servers to serve others. These nodes are often called super peers. In this way, resource locating can be done by both decentralized search techniques and centralized search techniques ( super peers), and hence the systems benefit from the search techniques of centralized P2P systems.

### B. Trust Models

The first trust algorithm designed by Aberer and Despotovic et al[8] is to identify dishonest peers by a complaint-based system. But it doesn't give trustworthiness to new peer and only the negative feedbacks is maintained. NICE trust[9] model is used to guard against malicious peers. Each peer at the ends of an interaction, creating a cookie with feedback about the other peer assigns it. The signed cookies are exchange among them. If the transaction is successful, the value of the cookie is positive, otherwise, the value is negative. The validity of the cookies provided will be justified by the provider. The Eigen trust[10] algorithm is performed as, the trust value of one peer is computed by some other peers. The global reputation of each peer is marked by the local trust values assigned to the peer by other peers,and it is weighted by the global reputation of the assigned peers.

Peer Trust[11], model evaluate a peer's trustworthiness based on past interactions. The parameters for trust evaluation are the feedback a peer obtains from other peers,the feedback scope, such as the total number of transactions that a peer has with other peers, the credibility factor for the feedback source, the transaction context factor for discriminating mission critical transactions from less or noncritical ones, and the community context factor for addressing community related characteristics and vulnerabilities. The Power Trust[12] system dynamically selects small number of power nodes that are most reputable using a distributed ranking mechanism. A trust overlay network is used to model the trust relationships among peers. It collects locally generated peer feedbacks and aggregates them to yield the global reputation scores. By using a random-walk strategy and utilizing power nodes, feedback aggregation speed, and global reputation accuracy are improved.

Gossip Trust[13] computes global reputation scores of all nodes concurrently . By resorting to a gossip protocol and leveraging the power nodes, Gossip Trust is adapted to peer dynamics and robust to disturbance by malicious peers. The Gossip-based Reputation Aggregation module supports both initial reputation computation and reputation updating. After each round of global reputation computation, Gossip Trust will identify power nodes for the next round of reputation updating. A partially decentralized reputation-based Trust Management System(TMS) [14] for BitTorrent(BT) uses global trust scores to evaluate peers as well as their local trust scores. Each peer assigns a trust score to each of its neighbors and the tracker of each BT swarm to maintain global trust scores. The tracker is a peer that assists in the communication between peers using the protocol by keeping complete membership information.

### C. Trust Redemption

Trusted peers becomes loss their trustworthiness due to some unintentional errors such as network loss. Trust values are dynamic,ie, the values are changed after transaction. Redemption techniques are used to recover trust values for untrusted nodes. Two types of redemption methods are 1)Behaviour based redemption recovers trust based on subsequent behaviours and 2) Time based redemption recovers trust based on time. The combination of these two redemption methods are called combined redemption method. Redemption techniques helps peers to get a second chance to recover their trust value which has been erroneously evaluated as malicious. This method is applicable to on-off attacks[15][16].

## III. Trust Method

The self-organizing and predictability trust model is designed for secure peer to peer file sharing applications. Centralized P2P architecture used in this method. The central server is used for indexing the trustworthy peers and file sharing done in the distributed fashion. Peers can join and leave the network occasionally. Two types of interactions are considered- Upload and Download of files. No trust value calculation for uploading a file. Download files from peers based on their trust value indexed in the central server. Trust metrics evaluation is done during downloading. Trust evaluated by using two methods- Service trust metric by self- organizing trust model and predictability trust. High ranked peers have upload authentic file and less ranked are malicious.

### Trust Metric ($t_{ij}$ )

Satisfaction is denoted as 'S ' and is calculated using the variables bandwidth and online period.

**Band width**- Before starting an interaction, a downloader makes a bandwidth agreement(AgrBw) with the uploader, which declares the amount of bandwidth it can use. The ratio of average bandwidth (AveBw) and agreed bandwidth (AgrBw) is a measure of reliability of an uploader in terms of bandwidth

**Online period** - The ratio of online (OnP) and offline (OffP) periods represents availability of an uploader.

satisfaction of $k^{th}$ interaction with pi and $p_j$ calculated by using equation.

$S_{ij}^{k} = \{((AveBw/AgrBw)+(OnP/(OnP+OffP)))/2$ if AveBw<AgrBw}

$S_{ij}^{k} = (1+(OnP/(OnP+OffP))/2$ otherwise

The weight of an interaction is calculated based on two variables: File size and popularity. Large file have high importance due to high bandwidth requirement. Therefor files over 100MB have the same importance. Popular files are more important than unpopular ones. $Uploader_{max}$ is the number of uploaders of the most popular

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

file. size and #Uploaders denote the file size and the number of uploaders, respectively. Weight parameter of $k^{th}$ interaction of $p_i$ and $p_j$ calculated by using equation.

$W_{ij}^{k}$={((size/100MB)+(#Uploaders/$Uploader_{max}$))/2if size<100MB }

$W_{ij}^{k}$= (1+(#Uploaders/$Uploader_{max}$)/2 otherwise

Fading effect is denoted as 'f' and fading effect of $K^{th}$ interaction of $p_i$ with $p_j$ calculated by following equation.

$f_{ij}^{k}$ =k/$sh_{ij}$

Where $sh_{ij}$ is the service history between $p_i$ and $p_j$. $sh_{ij}$ evaluated using satisfaction and weight parameters of previous interaction.

The trust metric evaluation done by equation

$t_{ij}$= $1/\beta_{cb}\Sigma_{k=1}^{sh_{ij}}(S_{ij}^{k}.W_{ij}^{k}.f_{ij}^{k})$

$\beta_{cb}=\Sigma_{k=1}^{sh_{ij}}(W_{ij}^{k}.f_{ij}^{k})$ is the normalization coefficient. If all interactions completes successfully then $t_{ij}$=1. The value of $t_{ij}$ is between 0 and 1.

### Predictability Trust ($PT_i$)

Predictability trust work with self-organizing model to identify the attacks. The trust value computed by trust metric is used to find the predictability value of peers. This method is used for finding the consistency in the performance of peers. The predictability trust evaluation is done using a beta reputation system Bayesian formulation [17].

$PT_i$ =($GB_i$+1)/($GB_i$+$BB_i$+2)

where $GB_i$ is the good behaviour of peer i, ie, peer i having trust value above 0.5 and $BB_i$ is the bad behaviour of peer i, the trust value below 0.5.

**Algorithm** : For selection of service provider to download a file

1: Input : Peers with trust value zero
2: Output: Ranked peers based on trust value to download file.
3: Procedure
4: if peer i do
5: Send the query for file to download from the network
6: if number_of_ peers_ have_ file == 0
7: terminate the query process.
8: else
9: get list of all peers having the file
10: select peer based on high trust value
11: start download file from selected peer
12 :end if
13: end if
14: compute trust metric $t_{ij}$ after interaction by server
15: Update trust value $t_{ij}$
$t_{ij}$= $1/\beta_{cb}\Sigma_{k=1}^{sh_{ij}}(S_{ij}^{k}.W_{ij}^{k}.f_{ij}^{k})$
16: Store updated $t_{ij}$ on server
17: Compute $PT_i$ value using $t_{ij}$
18: if ( $PT_i$<threshold)
19: decrease reputation rank and update it.
20: else if($t_{ij}$<=0 ||$PT_i$<=0)
21: Delete the peer.
22: else
23: Increase reputation rank and update
24: end if
25: end procedure

The threshold value is assumed to 0.50 to measure behaviour for predictability trust. Peers having files with trust value in $0.75 \leq tij \leq 1$ are considered as peer having high reputation and marked in blue. Peers below the threshold value marked in red colour.

## IV. Experimental Evaluation and Performance Measure

The file sharing programme between peers implemented using language java with Net beans IDE framework. A centralized peer to peer architecture is used to implement sharing of the files. No trust value is used to upload a file. A file search request retrieves all peers having file with high reputation value. The indexed files are stored on the tracker server. The peer chose the peer having file to download with high reputation value. A file is downloaded from one uploader at a time. All peers are assumed to have anti-virus software so they can detect infected files. The major attack that have to be studied is on-off attack. Predictability trust is the method to identify on-off attack. The predictability trust calculation gives each peer a chance to recover its trust value. Trust value evaluation performed after every interaction and the trust value changed dynamically.

Performance measure of the system computed as the ratio of number of successful transaction by peers with the total number of transactions. The peers with high rank will result good performance measure. Peers with higher capabilities (network bandwidth, online period, and number of shared files) can finish more interactions successfully. Therefore, these peers have high reputation value.

### Evaluation

Transaction success rate is the metric to measure the performance and security level of a communication in file sharing. A transaction is considered successful if both of the participating peers share a file. Otherwise one or both of the peers is marked as malicious by the server. The successful transaction rate is defined as a ratio of the number of successful transactions over the total number of transactions in a certain time interval. A peer having higher transaction success rate has a higher productivity and a stronger level of security.

Success Rate = Number Of Valid Files / Total Number Of Transaction

### Analysis

The self organizing trust method evaluate the trust value of each peer. If any peer does not participate in any transaction have trust value zero. After every transaction the trust value of the peer participated in the transaction got changed. Peers are classified in to two based on the trust value evaluated by self organizing trust model as good peers and bad peers. Good peer is the peer having self organizing trust value trust value above 0.50 and bad peer having the trust value below 0.50. The experiment proceeds by repeatedly having randomly selected peers initiating transactions. A selected peer(client peer) initiates a transaction by sending query to search for a file. A number of peers that are active(online) and having the

searched file will be listed by the server. The client peer needs to select a peer from the peer candidates(Server Peer) in the list to perform the transaction. The two peers then perform the transaction and cooperate or defect according to their trustworthiness status and malicious rate. After transaction server evaluate trust value and update trust value of the server peer. Then record whether the transaction succeeds and compute the transaction success rate when the experiment proceeds.

### Simulation Design

The two trust methods are analysed to measure the performance.

First is the existing self organizing trust model and second is the self organizing trust with predictability trust. The transaction success rate with the average number of transactions of each peer has at current time is evaluated.

## Simulation Result

The graph presents observations of performance. First, see the gain of the transaction success rate in both trust models. This confirms that trust is an important feature in a P2P file sharing. As the number of transactions increases the number of valid files increases. This is because as peers interact with each other over the time, peers successfully select trustworthy peers to interact with. In some point of time some peers may become malicious and provide infected files. The SORT model does not eliminate malicious peers. Therefore, the transaction success rate becomes decreased. By using predictability trust method malicious peers are eliminated from the system. So the transaction success rate of self organizing trust with predictability trust becomes stable after the number of transactions.

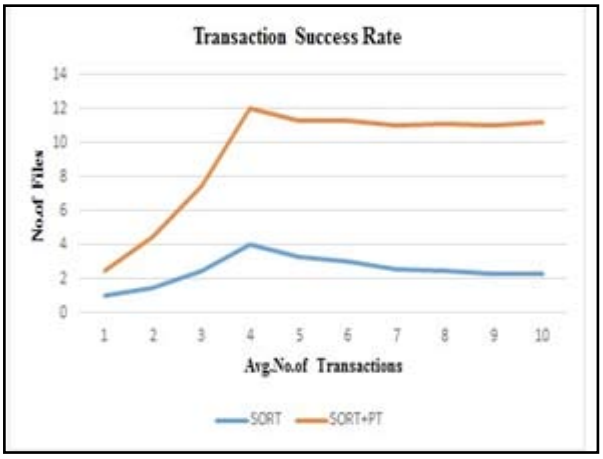


Fig. 1: Transaction Success Rate

## V. Conclusions

Peer-to-Peer systems offer many advantages for free sharing of resources between users. But these networks are more vulnerable to different types of attack. The aim of this work is to improve the security in Peer to Peer file sharing by removing the malicious users and makes the networks more secure. The trust model for peer to peer network is implemented by incorporating two types of trust model. The trust methods are not always completely capable of removing malicious users but it enhance the security. Therefore some feed back mechanisms incorporated in this method improve the performance can done as future work. Through simulation, it has been shown that this approach has good impact in reducing the percentage of unauthorized users and increasing the success rate of file sharing.

## References

[1] *K. Hoffman, D. Zage, and C. Nita-Rotaru, "A Survey of Attack and Defense Techniques for Reputation Systems," ACM Computing Surveys, vol. 42, no. 1, pp. 1:1-1:31, 2009.*

[2] *Quang Hieu Vu, Mihai Lupu,Beng Chin Ooi "Peer-to-Peer Computing Principles and Applications" , Springer 2010.*

[3] *Ahmet Burak Can, Bharat Bhargava, " SORT: A Self-Organizing Trust Model for Peer-to-Peer Systems", IEEE Transactions on Dependable and Secure Computing,vol. 10, NO. 1, Feb. 2013.*

[4] *Younghun Chae, Lisa Cingiser DiPippo,Yan Lindsay "Trust Management for Defending On-Off Attacks" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 26, NO. 4,APRIL 2015.*

[5] *BitTorrent. (2013) [Online]. Available: http://www.bittorrent.com/*

[6] *Napster home page. (2002) [Online]. Available: http://www.napster.com*

[7] *Gnutella home page. (2003) [Online]. Available: http://www.gnutella.com*

[8] *K. Aberer and Z. Despotovic," Managing Trust in a Peer-2-Peer Information System", Proc. 10th Intl Conf. Information and Knowledge Management (CIKM) 2002.*

[9] *Lee, S., Sherwood, R., et al. Cooperative peer groups in NICE. In Proceedings of the IEEE Infocom.San Francisco, USA, Apr 1-3, 2003.*

[10] *S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The (Eigentrust) Algorithm for Reputation Management in P2P Networks ",Proc. 12th World Wide Web Conf.(WWW) 2002.*

[11] *L. Xiong and L. Liu, "Peertrust: Supporting Reputation Based Trust for Peer-to-Peer Ecommerce Communities", IEEE Trans. Knowledge and Data Eng., vol. 16, no. 7,pp. 843-857 July 2004.*

[12] *R. Zhou and K. Hwang," Powertrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing",,IEEE Trans. Parallel and Distributed Systems, vol. 18, no. 4, pp. 460-473, Apr, 2007.*

[13] *R. Zhou, K. Hwang, and M. Cai, "Gossiptrust for Fast Reputation Aggregation in Peer-to-Peer Networks", IEEE Trans. Knowledge and Data Eng., vol. 20, no. 9, pp. 1282-1295, Sept. 2008.*

[14] *Behrooz Shafiee Sarjaz Maghsoud Abbaspour, "BitTorrent using a new reputation-based trust management system", Springer Science+Business Media Sept. 2012.*

[15] *C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Ad Hoc Netw., vol. 1, no. 2/3, pp. 293–315, 2003.*

[16] *P. Dhungel, X. Hei, K. W. Ross, and N. Saxena, "The pollution attack in p2p live video streaming: measurement results and defenses," in ACM SigComm Workshop on P2P streaming and IP -TV , Kyoto, Japan, Aug. 2007.*

[17] *A. Jøsang and R. Ismail, "The beta reputation system," in Proc.15th Bled Electron. Commerce Conf., 2002, pp. 41–55.*