Trusted Server to minimize Sybil Attack

ChinkyAggarwal,Email-rashigarg04@gmail.com
SRCEM, Palwal, Haryana

Abstract— Sybil attack is one of the most challenging problems in Peer-to-Peer networks. The huge number of fake identities created by malicious users may attempt to gain a large influence on the network Using identity management scheme the Sybil behavior of a node can be identified, and those suspected as Sybil are limited from inviting others. Moreover nodes may contact one another for file sharing and super nodes calculate rank matrix and uses these values also for assignment of new identities. Although false positives and false negatives may occur in the labeling process, we have to minimize it as far possible. In future, the efficiency can be increased by considering more parameters for labeling a node as Sybil or genuine.

Trusted Server can be used for backup .It acts like repository which contains information about each node. If any node is detected as Sybil then we can remove that node and maintain the hierarchy using trusted server because trusted server knows which node will be link to which node. We can check behavior of nodes to determine it is Sybil node or Genuine Node..

KEYWORDS- Trusted Server ,Final Rank ,Direct Rank ,Indirect Rank

I. INTRODUCTION

A Peer-to-Peer Network is a distributed network composed of a large number of distributed, heterogeneous, & independent peers.

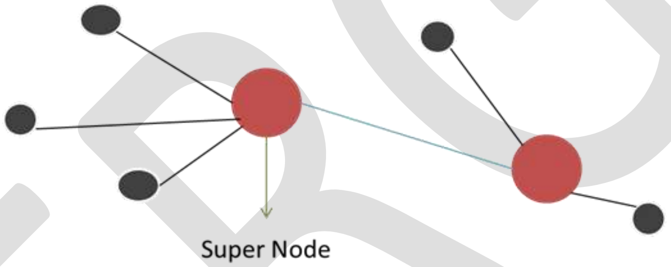


Figure 1. Peer-to-Peer network

P2P networks provide an alternative to the traditional client-server communication model in which a node in a P2P network can act as a server and a client at the same time. The P2P computing provides properties like no central point of failure and no service bottlenecks by decentralizing the service among participating nodes. In recent years many research work have been done and are still in progress to improve their robustness, security and scalability. P2P networks are less secure than a client-server network because of their decentralized nature.

P2P specific security problems include targeted denial of
service attacks, forgery, pollution attack, Sybil attack, attacks on routing queries and attacks on data integrity.
For efficient routing and load balancing in P2P networks,
every node should have a unique identifier and there should be

an identity management scheme for handling identities in distributed environment. The term identity refers to information about an entity that is sufficient to identify that entity in a specific context and any entity, either in the digital world or in real world, is associated with an identity. Identity management plays a crucial role in operational efficiency, management control and cost savings. Systems need to manage the growing number of users, their dynamicity, their access to information and applications scattered across heterogeneous systems.

Identity management includes three major aspects:
acquisition of identities, authentication, and authorization.
Authentication is the process that verifies the association between an entity and the corresponding identity. Different authentication mechanisms have been widely used like password checking, challenge and response and biometric verification. Authorization grants the permission to an authenticated identity for accessing resources that it is eligible for (example, by using Access Control List).
In P2P networks, the issues related to identity
management may fall in the areas like secure assignment of
node identities, entity-identity association, distributed trust among and damage discovery. Distributed environment works on the usual assumption that each participating entity controls exactly one identity. When this assumption is non-verifiable, the system is subject to a condition in which an individual entity generates huge number of fake identities. This problem, named as Sybil attack refers to a

situation in which individual malicious users may join the network multiple times under multiple fake identities and these fraudulent ones may try to inflate their own reputation in the network to appear more trustworthy than they really are and the integrity or the availability of the P2P network may be disrupted. This attack usually happens when obtaining a new identity is not expensive. Sybil identities can easily overcome the genuine users in various collaborative tasks, recommendation systems, redundant/false routing and data replication in DHTs.

Sybil defenses aim at limiting the number of Sybil identities, but false positives and false negatives are acceptable to an extent in this process. Complete elimination of false negatives (assigning Sybil identity as genuine) are not necessary since the distributed system should be able to tolerate some fraction of byzantine identities, otherwise, even without Sybil attack it is not robust. Thus, a sybil defense should be able to limit the total number of false negatives below the tolerance threshold of the system. Most of the applications can easily tolerate with a small fraction of false positives (labeling genuine nodes as sybil). For example, in a P2P backup system, if a node considers another one as sybil, then it will not trust that node for storing its data. A false positive rate of 20% means that, the given node will still trust 80% of the genuine nodes, and can use these. Also, if it is a recommendation system, then it can use votes from 80% of the genuine identities. From these observations, we can conclude that defenses against sybil attack permits some bounded fraction of false positives and false negatives also. In this paper, we propose a sybil defense based on invitations and systematic distribution of identities. Initially, each peer assigns a set of identities to peers invited by them and later based on how they utilized the earlier ones. As the network grows, the super nodes occasionally computes the rank matrix based on the transaction between peers and considers these referral values also, for assignment of new set identities when nodes request more.

II. RELATED WORK

In the absence of a centralized authority concurrently certifying all identities, a possibility of sybil attack always exists and it was first proposed by J. Douceur. Many papers suggest certification as a solution to the sybil attack, and it is the most common solution. But trusted certification usually depends upon a centralized entity which ensures that each entity is associated with exactly one identity.

Resource testing is another approach to defend sybil attack in which it tries to check whether a number of identities possess fewer resources than would be expected if they were independent. These checks include tests for processing power, memory capacity, network bandwidth etc. This can be considered as a minimal sybil defense, but for many applications it is not sufficient if an attacker is able to obtain large number of identities for a successful attack, even if it is expensive. Another approach is to impose a fees (one time cost) for obtaining an identity. However, here the issue is how to put a limit on fees such that it must be low enough to allow everyone to join, but also be high enough to prevent malicious users from obtaining many identities. Recently, many mechanisms leverage social networks for limiting sybil attack. A social network refers to an undirected graph where vertices of the graph correspond to nodes/identities and edges correspond to human established trust relations between users. Social network based schemes work on the assumption that, even if a malicious user creates a large number of sybil identities, it can establish only very few edges with genuine nodes. So, the network can be divided into sybil region and non-sybil region by computing the minimum cut along the graph. The main drawback is that these techniques depend on the limited availability of real world friendship edges between nodes and P2P application in use may have only little intersection with this. Similarly, these friendship relationships are difficult to construct as it requires out of band communication.

There are many other sybil defenses which do not leverage social networks such as sybil defense mechanism based on network coordinates , in which the scheme offers guarantee under certain assumptions on the network position of the attacker. Dsybil uses user feedbacks to defend against sybil attacks in recommendation systems. Another approach is a referral system based on multiplicative reputation chains in which it shows how a reputation system with chain referrals adds referrals from different referral paths/chains, is sybil-proof. In an existing member has to invite another user for obtaining an identity in the network. This method is based on the construction of a perfect tree representing social relationship between users. The top of the tree consists of founding members which emulate root node by sharing private key of the root through threshold cryptography. The invitations are delivered based on the value of a factor parameter which is calculated by each node based on their local policies. Here the of a node corresponds to number of to maximum attainable weight. The algorithm tries to construct a perfect tree in which, for each child, weight is equal to the potential and for each parent their children have a potential corresponding to the factor parameter. The performance depends on proper selection of value of the factor parameter.

III. PROPOSED TRUSTED SERVER MODEL

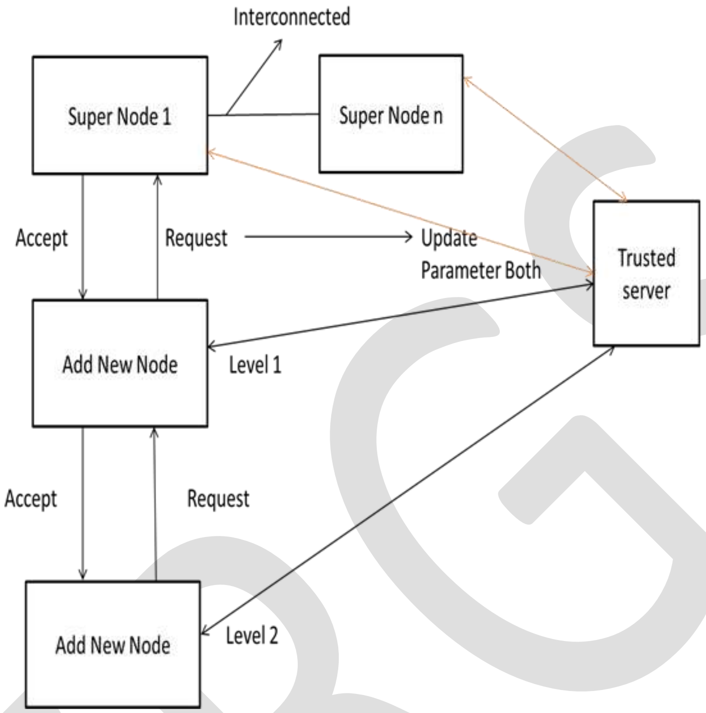


Figure 2. Peer-to-Peer network with Trusted Server

Trusted Server contains backup of each node of network.
In this paper we are proposing an approach to minimize Sybil attack using trusted server.

Step 1: Initially few prerequisite peers with sufficient CPU, Memory and Network Bandwidth are assigned as Super Peer nodes by the service provider. Every Super Peer is assumed to have a Set of Identities.
Step 2 : Now we introduced a Trusted Server who will maintain a details of each member s of network.
Step 3 : When any new node want to join the network then already exist member super node or normal peer invite them to
assign a Unique Identifier and set of identities(N) for inviting others. Limit the invitations count by giving only (N/1+log2 N) th fraction. It is around N/10.
Step 4 : When a node has no more invitations to deliver, the node requests to its parent . If parent has unused invitations

then the parent gives invitation from that to its child. If the parent does not have unused invitations, the node asks its parent, and it continuous until it reaches to the Super Peer Node.

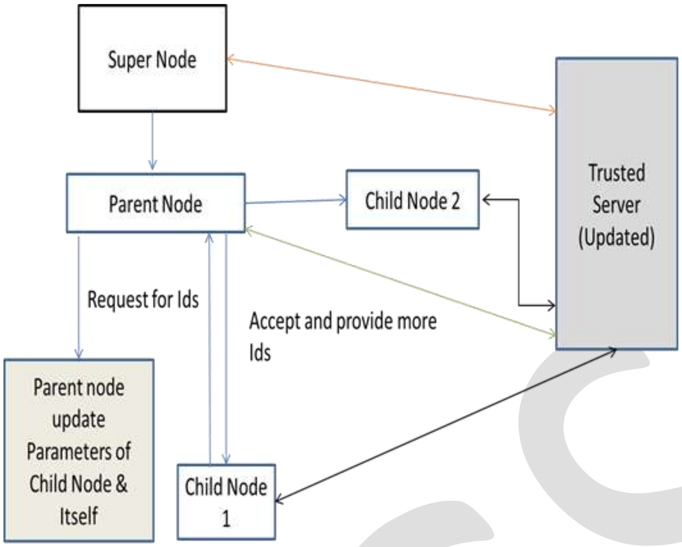
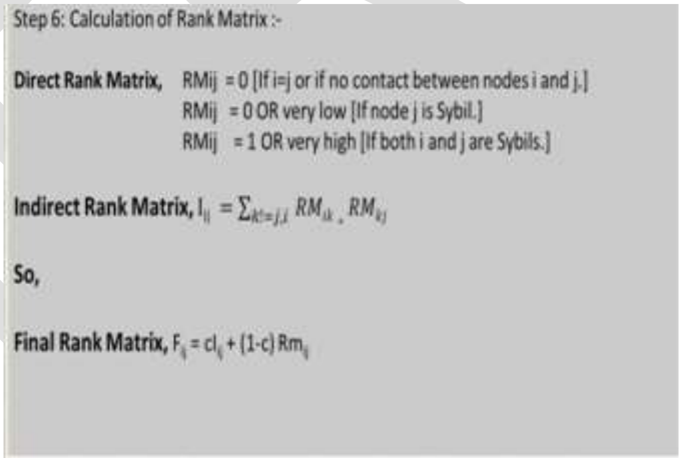


Figure 3. Trusted Server with parent child node

Step 5 : Then Parent node compare following parameter of child node with its sibling :-

1. Level of the node in the hierarchical structure, considering super node at level 0.
2. Count of Invitations Assigned previously.
3. Number of times it has requested compared with its siblings.
4. Duration between requests (comparing Timestamp with current system time) compared with its siblings.
5. Frequency of usage of invitations compared to general behavior of network.
6. Reputation value in total rank matrix if ever super node has done the calculation.
7. Checking the node request is real or fake. i.e. may be possible that requested node already stored ids but demand more.

After the Node will be assigned ‘Genuine’ or ‘Sybil’.



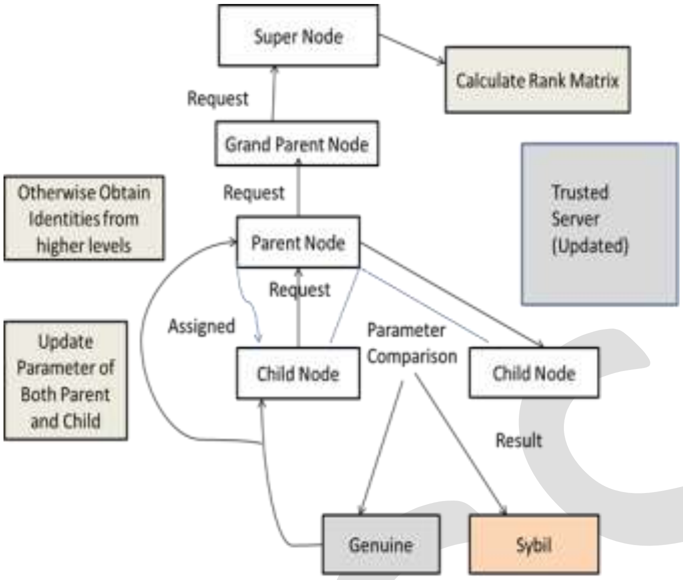
Step 6: Calculation of Rank Matrix :-

Direct Rank Matrix, RMij = 0 [If i=j or if no contact between nodes i and j.]
RMij = 0 OR very low [If node j is Sybil.]
RMij = 1 OR very high [If both i and j are Sybils.]

Indirect Rank Matrix, $I_{ij} = \sum_{k!=j,i} RM_{ik} . RM_{kj}$

So,

Final Rank Matrix, $F_{ij} = cI_{ij} + (1-c)\,Rm_{ij}$



Invitation of another node when parent has no unused set of Invitations

Trusted Server can be used to identify node is Sybil or not . After eliminating Sybil node from network , we can maintain hierarchy of network using trusted Server .

IV. CONCLUSION

This paper proposes a model for minimizing sybil attack using Trusted Server in P2P networks. Using this scheme the sybil behavior of a node can be identified, and those suspected as sybils are limited from inviting others. Moreover nodes may contact one another for file sharing and super nodes calculate rank matrix and uses these values also for assignment of new identities.

REFERENCES:

[1] Ratnasamy, S., Francis, P., Handley, and Shenker: A scalable content-addressable network. In Proceedings of ACM SIGCOMM San Diego, California, Aug. 2001.
[2] I. Stoica, R. Morris et al., “Chord: A Scalable Peer-to-Peer Lookup Protocol for Internet Applications,” IEEE/ACM Trans. Net., vol. 11, no. 1, 2003, pp. 17–32.
[3] A. Rowstron and P. Druschel, “Pastry: Scalable, Distributed Object Location and Routing for Large-scale Peer-to-peer Systems,” Proc. Middleware, 2001.
[4] B. Y. Zhao et al., “Tapestry: A Resilient Global-Scale Overlay for Service Deployment,” IEEE JSAC, vol. 22, no. 1, Jan. 2004, pp. 41- 53.
[5] P. Baecher, M. Koetter and M. Dornseif. The nepenthes platform: An efficient approach to collect malware. In Proceedings of 9th International Symposium On Recent Advances in Intrusion Detection (RAID’06), 2006.
[6] J.Douceur: The Sybil Attack. Proceedings of the First International Workshop on Peer-to-peer Systems. Springer, March 2002.
[7] J. Ledlie and M. Seltzer. Distributed, secure load balancing with skew, heterogeneity, and churn. In Proc. IEEE INFOCOM, Mar. 2005.
[8] Brian Neil Levine, Clay Shields, and N. Boris Margolin, “A Survey of Solutions to the Sybil Attack,” Tech report 2006-052, University of Massachusetts Amherst, Amherst, MA, October 2006
[9] N. Borisov. Computational puzzles as sybil defenses. In Proceedings of the 6th IEEE International Conference on Peer-to-Peer Computing (P2P), volume 0, pages 171–176. IEEE Computer Society, 2006.
[10] P. Druschel and A. I. T. Rowstron. PAST: A large-scale, persistent peer-to-peer storage utility. In Proceedings of the 8th IEEE Workshop on Hot Topics in Operating Systems. IEEE Computer Society, 2001.
[11] B. Awerbuch and C. Scheideler. Group Spreading: A Protocol for Provably Secure Distributed Name Service. In Proc. Automata, Languages and Programming (ICALP), pages 183–195, 2004.
[12] H. Rowaihy, W. Enck, P. McDaniel, and T. L. Porta. Limiting sybil attacks in structured P2P networks. In INFOCOM, pages 2596–2600. IEEE, 2007