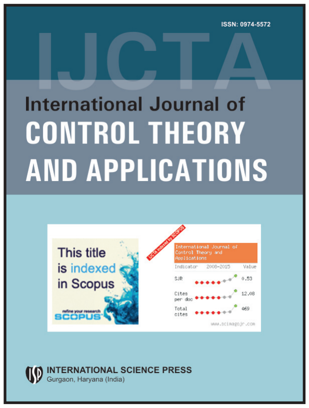

International Journal of Control Theory and Applications

ISSN : 0974-5572

© International Science Press

Volume 10 • Number 16 • 2017

P2P Trust: An Efficient and Secure File Sharing Management in P2P Networks

Vimal S[a,c] and Srivatsa S.K.[b]

[a]Research Scholar, Sathyabama University, Tamilnadu, Chennai. Email: vimalshan@gmail.com
[b]Retired Professor, MIT, Anna University, Tamilnadu, Chennai. Email: prosks@rediffmail.com
[c]Assistant Professor, Jeppiaar Engineering College, Chennai

Abstract: The present system fails to utilize the trust in the social network or it will fail in certain attacks like free riding and collision in Peer to Peer file sharing systems. To overcome this issue, a trust management system named "Social Link" is used to utilize the social network and predefined transaction links. The Social Link manages the novel weighted transactions and networks. The link is constructed using the historical file transaction. Two friends can share their files and increased trust can be guaranteed with the help of Social Link. The weighted network transaction can be used to evaluate the fairness in the transaction and to deduce the trust of client on server. By this process, Social Link will reduce transaction misbehaving, avoids free riding and promotes nodes to transact data files to non friends. Whitewashing and collision can also be rectified using Social Links.

Keywords: Reputation, File Sharing, Trustworthy, Free-Riding.

1. INTRODUCTION

The Peer-to-Peer file sharing systems are selfish or malicious because of their distributed and open environment. Without any central access control, malicious system will distribute its corrupted files without any interruption. From previous researches, it is found that 44% of files [1, 2] downloaded from the Kayak Application which has malicious code and 85% of Gnutella users are not sharing the files. This will degrade the efficiency and stability of P2P systems. Thus, we need some cooperation incentives to encourage the cooperative behaviours and to eliminate the misbehaviours that are found in P2P systems.

Trust Management system is one of the cooperation incentive method used in P2P systems in these recent years. This is implemented in online market platforms to compute global trust nature for each and every user with the help of collected ratings. Whenever a client requests a service, it will raise queries in trusted system to get trusted values of corresponding servers and will select the server that holds highest reputation. The nodes with lower values than a required threshold will be considered as untrustworthy and its corresponding requests are rejected. The systems will suffer from attacks like Sybil attack, Collision and Whitewashing. A free rider will maintain its reputation which is slightly higher than the required threshold to receive files without sharing the files with others. In Whitewashing, a low reputed node will abandon its account and will create a new account with initial reputation to receive its services. Sybil nodes will give good feedbacks to many nodes in order to increase its reputation. These boosted reputations will result in malicious behaviours.

Recently, many methods are proposed to have trusty P2P system with the help of Social network properties. In these systems, node will seek services from its friends as social friends are more trustworthy. As a result of fewer members in social network, client will not be able to find the file from its friend which will lead to limited file availability. Therefore, this social network must be complemented by reputation system to achieve global availability of files. At the same time, a mechanism is also required to prevent attacks in normal system. Social Link, a social network is based on a trust management system that allows a node to receive reliable file services and will resist all attacks.

2. FILE SHARING

1. *Between Non-Friends Node:* Social Link will maintain a weighted transaction network. Whenever a server N_i provides a file to its client N_j for the first time, a new link between the nodes N_i and N_j will be created along with weight that is equal to the file size. For example, if weight of link $N_i \rightarrow N_j$ is W_1 and $N_j \rightarrow N_i$ is W_2, then it is understood that N_i has the trust [3] and permission to provide file with size W_1 to N_j and similarly N_j has to provide file of size W_2 to N_i. This type of information is used to ensure fairness and reliability of files.

   Since non-friends are connected by a path that has a number of links, we can define the link weight of path as a minimum link weight which will show the path's trust. For a client and identified server, its trust is known to be maximal one among the weights of all paths and their upload-flow is maximal among all client-server paths. Also, Social Link needs trust flow which is larger than the requested size in order to avoid faults. The free-riding is avoided only when the difference between upload and trust-flow is within a reasonable range.

2. *Between Friends:* Social network has reliable users – frequently contacted nodes and real world friends to maintain a serial link. For a given number of servers, a user will choose friends directly if they are trustworthy. So, the file sharing will be efficient. This will discourage selfish behaviours and the file will be continuously cooperative because 1) User may have more online friends for many resources and 2) People do not want to destroy the real life reputation among their friends.

   In addition to this, Social Link will avoid Sybil attack, Collision to a certain degree. Whenever a new account is created by whitewasher, file transfer from non-friends are prevented. So, whitewash will not allow free-riding. Though Collider boosts its own trust, it would require actual transaction with other nodes than its friends to build a link and receive files.

3. RELATED WORK

1. *Social Network Based P2P File Sharing System:* Many properties like "Friendship faster cooperation", "Online social networks reflect those in offline world" and "Average network properties will be stable relatively" are exploited in order to have reliable services in P2P network.

   This will construct an overlay on pre-existing trust relation between users to have secure and private sharing of sensitive data with "friend-to-friend" file exchange method. Tripler extension of Bit Torrent will use social phenomena and existence of communities with same taste to increase performance and usability. My Net in P2P will allow participating user to use and share their server and resources safely without contacting any central control. Social-Helpers will use social network for node trust evaluation. Social P2P will collect common nodes and form a cluster to connect socially close nodes within clusters. Social-Trust will use social network for trust management. Barter cast will discover each node's local trust graph and max flow algorithm to detect free-riders.

2. *Reputation Management System:* P2P system is mainly based on Reputation Management Systems. Eigen Trust will minimize the influence of malicious nodes. This is calculated by global reputation of a node in the system which will be treated as the left principal eigenvector of a matrix of normalized local values. Similarly Power Trust will use a trust overlay model for managing trust relation among the nodes. Then it will find few highly reputed "Power Nodes" in order to increase the global reputation accuracy and aggregation speed. These are all based on discovered power-law distribution in users. The distributed trust management is based on past behaviour of peer that is reflected by its digital reputation with the help of cryptographic protocol. Peers can either download or upload files but one at a time. Thus each node will earn a value whenever it uploads a file to others and at the same time, server will consider client's trust value in order to find whether it can satisfy client's request. Thus all the nodes in the system are encouraged to contribute a network link for uploading. Belief Reputation (BP) P2P system will select a factor graph that appropriately represent the P2P system in order to evaluate trust and to find the trustworthiness of the nodes.

4. DESIGNING A SYSTEM

The Social Link will provide trusty and effective P2P file sharing and also resists attacks. Social Link has two main components: A weighted transaction network and a social network that is based on server selection. The social network will include trustable online friends and real world social acquaintances to share files whenever a client wants to select a server from server candidates. It will select its friend from the network if they are available. Whenever there is no friend in server candidates, then the Social Link relies on weighted transaction network to find whether the transaction is fair and trustable for all servers.

1. Social Network Based Server Selection

Whenever a user is online, then it includes off line and online connection. Similarly, friends in Social Link also include trustworthy online and offline acquaintances to share files with nodes frequently. Whenever a new node wants to join the system, it is possible only for trustable nodes to get added and will not consider whether the node is offline or online. Hence insertion and removal of nodes in Social Link is user dependent and user is the person who is responsible for this activity.

I. *Construction of Social Network:* Every user will create and maintain friends. When a node N_i wants to add another node N_j into its friends circle, then it will send an invitation to N_j. Once the invitation reaches N_j, it will decide whether it should accept the invitation or not. The Social Link has bi-directional relationship (i.e.) whenever N_i deletes N_j from its circle, then N_i will be automatically removed from N_j. When a node joins the system, it will add only its offline acquaintances as its friends. After some time, the node will add online friends after conducting enough file transaction with others.

For example, when a node N_i has successfully downloaded a file from node N_j, if there is a link between, then its weight W_{ji} will be updated based on the size of shared files and ratings from N_i. If there is no link between the nodes, a new weighted link between N_i and N_j is established. When both

W_{ji} and W_{ij} reach a predefined threshold T_1, Social Link will notify N_i and N_j that they are friend of each other. Only when both of them agree to insert other node as a friend, friendship relation is established among them.

The friendship relation will represent certain level of trustworthiness. Real life friend will offer high QoS to all nodes. Also users do not want to damage their trust in their communities. Thus real life friendship network will be cooperative continuously. Also, frequently interacted nodes will also have probabilities to have high QoS in order to have previous behaviours. Thus, to maintain friendship which is a reflection of trust value, the node would have to reduce the QoS.

II. *Selecting a Server:* In order to identify fast server selection, Social Link exploits friends to reduce reputation queering cost. Usually, whenever a request to a file is issued, a client will ask from its friends. Thus, efficiency of sharing is increased by saving the query cost. Whenever a client wants to download, it will find servers based on P2P file sharing techniques and algorithms. Then, client will verify whether there are any friends in its server list. If friends are present, the node will select a friend as server for the file without any queries. If multiple friends are present in the list, then the friend with highest reputation is chosen. If there are no friends available, node will use weighted transaction network in order to select a server. After this file transaction, client will send feedback to the system for updating the link weight.

2. P2P Service Centre

We will consider a trusted P2P service in the network will offer P2P file sharing service with the give Social Link. It will have normal P2P file sharing methods and it will assume Social Link as trust Management module. First the nodes want to register at service centre to participate in P2P file sharing. Whenever a node requests a file, they will send its request to service centre. Then the centre will return the list of available servers. Once the transaction is done, the nodes will send a feedback to the service centre in order to update the transaction weight of the network.

3. File Sharing Process in Social Link

Whenever a client requests a file, if there are friends in its server list, then the client will directly ask the file from its friend. Else the weighted [4, 6] transaction network is used in order to find whether the transaction should be executed and which server to be selected.

First it should recall that weight of link $N_i \rightarrow N_j$ to represent size of the file that N_j can trustingly obtain from N_i which is based on previous record. This also provides us that N_j should upload files with size no smaller than this weight to N_i for trading and free-riding prevention.

Two nodes can be connected by a number of links which will form a path in $N_i \rightarrow N_j$. We will represent the smallest link weight in the all link on path as weight of the path. This will represent the trust of N_j and N_i in proving file which is based on the trust transited along this path. There will be multiple paths which will connect N_i and N_j. The *trust-flow* network is defined as the largest path weight among all paths from the server N_i to the client N_j. It will represent the client node's reputation on the server to provide files within size W_{ij}. The *upload-flow* is defined as the largest path weight among all the weights of paths from client to server. It will represent an accumulated size of files that each server N_i should provide to client N_j for fair trading. Then the trust-flow is used to find whether server is trustable to provide the requested file and also the difference between trust and upload flow is used to ensure the fairness of the transaction. The "six degree of separation" property will indicate that two people are connected by maximum of six steps on average. Hence we limit server-client and client-path length as 6 hops in weighted transaction network.

For example, if a node N_i request a file with size S and if server candidate list includes ‘k’ servers N_{S1}, N_{S2}… N_{SK} and not one of server is N_i’s friend, then sharing follows.

- Social Link can calculate client’s upload flow for each server which is denoted as UF_{im} and each server’s trust-flow to client is denoted as TF_{mi} where M ε [I,k]
- In order to verify fairness, only the servers with $(UF_{im}-TF_{mi})>= S$ or $|UF_{im} - Tf_{mi}| <=Th_r$, will provide files to Ni, Thr is fairness threshold.
- The first condition will tell us that the server owes more than the size of the requested file to the client in order to make the trading pair.
- The second condition means a gap on mutual contribution on roughly equal status. This will tell us that transaction is allowed between two nodes and only these servers are allowed in server list.
- For required file sharing, the server with trust-flow smaller than required file’s size ‘S’ are removed from the list because they are not trustworthy to provide the file.
- A last the client will select a server with the highest trust-flow for transaction as it is most trustful.

Thus by this processing step, Social Link will ensure that server will have high probability to provide requested file. Also the client is not a free-rider. There is also possibility for a chance that server candidate might be empty after first step. To have broad file sharing, Social Link will return several servers with TF_{mi} and high $(UF_{im} - Tf_{mi})$ or low $|UF_{im} - Tf_{mi}|$ as a backup, because these servers are very close in order to satisfy requirement of server and these are assumed to be very trustworthy. Client will also consider other factors like common file interest, [10] third party reputation system, and social connection strength in order to evaluate whether the transaction can be conducted with any one of these servers.

4. Weighted Transaction Network

We know that Social Link [11] is representation of trust and this will allow friends to share files but however node can have only limited friends. Thus solely relying on friendship for file sharing will limit the availability of file resources. Hence it is important to provide trusted information for non-friends in order to have trustable file sharing service. Also, fairness of file sharing is important to avoid free-riders.

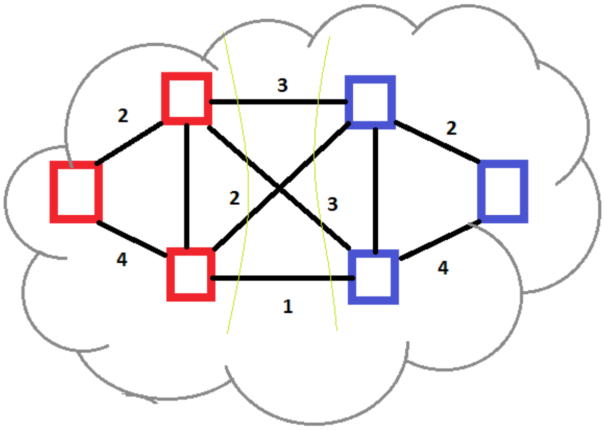

Figure 1: Weighted transaction network in Social Link

To have these objectives, the Social Link will build a weighted transaction network based on past record between node transactions. The nodes are connected by weighted directional link. When the system is started, the trust information among nodes cannot be evaluated, as there is no transaction among them. The friendship relation will represent certain reputation among friends, the weighted transaction network is initialized with weight Δ_w that connects each pair of friends in both directions. There will be default link weight to allow non-friends to satisfy requirements of file sharing at the beginning stage of system. Thus to participate in Social Link, a node should have friendships. Else it has no other chances for file sharing and also it will be isolated from the network Δ_w is set to mid value to have bootstrap of the network. Also Social Link will allow downloading large files from many servers to ensure that in bootstrap stage, large files can be downloaded.

Since many transactions occur, weighted links will be constructed between non-friends also. When a node N_i successfully provide to N_j, weights on path are used to decide fairness and reputation of transaction, according to file size and ratings on file quality. Also, when there is no link between N_i and N_j, then a new link will be built from N_i to N_j with weight that is equal to file size. The link weight means size of file that node N_j obtained from non-friend N_i with trust.

5. Meaning of the Link Weight

The weight of link between two non-friends is denoted as L_{ij} for the link between N_i and N_j, means servers as N_j's trust on N_i's to have file sharing. Also, these two nodes are always not connected. They will have multiple link trust relaying used to calculate the reputation on file providing ability.

For example, there is path with 3 links. $N_a \rightarrow N_b \rightarrow N_c \rightarrow N_d$ and their weights are $W_{ab} = 5$, $W_{bc} = 3$, $W_{cd} = 7$. Here N_b will recommend N_c that N_a's file providing ability is W_{ab}. Since node's recommendation should limited by its reputation, we use smaller one of its trust.As its effective and efficient recommendation. Thus, N_e 's trust on N_a file providing ability is $W_{bc} < 3$ since $W_{bc} < W_{ab}$. Also $W_{cd} > W_{bc}$, N_d's trust on N_a's file providing ability is still $W_{bc} = 3$.

First, when N_i provides file to N_j for first time, L_{ij} is initialized with weight which is equal to the size of shared file. Second, when path include L_{ij}, it has been used in order to represent the reputation, weight of L_{ij} updating depends on the transaction rating.

With this design, weight of link can be changed between nodes. Thus as a result malicious nodes can lower their weights to decrease weights of some paths or to disconnect the node then the decrease of weights of links reflect the true situation which means that recommendation is very low. The probabilities that malicious node are selected as server are decreased, this will give benefits for file sharing system.

6. Computing and Communication Complexity

P2P service centre has a single trust manager to decide paths from a client to serve in weighted transaction networks. For each and every file request, communication overhead is O(1) between client and P2P service centre. To decide the paths from client to file server, Social Link depends on breadth first search solution. Thus, complexity is O(m+n) where m and n are the number of edges and nodes in weighted transaction network.

7. Link Weight Update

Link weight is not updated after transaction between two friends because link weight is used to provide an evaluation for reputation among non-friends, and node's QoS to its friend cannot reflect its QoS to non-friend. Thus, updating of link weight age between two friends will lead to evaluate trust between non-friends.

For example, two friends will always provide good services and feedbacks to each other and bad services to non-friends in extreme case.

If the transactions between nodes are considered in calculating upload flow and trust flow, it will lead to misleading of reputation of nodes.

The link weight is updated only after transaction between non-friends. Based on ratings Social Link update link weights as follows

- *Positive feedback:* Whenever client receives satisfactory file, then it will give positive feedback. Then weight of each link for the trust flow is added by the file size. If server and client are not connected directly, ten a new link between tem will be established wit its weight equal to size of the file
- *Neutral or No feedback:* If a client report neutral feedback, then social link will not update link weight age.

  The neutral feedback will tell us that file from server is not faulty, but client may not be completely satisfied with file. Also, it is not necessary to furnish the server and client may want to keep the link to server for future.
- *Negative feedback:* Whenever the non-malicious client provides a negative feedback for faulty files, social link will lower the weight of each link to find the trust flow. The link which has weights smaller than 0 are removed.

While designing, we also fade out weight links over time and we can set a limit for link weight for practical consideration. First, weight of a link is faded with a factor β e [0.5,1] for every Td. This fading factor will make the recent behaviours more important to deice nodes reputation. The values for β and Td should be found by the factor that how active nodes are in the system. Generally β and T_d are set to large value like 0.95 and 1 day, respectively in order to avoid disconnecting the network. Further, for practice, we set maximal weight for a link to avoid overflow, which is set as maximal value to represent link weight variable in the original system.

This design will encourage both server and client to be co-operative. Whenever a node receives negative feedback frequently, all its link to another node will be removed and it will have few opportunities to obtain files from others. As a result, servers are encouraged to have high QoS. Then, when client provides negative feedback, the weight of path from high QoS server to the node will be reduced. Then high QoS server cannot be differentiated from others, this may avoid client form finding reputed serves in future. On another side, when client issues positive feedback it will enhance the reputation of misbehaving sever. This means that it is likely to receive low quality files again.

8. Attack Resistance and its Extensions

Social Link works under several malicious behaviours and possible extensions to better avoidance against attacks.

- *Free-riding:* The fairness during transaction of file will avoid free-riding in Social Link. A server is willing to provide a idle to client whenever there is difference between trust flow and upload-flow satisfies either $(UF_{im} - TF_{mi}) \geq S$ or $|\ UF_{im} - TF_{mi}| \leq Th_r$, which means that client node has at least S more files than server has provided or server and client has provided similar amount of files to each other.
- *White washing:* This can't enable malicious node to proceed in providing faulty files in social Link. First, a link is created in weighted transaction network after successful transaction whenever white-

washer creates a new account, it only has link to friends. Then it can rely on friend's link to other nodes that is to be selected by non-friends as the file server. White washer can have normal friends unless they are colluding. As a result, without link whitewasher will not be selected by non-friends as server. Also, whitewasher can download files only with the help of friend's link. As a result, they can continuously free ride due to same reason.

5. PERFORMANCE EVALUATION

We have conducted extensive simulation to find the performance of Social Link in detecting malicious transaction preventing malicious behaviours and in saving querying cost in different network we randomly select a medium social network with 5000 nodes from a Live-Journal, is a social network trace in order to build their mutual friendship in our simulation. The three types of nodes are good, bad and neutral. In order to avoid bias we select bad nodes among all nodes. Because of small scale of number of nodes, to avoid weighted transaction network disconnection, we select 10% nodes a bad node, these node will have low quality files and will provide dishonest feedbacks. Thus, we randomly select 70% and 20% as good and neutral nodes, respectively. These good and neutral nodes provide high quality and medium quality files respectively and will give honest feedback we simulate one single trusted manager to store and respond to request. Also centralized manager will have sufficient storage and computing capacity to serve all requests.

To measure performance in social network from the trace, random distributions for all parameters are assumed. We configured 1,000 files with sizes from [1.100] MB. Each file has 'n' replicas where n is chosen from [1.5]. The quality of files by levels are selected from range [1,10] to differentiate different types of files. Good files will have quality range [7, 10], neutral files will have quality level range [4, 6] ad bad files will have [1, 3]. File holder is selected from good, neutral and bad ones for high, medium ad low quality, respectively. In our explanation, when size of P2P file is increased by m times, the number of files is also enlarged by m times with same percent of good, neutral and bad nodes. We set T_f to be largest file size in order to make sure that there is at least one file that can be shared between server and client at the starting itself. We also set to T_f as two times of the largest file size because the strangers become friends after sharing 4 files on average.

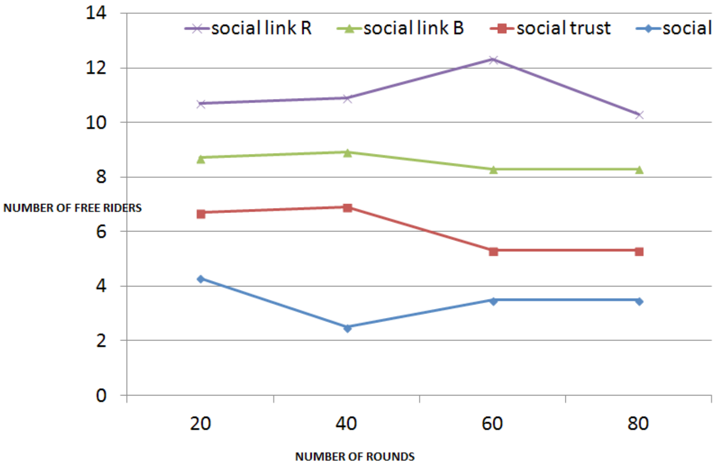

Figure 2: Accumulated No. of free riders

In this process, friendship threshold is set to 200. We execute experiment for 100 consecutive rounds. In each and every round, every node generates a file request. The requested files of node are selected from the files which are not owned by that node. Different feedbacks are given to server based on the type of client and the quality of received file. This node can share its received files with other nodes.

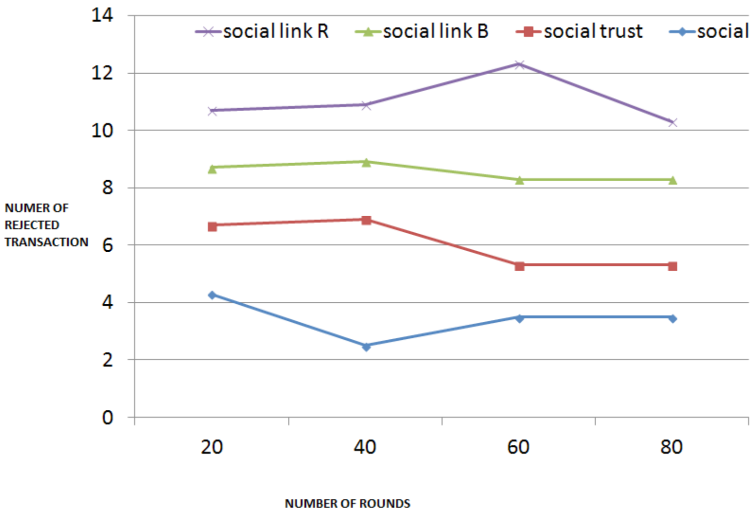

Figure 3: Accumulated No. of rejected transaction

Social Link is compared with a reputation system which is based on a social trust denoted as social, in which each node is defined as the maximum path length in order to find requested files. We also compare Social Link with Social Trust which is also a social network that is based on trust management system. In Social Trust, trust value is initialized to 0 for each node and increased or decreased by 1 for each positive and negative feedback respectively. Thus Social network is built on interaction in Social Trust to facilitate server selection. The threshold is set to 0 by default. We know in Social Link that suspicious transactions are blocked. In this case, we use Social Link-B and Social Link-R to denote Social Link with these two strategies.

1. Free-Riding Prevention

In free-riding nodes are tend to reject requests but download freely from non-friend nodes. Here, we assume that 20% of 5000 riders are free riders in the system that has 50% probability to reject file requests. We observe that *Social Link-B* < *Social Link-R* < *Social Trust* because free-riders do not contribute to downloading. Thus, transactions are blocked for not finding a reliable path from free rider to server with $(UF_{im} – Tf_{mi})>=S$ or $|UF_{im}-TF_{mi}|<=Th_r$. On the other side, Social Trust was unable to prevent all free-riders with high trusted values from downloading from non-friend. Social Link-R will check the path between nodes in weighted transaction network. This will manage all suspicious transaction from querying the trusted values of available servers. As a result, some free-riders still request files when they have high trusted values. Therefore, it generates fewer downloads from free-riders than Social Trust and more rejected transactions than Social Link-B. Social has the most downloads from free-riders as it does not use trust to distinguish malicious nodes with social relationship.

The result that follows is *Social Link-B* < *Social Link-R* < *Social Trust* < *Social*. Thus, accumulated number of rejected transactions will not increase in the subsequent rounds in Social Link-B.

2. Accuracy in Detecting Suspicious Transactions

We calculate that number of total suspicious transaction and the number of falsely marked transaction in each round. We mention the falsely marked suspicious transaction as false negative and falsely marked normal transaction as false positive. Hence the percentage of falsely marked suspicious transaction is a method to measure the accuracy of Social Link-B in detecting fraudulent transactions.

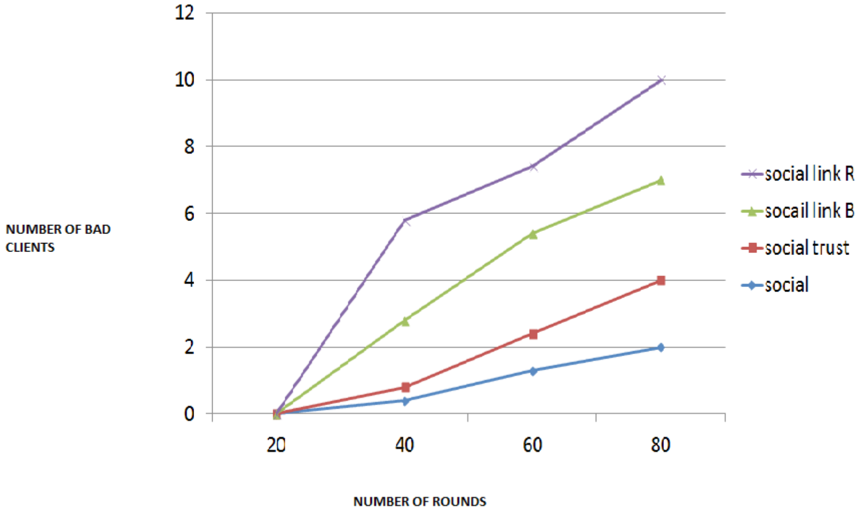

Figure 4: Accumulated No. of bad clients

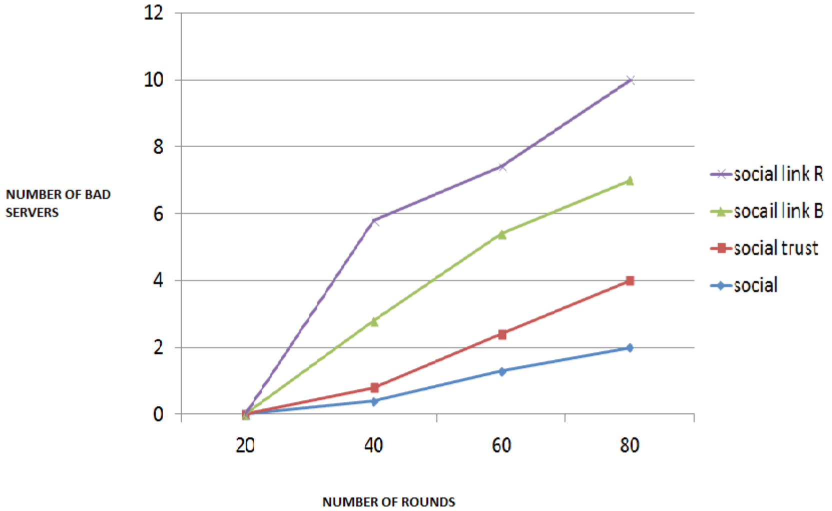

Figure 5: Accumulated No. of bad servers

The path of friend-of-friend connection may be used to select bad node as servers. High percentages of servers are detected as suspicious and there are 91.1% chances for false negative and positive transactions. After directional weighted links are generated between nodes as number of transaction increased, number of suspicious transactions decrease rapidly.

3. Sybil Attacks and Resisting Collision:

Here all the bad nodes colluded with their colluding nodes or Sybil's are identified a long time before first round to measure the damage of these threats. With this, each bad node in Social Link-B, Social Trust, Social Link-R and Social conducts 100 transactions with selected colluders and receives all positive feedbacks. Though nodes collude in the same way in all the systems, results of collision are different. Bad nodes in Social Link build links with expected weight value as 5000 as the expected file size as 50, but they will still have no links to non-friend nodes since no transactions happened between non-friends. On the other side, bad nodes in Social Trust will enhance their trust to 100 before first round.

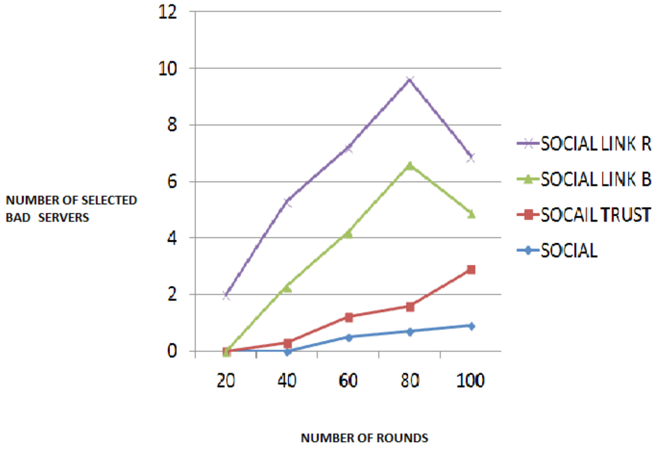

Figure 6: No. of bad servers

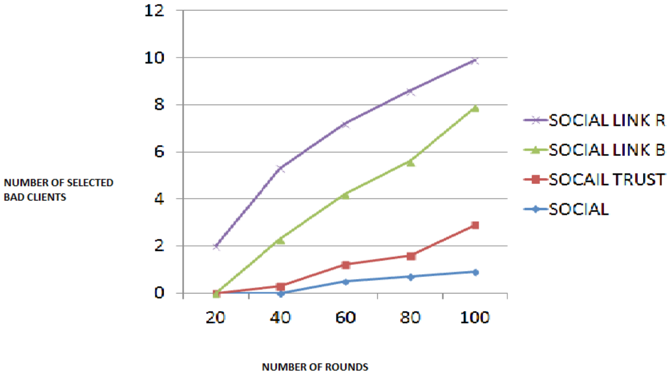

Figure 7: No. of bad clients

We found that result follows as Social Link-B < Social Link-R < Social Trust < Social in all rounds. In Social Link-B, malicious nodes community will be blocked entirely by others since the weights of links connecting colluders reduces by sending bad files to others. Thus, smallest numbers of transactions with bad nodes are generated. On the other hand, Social Trust can differentiate bad nodes and this will stop selecting them as servers. However, colluders can make conclusion again to defeat Social Trust. Instead of blocking suspicious transactions, Social Link-R uses trust values by colluding.

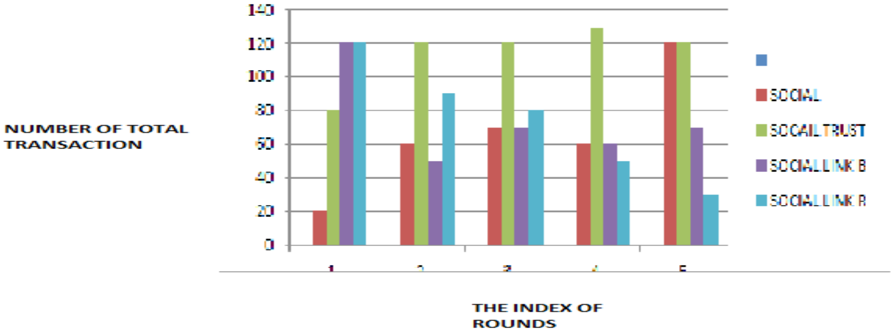

Figure 8: No. of total transaction

Accumulated number of bad servers in Social Link-R is more than Social Link-B and less than Social Trust. As a result, Social Link-R selects fewer bad nodes as servers depending on weighted transaction network. Social selected largest number of bad servers as it cannot differentiate bad nodes by only trusting social closeness within 2 hops. The accumulated number of selected bad client will follow Social Link-B < Social Link-R < Social Trust.

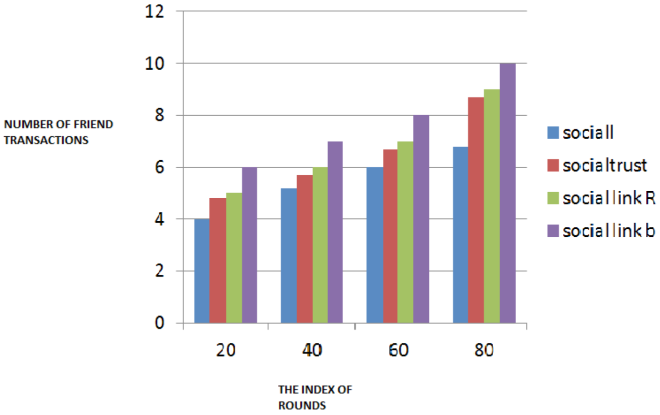

Figure 9: No. of friend transaction

4. Reducing the Adverse Effect of Whitewash

This will show how the Social Link reduces adverse effect of Whitewash. In each round, 50% of malicious nodes will delete their current accounts. By Whitewashing, they will remove low trusted values and will restore their reputed values to initial value 0. The number of selected bad servers and client will refer to the number of transactions that take bad nodes as servers and clients respectively.

The accumulated number of selected bad servers of all system follow Social Link-B<Social Link-R<Social Trust<Social. Social will select largest number of bad servers. Social trust will prevent malicious behaviour of bad servers but with whitewash, malicious nodes clean their low trust values and are selected as server in subsequent rounds again. Thus, it will select fewer bad servers than Social. However, Social Link-B will remove all links of node when account of node is deleted. Social Link-R will conduct suspicious transaction with reputed values so that bad nodes are selected as servers with reputed values that are not accurate. Then, in weighted transaction network only small numbers of bad nodes are selected as servers. Social Link has the capacity to avoid the malicious servers from whitewash in a better way than other methods.

6. CONCLUSION

In this paper, we propose a social network transaction based on trust management system called Social Link to have efficient reputation management in P2P file sharing systems. Social Link will exploit social network to allow friends to share file directly. To have fie sharing among non-friends, Social Link will design a novel weighted transaction network to manage trust among non-friends depending on transaction records in which link weight from one node to another node will denote the file size. This kind of design will avoid collision, Sybil attack and whitewashing as malicious nodes cannot interact with other links. Finally, extensive real trace base experiment will demonstrate efficiency and effectiveness of Social Network.

REFERENCES

[1] S. Shin, J. Jung, and H. Balakrishnan, “Malware prevalence in the kazaa file-sharing network.” in Proc. of IMC, 2006.

[2] S. Kamvar, M. Schlosser, and H. Garcia-Molina, “The EigenTrust algorithm for reputation management in P2P networks,” in Proc. of WWW, 2003.

[3] R. Zhou and K. Hwang, "PowerTrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing," IEEE TPDS, 2007.

[4] R. Zhou, K. Huang, and M. Cai, "GossipTrust for Fast Reputation Aggregation in Peer-To-Peer Networks," IEEE TKDE, 2008.

[5] J. A. Pouwelse, P. Garbacki, J. Wang, A. Bakker, J. Yang, A. Iosup, D. H. J. Epema, M. Reinders, M. van Steen, and H. J. Sips, "Tribler: A social-based peer-to-peer system," in Proc. of IPTPS, 2006.

[6] J. Li and F. Dabek, "F2F: Reliable Storage in Open Networks," in Proc. of IPTPS, 2006.

[7] D. N. Kalofonos, Z. Antonious, F. D. Reynolds, M. Van-Kleek, J. Strauss, and P. Wisner, "MyNet: A Platform For Secure P2P Personal And Social Networking Services," in Proc. of PerCom, 2008.

[8] P. Mittal, M. Caesar, and N. Borisov, "X-Vine: Secure and pseudonymous routing using social networks," CoRR, 2011.

[9] M. S. Artigas and B. Herrera, "SocialHelpers: Introducing social trust to ameliorate churn in P2P reputation systems." in Proc. of Peer-to-Peer Computing, 2011.

[10] Z. Li and H. Shen, "Social-P2P: Social network-based P2P file sharing system," in Proc. of Network Protocols (ICNP), 2012.

[11] K. Chen, H. Shen, K. Sapra, and G. Liu, "A social network integrated reputation system for cooperative P2P file sharing," IEEE TPDS, 2015.

[12] M. Meulpolder, J. A. Pouwelse, D. H. Epema, and H. J. Sips, "Bartercast: A practical approach to prevent lazy freeriding in p2p networks," in Proc. of IPDPS. IEEE, 2009, pp. 1–8.

[13] E. Pennisi, "How did Cooperative Behavior Evolve?" Science, 2005.