Secured P2P Network using Self Organizing Trust Model (SORT)

Prof. S. S. Shinde[1] Atul Pawale[2] Vishakha Satkar[3] Shital Sutar[4] Pooja Tamke[5]
[1]Assistant Professor [2,3,4,5]Student
[1,2,3,4,5]Department of Computer Engineering
[1,2,3,4,5]MMIT Lohagaon, Maharashtra, India

Abstract— Drawback of unpredictable nature of peer to peer model is that they are vulnerable to malicious activity. Attacks of malicious peer/users can be minimize by building trust relationships among peers/users. Distributed algorithm in this system enable a peer to know about trustworthiness of other peers based on past interactions and recommendations. By using local information available peers create their own trust network in their proximity. Service context and recommendation context of trust are measured based on importance of peer, recentness and satisfaction of peer parameters. Also while calculating recommendation, trustworthiness of recommender's and recommendation confidence is considered. In this system, untrusted peers i.e., Malicious peer are isolated and good peers are able to form trust in their proximity.

Key words: Peer to Peer Systems, Trust management, Reputation, Security, Recommendation, Service

I. INTRODUCTION

A user may provide good service but gives bad recommendation or vice versa. Thus, Secured P2P Network using SORT Model defines two trust contexts i.e., service context and recommendation context so it differentiate providing services and giving recommendations as two different tasks. Information related to interactions and recommendations happened in the past are stored separate to assess competence and integrity of peer in these contexts. Secured P2P Network using SORT Model estimates three trust metrics. Based on recommendations value Reputation metric is calculated. When deciding about strangers and new acquaintances Reputation value is important. When peers have more interaction Reputation value is become less important. In service and recommendation contexts Service trust and recommendation trust are primary metrics to measure trustworthiness, respectively. While selecting service providers the service trust metric is used. When recommendations are needed the recommendation trust metric is important. During the estimation of reputation metric, recommendations are evaluated based on the recommendation trust metric. We conducted experiments by implementing a P2P file sharing simulation tool to understand impact of Secured P2P Network using SORT Model in minimizing attacks. . To enable to make more realistic observations on evolution of trust relationships parameters like peer bandwidth, number of shared files online/ offline periods, waiting time for sessions file sizes, popularity of files are approximated to several empirical results. We also studied types of service and recommendation- based attacks. Secured P2P Network using SORT Model minimized service-based attacks in all cases. Experiments with Secured P2P Network using SORT Model show that good peers without having global trust information can defend themselves against attackers. Secured P2P Network using SORT Model trust metrics let a peer assess trustworthiness of other peers based on local information.

II. LITERATURE REVIEW

To make our proposed system more strong. A lot of researchers have carried out their work in the area of P2P system in the past decade by using various techniques.

Authors Karl Aberer, Zoran Despotovic et.al in paper[1] present an approach that resolve the problem of reputation-based trust management at both the data management and the semantic level. There are Various problem of managing trust in a decentralized information system are: Global trust model, Local algorithm to determine trust and Data & communication management. This paper proposes a simple yet effective method that implements a straightforward reputation trust model but covers all the relevant aspects. It employ at both levels scalable data structures and algorithms that require no central control and allow to assess trust by evaluating peer reputation from its past interactions with other peers. Thus the method can be used in a P2P area and it also support well for very large numbers of peers.

Another work by Sepandar D. Kamvar et.cl in paper [2] has proposed an algorithm that decrease the number of downloads of inauthentic files in a P2P network. Issue in Open nature of P2P networks is an almost ideal environment for the spreading inauthentic files. Based on the users history of uploads. it gives each user a unique global trust value. With the help of Power iteration, it represent a decentralized and secure method to estimate global trust values,. With these peers use these values to choose the files from peers whom they download, the system identifies attacker peers and isolates them from the system. In experiment, EigenTrust reputation system, it is used to significantly decrease the number of malicious files on the network. It represents a method in which each peer i is have a distinct global trust value that reflects the interactions of all peers in the network with peer i. In this approach, all peers in the system participate in evaluating global trust values in a decentralized and node-symmetric manner with minimal overhead on the network. This paper present a reputation system that combine the local trust values of all of the peers in a natural manner, and it also have minimal overhead in terms of message complexity.

Runfang Zhou, Kai Hwang et.al in paper [3] proposes a gossip-based reputation system GossipTrust for fast gathering of global reputation scores. It pulls a Bloom filter based scheme for efficient score ranking. GossipTrust does not need any secure hashing or fast lookup mechanism, thus it is applicable to both unstructured and structured P2P networks. With the help of Bloom filters, it can reduce the memory overhead per node to 512 KB for a 10,000-node network. This system is a robust, scalable, and secure reputation management system and it is specifically designed for unstructured P2P networks. GossipTrust system uses a gossip-based protocol to combine global

All rights reserved by *www.ijsrd.com*

reputation scores fast and accurately. The basic idea behind this is to allow peers to share local trust values with randomly-selected peers until reaching some global consent on peer reputations. Gossip-based protocols do not need an error recovery mechanism, so enjoy the simplicity and low overhead, compared with using other deterministic protocols.

III. PROPOSED SYSTEM

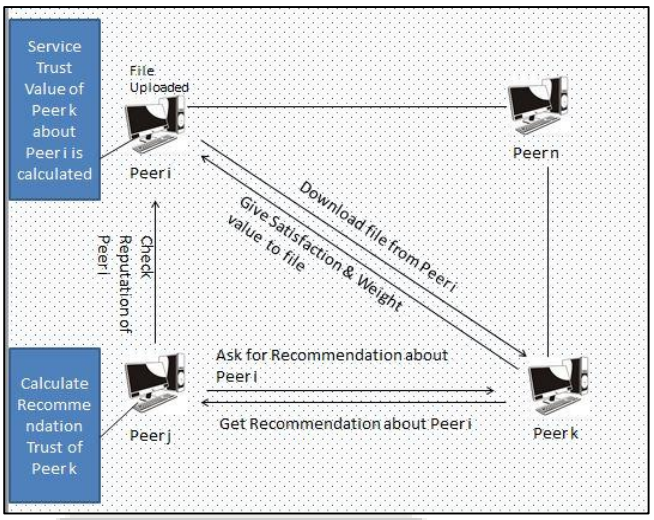

Fig. 1:

In our proposed system, at beginning each peer is stranger to each other. Peer's build trust relationship among themselves by using services of each other. When peer i uses service of other peer j, peer i gives satisfaction and weight value based on quality of service. Based on these value Service Trust of peer i about peer j is calculated.

When peer i want to use service of stranger j, it first check reputation of peer j by getting recommendation from his acquaintances who already uses service of peer j.

After checking reputation and using service of peer j, peer i evaluates recommendation given by his acquaintances based on his experience after using service. Because of these metric values, it create trust relationship among peers.

IV. CONCLUSIONS

A trust model for peer to peer networks is presented, in which a user can develop a trust network in its proximity. A user can isolate malicious users around itself as it develops trust relationships with good users. Two context of trust, service and suggestion contexts are defined to measure capabilities of users in providing services and giving recommendations SORT modify both service and recommendation-based attacks in most experiments. However, in extremely malicious environments such as a 50 percent malicious network, associate can continue to disseminate large amount of misleading recommendations. Another issue about SORT is preserve trust all over the network. If a user changes its point of attachment to the network, it might lose a part of its secure network. These issues might be studied as a future work to extend the trust model. Using trust information does not solve all privacy problems in peer to peer systems but can enhance security and efficiency of systems. If interactions are modeled correctly, SORT can be adapted to various P2P applications, e.g., CPU sharing, storage networks, and user to peer gaming. Defining application specific context of trust and related metrics can help to assess trustworthiness in various tasks.

ACKNOWLEDGEMENT

I would like to thanks to my guide Prof. S. S. Shinde for his highly appreciable support and encouragement also thanks to my HOD Prof. P.M. Daflapurkar. Their guidance is a force behind the completion of this paper. I am grateful for all the solutions and hints provided by him. My acknowledgement of gratitude to all who supported to make it possible.

REFERENCES

[1] K. Aberer and Z. Despotovic, "Managing Trust in a Peer-2-Peer Information System", *Proc. 10th Int'l Conf. Information and Knowledge Management (CIKM)*, 2001.
[2] S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The (Eigentrust) Algorithm for Reputation Management in P2P Networks*", Proc. 12th World Wide Web Conf. (WWW)*, 2003.
[3] 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.
[4] A.A. Selcuk, E. Uzun, and M.R. Pariente, \A Reputation-Based Trust Management System for P2P Networks", *Proc. IEEE/ACM Fourth Intl Symp. Cluster Computing and the Grid (CCGRID)*, 2004.
[5] G. Draper and R. Riesenfeld, "Who votes for what? A visual query language for opinion data", *IEEE Transa. Vis. Comput. Graphics, vol. 14, no. 6. 11971204*, Nov./Dec. 2008.

All rights reserved by *www.ijsrd.com*