P. Ponmalar *et al*, International Journal of Computer Science and Mobile Applications,
Vol.2 Issue. 5, May- 2014, pg. 14-19 **ISSN: 2321-8363**

A SELF-SYSTEMATIZE DEPENDENCE SCULPT FOR DECENTRALIZED SYSTEMS

P. Ponmalar,
II M.E CSE,
Francis Xavier Engg. College,
Tirunelveli

K. Rajasundari, M.E.,
Asst. Professor,
Francis Xavier Engg. College,
Tirunelveli

Abstract—Open nature of peer-to-peer systems exposes them to malicious activity. Building trust relationship among the peers can mitigate attacks of malicious peers. This paper proposed the distributed algorithms that enable a peer to reason about trustworthiness of other peers based on past interactions and recommendations. Peers create their own trust network in their proximity by using local information available and do not try to learn global trust information. Two contexts of trust, service, and recommendation contexts are defined to measure trustworthiness in providing services and giving recommendations. Interactions and recommendations are evaluated based on relevant, recentness, and peer satisfaction parameters. Additionally, recommender's trustworthiness and confidence about a recommendation are considered while evaluating recommendations. Simulation experiments on a file sharing application show that the proposed model can mitigate attacks on different malicious behavior models. In these experiments, good peers were able to form trust relationships in their proximity and isolate malicious peers.

Keywords: Distributed algorithm, Auto update mechanism, Trust relationship for Peers systems

I. INTRODUCTION

The concept of witness anonymity for peer-to-peer systems, as well as other systems with the peer to peer nature. Witness anonymity combines the seemingly conflicting requirements of anonymity (for honest peers who report on the misbehavior of other peers) and accountability (for malicious peers that attempt to misuse the anonymity feature to slander honest peers). The Secure Deep Throat (SDT) protocol to provide anonymity for the witnesses of malicious or selfish behavior to enable such peers to report on this behavior without fear of retaliation. On the other hand, in SDT, the misuse of anonymity is restrained in such a way that any malicious peer attempting to send multiple claims against the same innocent peer for the same reason (i.e., the same misbehavior type) can be identified. In a peer-to-peer (P2P) network, every machine plays the role of client and server at the same time. Although a P2P network has a number of advantages over the traditional client-server model in terms of efficiency and fault-tolerance, additional security threats can be introduced. Users and IT administrators need to be aware of the risks from propagation of malicious code, the legality of downloaded content, and vulnerabilities within peer-to-peer software. Security and preventative measures should be implemented to protect from any potential leakage of sensitive information and possible security breaches. Within corporate networks, system administrators need to ensure that peer-to- peer traffic complies with the corporate security policy.

II. SYSTEM ANALYSIS

A. PROBLEM DEFINITION

To identify the malicious peer in P2P system and to create the trust relationship and to create the trust relationship among the peer. To provide two contexts of trust services and giving recommendations to measure the trustworthiness. It represents distributed algorithms to ensure trustworthiness in peer based on past interactions and recommendations.

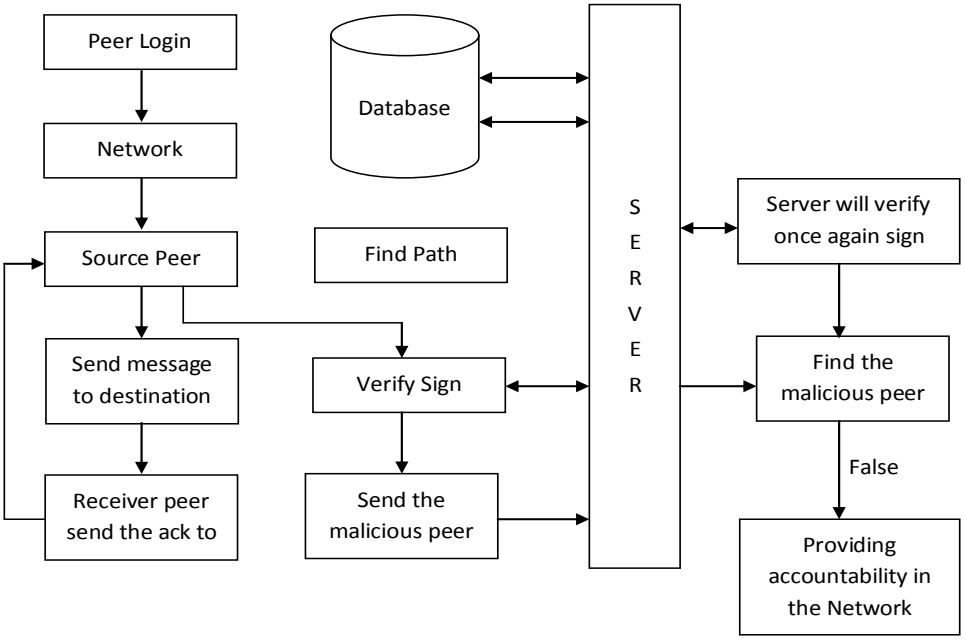
B. EXISTING SYSTEM

Most previous works on trust management in peer-to-peer systems have focused on the Reliability. A peer that issues a query for the trust ratings of another peer should be able to compute the true trust value despite the presence of malicious peers. In these systems, a peer is assigned a trust value or reputation based on a trust metric. Although various systems differ in how this metric is defined, in general, the trust value associated with a peer is calculated based on the feedback provided by other peers. Peers rate the performance or behavior of another peer based on their previous interactions.

C. PROPOSED SYSTEM

To introduce the term witness anonymity to refer to this combination of seemingly conflicting requirements, i.e., identity anonymity for honest peers and accountability for misbehaving peers. The major goal of the work is to show how peer-to-peer trust management systems can be extended to provide witness anonymity. Another important motivation for witness anonymity is simply to preserve the privacy of peers participating in the peer-to-peer trust management system. A protocol called the Secure Deep Throat (SDT) for providing witness anonymity in peer-to-peer systems. To the best of the knowledge, SDT is the first protocol that can support both aspects of witness anonymity.

III. SYSTEM ARCHITECTURE



IV. SYSTEM MODULES

A. Peer Registration

To add any number of Peers dynamically and construct the connections dynamically. Construct the dynamic network topology. Peer can easily leave from the network. Distributed hash Table (DHT) maintains the peer details and also it updates the status of each peer in network.

B. ERT Construction

In this module, Elastic Routing Table in each node is constructed. It contains the in link and out link details of each node. In degree and out degree calculated for each node depends upon the connections details.

C. In degree Construction

The degree of each node is updated based on the degree value. The load status of each peer in the network is measured here. Capacity value also calculated by using available degree value divide by total degree value. Capacity value maintain in the elastic routing table.

D. Best Peer Selection

Best peer selected based on high degree value and capacity value. That means high capacity value peer has less amount of load in the network. So high capacity value peer is selected. So allocated work completed in very less time period. Network also avoids the unwanted load problem in process time. Peer join and reliving suffer degree value of each peer.

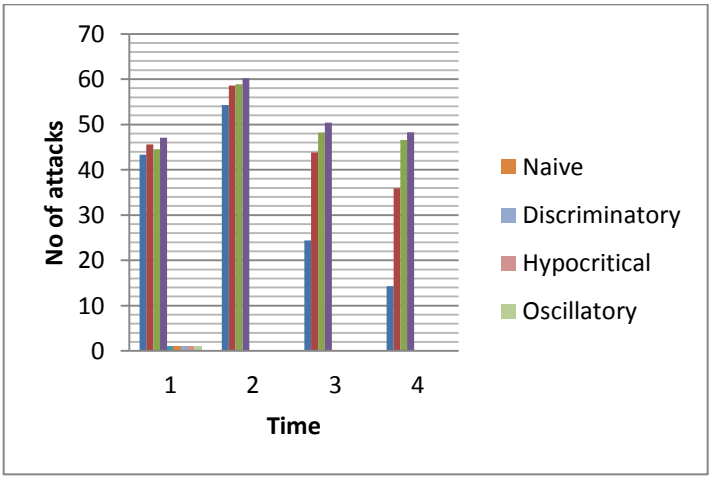


Fig. Individual Attacker (10% malicious)

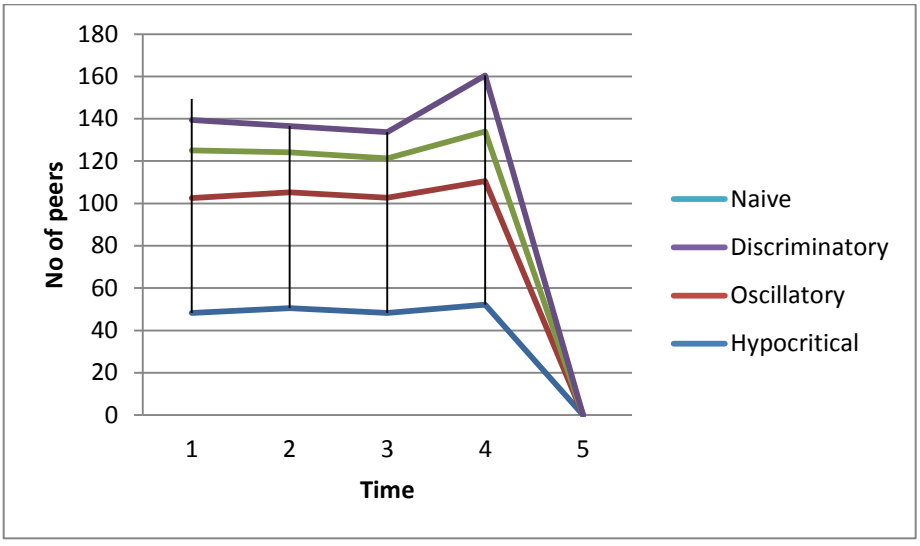


Fig. Individual Pseudospoofers(10% malicious)

V. CONCLUSION

A trust model for P2P networks is presented, in which a peer can develop a trust network in its proximity. A peer can isolate malicious peers around itself as it develops trust relationships with good peers. Two context of trust, service and recommendation contexts are defined to measure capabilities of peers in providing services and giving recommendations. Interactions and recommendations are considered with satisfaction, weight and fading effect parameters. A recommendation contains the recommenender's own experience, information from its acquaintances, and level of confidence in the recommendation. These parameters provided as a better assessment of trustworthiness. My future work will enhance the security of P2P system and recommendation-based attacks in most experiments. If a peer changes its point of attachment to the network, it might lose a part of its trust network. These issues might be studied as a future work to extend the trust model.

REFERENCES

1. Aberer.A, A.Datta, and M.Hauswirth(2005),'P-Grid:Dynamics of Self-Ststems and Applications',Vol. 3845, No. 3, pp. 31-38

2. Boyd.S, Ghosh.A, Prabhakar.B, and Shah.D(2006),'Randomized Gossip Algorithms',Vol. 52,No. 6, pp. 2508-2530.

3. Friedman.E.J and Resnick.P(2001),'The Social Cost of Cheap Pseudonyms', J.Economics and Management Strategy,Vol. 10,No. 2, pp. 173-199.

4. Hoffman.K, Zage.D, and Nita-Rotaru.C(2009),'A Survey of Attack and Defence Techniques for Reputation Systems',ACM Computing Surveys,Vol. 42, No.1, pp. 21-31.

5. Ratnasamy.S, Francis.P ,Handley.M, Karp.R, and Shenker.S(2001),'A Scalable Content-Addressable Network',ACM SIGCOMM Computer Comm.Rev, Vol. 31, No. 4, pp. 161-172.

6. Resnick.P, Kuwabara.K, Zeckhauser.R, and E.Friedman(2000),'Reputation Systems' Comm.ACM,Vol. 43,No. 12, pp. 45-51.

7. Ripeanu.M,Foster.and Iamnitchi.A(2002),'Mapping the GnutellaNetwork Properties of Large-Scale Peer-to-Peer Systems and Implications for System Design',Vol. 6, No. 1, pp. 50-57.

8. Sherwood.R, Lee.S, and Bhattacharjee.B(2006),'Cooperative Peer Groups in Nice',Computer Networks, Vol. 50,No. 4, pp. 523-544.

9. Song.S, Hwang.K, Zhou.R, and Kwok.Y.K(2005),'Trusted P2P Transactions with Fuzzy Reputation Aggregation'IEEE Internet Computing',Vol. 9, No. 6, pp. 24-34

10. Staab.S, Bhargava.B, Lilien.L, Rosenthal.A, Winslett.M, Sloman.M, Dillon.T, Chang.E, Hussan.F.K, Nejdl.W, Olmedilla.D, and Kashyap.V(2004), 'The Pudding of Trust',IEEE Intelligent Systems,Vol. 19, No. 5, pp. 74-88.

11. Stoica.I, Morris.R, Karger.D, Kaashoek.M.F, and Balakrishnan.H (2001),'Chord:A Scalable Peer-to-Peer Lookup Service for Internet Applications' ,ACM SIGCOMM Computer Comm.Rev, Vol. 31, No. 4, pp. 149-160.

12. Tran.N, Min.B, Li.J and Subramanian.L(2009), 'Sybil-Resilient Online Content Voting' Proc. Sixth USENIX Symp. Networked Systems and Implementation (NSDI),Vol. 12,No. 3,pp. 45-53.

13. Victor.P, Cornelis.C,De Cock.M ,and Pinheiro da Silva.P(2009),'Gradual Trust and Distrust in Recommender Systems',Fuzzy Sets Systems',Vol. 160, No. 10, pp. 1367-1382.

14. Yu.H, Kaminsky.M, Gibbons.P.B, and Flaxman.A(2006),'Sybilguard:Defending against Sybil Attacks via Social Networks',ACM SIGCOMM Computer Comm.Rev,Vol. 36,No. 4, pp. 267-278.

15. Zhou.R and Hwang.K(2007), '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.

Authors Bibliography

P. Ponmalar is doing her M.E in Francis Xavier Engineering College at Tirunelveli. She received her B.E degree in Computer Science Engineering from S.Veerasamy Chettiar College of Engineering, Chennai in 2008. She is an active member of the Computer Society of India (CSI). Her area of interest is Networking, Network Security, and Computer networks.

K. Rajasundari is presently working as an Assistant Professor, Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli. She completed her M.E in Computer Science and Engineering from Francis Xavier Engineering College at Tirunelveli. She received her B.E degree in Computer Science Engineering from National College of Engineering, Maruthakulam in Tirunelveli.

