ISSN 2395-1621

Securing P2P Interaction Using Self Organizing Trust Model

[#1]Akshay Pandey, [#2]Umesh Nagre, [#3]Sufiyan Pathan, [#4]Swapnil Dange,
[#5]Prof. Ms. Sonali Sonwane

[1]apandey2389@gmail.com
[2]umeshnagre123@gmail.com
[3]sufi.pathan143@gmail.com
[4]swapnildange1@gmail.com

[#1234]Department of Information Technology
[#5]Department of Information Technology
G. H. Raisoni College of Engineering and Management,
Wagholi, Pune.

ABSTRACT

Peer-to-peer (P2P) systems have attracted significant interest in recent years. In P2P networks, each peer act as both a server or a client. This characteristic makes peers vulnerable to a wide variety of attacks. Having robust trust management is very critical for such open environments to exclude unreliable peers from the system. This paper investigates the use of genetic programming to assess the trustworthiness of peers without a central authority. A trust management model is proposed in which each peer ranks other peers according to local trust values calculated automatically based on the past interactions and recommendations. The experimental results have shown that the model could successfully identify malicious peers without using a central authority or global trust values and, improve the system performance.

ARTICLE INFO

Article History

Received: 1st June 2016

Received in revised form :

1th June 2016

Accepted: 3rd June 2016

Published online :

4th June 2016

Keywords: Peer-to-peer systems, trust management, reputation, security.

I. INTRODUCTION

The popularity and wide spread usage of peer-topeer (P2P) systems has soared over the past several years. Throughout the evolution of P2P systems the definition of P2P has changed along with the software architecture of the various P2P applications. While the initial popular usage of P2P systems was for file sharing (more specifically the sharing of music files in mp3 format) the problem domain that P2P systems address today cover the range from data sharing to collaboration to distributed computing and beyond. For the continued increased usage of P2P systems, the need for security and trust arises. This chapter covers evolution of P2P systems through the examination of Napster, Gnutella, KaZaa, and BitTorrent, system capabilities and shortcomings, and security needs, which highlights the need for trust in P2P systems. With this basis we then present our vision for trust and security followed by a literature review of trust in P2P systems. We then introduce and develop a Universal Trust Set as a foundation for building trustworthy environment, and then our approach for implementing the set, and the future of P2P systems where we will discuss other open issues that need addressing. These guarantees are obtained using FosterLyapunov Theorem which ensures the stability of a controlled Markov chain if a Lyapunov function with negative expected drift is shown to exist. More specifically, the throughput optimal back pressure based policies as well as maximum weight schedules is reverse-engineered to be the very Existing System: Abdul-Rahman and Hailes evaluate trust in a discrete domain as an aggregation of direct experience and recommendations of other parties. They define a semantic distance measure to test accuracy of recommendations. Yu and Singh's model propagates trust information through referral chains. Referrals are primary method of developing trust in others. Mui et al. propose a statistical model based on trust, reputation, and reciprocity concepts. Reputation is propagated through multiple referral chains. Jøsang et al. discuss that referrals based on indirect trust relations may cause incorrect trust derivation. Thus, trust topologies should be carefully evaluated before propagating trust information. Terzi et al. introduce an algorithm to classify users and assign them roles based on trust relationships. Zhong proposes a dynamic trust concept based on McKnight's social trust model. When building trust relationships, uncertain evidences are evaluated using second-order probability and Dempster-Shaferian framework. Disadvantages: 1. To perform the recommendation need to take distance support its mandatory 2. There is no direct

recommendation, chain rules are applied 3. Time complexity is very high 4. Loss of packets when the data is transmitted 5. Peers can't collect Global information The popularity and wide spread usage of peer-topeer (P2P) systems has soared over the past several years. Throughout the evolution of P2P systems the definition of P2P has changed along with the software architecture of the various P2P applications. While the initial popular usage of P2P systems was for file sharing (more specifically the sharing of music files in mp3 format) the problem domain that P2P systems address today cover the range from data sharing to collaboration to distributed computing and beyond. For the continued increased usage of P2P systems, the need for security and trust arises. This chapter covers evolution of P2P systems through the examination of Napster, Gnutella, KaZaa, and BitTorrent, system capabilities and shortcomings, and security needs, which highlights the need for trust in P2P systems. With this basis we then present our vision for trust and security followed by a literature review of trust in P2P systems. We then introduce and develop a Universal Trust Set as a foundation for building trustworthy environment, and then our approach for implementing the set, and the future of P2P systems where we will discuss other open issues that need addressing. These guarantees are obtained using FosterLyapunov Theorem which ensures the stability of a controlled Markov chain if a Lyapunov function with negative expected drift is shown to exist. More specifically, the throughput optimal back pressure based policies as well as maximum weight schedules are reverse-engineered to be the very

II. EXISTING SYSTEM

Abdul-Rahman and Hailes evaluate trust in a discrete domain as an aggregation of direct experience and recommendations of other parties. They define a semantic distance measure to test accuracy of recommendations. Yu and Singh's model propagates trust information through referral chains. Referrals are primary method of developing trust in others. Mui et al. propose a statistical model based on trust, reputation, and reciprocity concepts. Reputation is propagated through multiple referral chains. Jøsang et al. discuss that referrals based on indirect trust relations may cause incorrect trust derivation. Thus, trust topologies should be carefully evaluated before propagating trust information. Terzi et al. introduce an algorithm to classify users and assign them roles based on trust relationships. Zhong proposes a dynamic trust concept based on McKnight's social trust model. When building trust relationships, uncertain evidences are evaluated using second-order probability and Dempster-Shaferian framework.

Disadvantages:

1. To perform the recommendation need to take distance support its mandatory.

2. There is no direct recommendation, chain rules are applied

3. Time complexity is very high

4. Loss of packets when the data is transmitted

5. Peers can't collect Global information

III.PROPOSED SYSTEM

Recommendation-based attacks were contained except when malicious peers are in large numbers.

In P2P networks, clients both provide and use resources. This means that unlike client-server systems, the content serving capacity of peer-to-peer networks can actually increase as more users begin to access the content (especially with protocols such as Bit torrent that require users to share, refer a performance measurement study.

This property is one of the major advantages of using P2P networks because it makes the setup and running costs very small for the original content distributor.

Peer-to-peer content delivery networks.

Peer-to-peer content services, e.g. caches for improved performance such as Correli Caches.

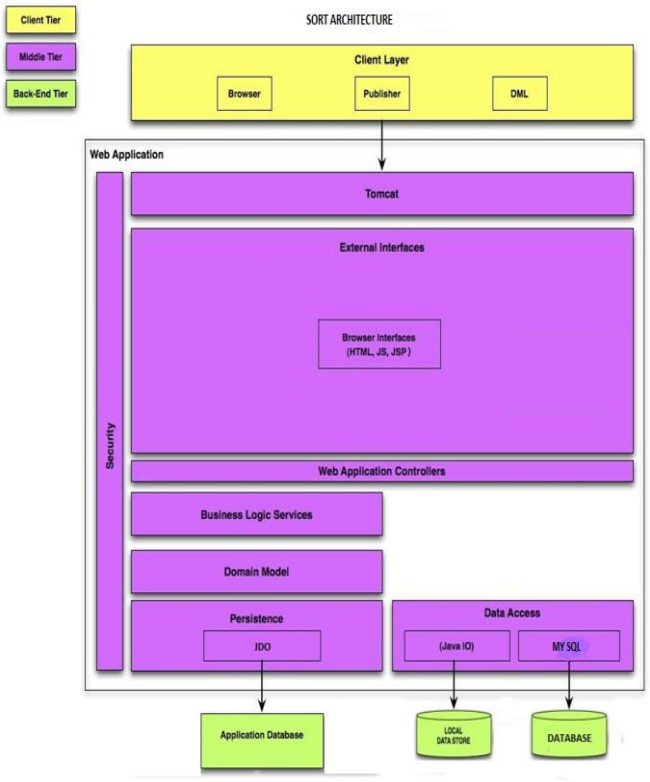

Fig 1. System architecture

Following are the steps we can perform to Self-Organizing Trust Model:

1. Initially we give .Java class file as input.
2. Using reflect API we extract the basic features of class(Number of Constructor, Parent Class name, Class Is Public or Not ,Number of Public Variables, Number of Methods and Respective names etc.).
3. After that We Parse the code for Calculating Number of If/For/While etc. Loops.
4. After getting all the Features we compare with stored Feature using Similarity Measures.

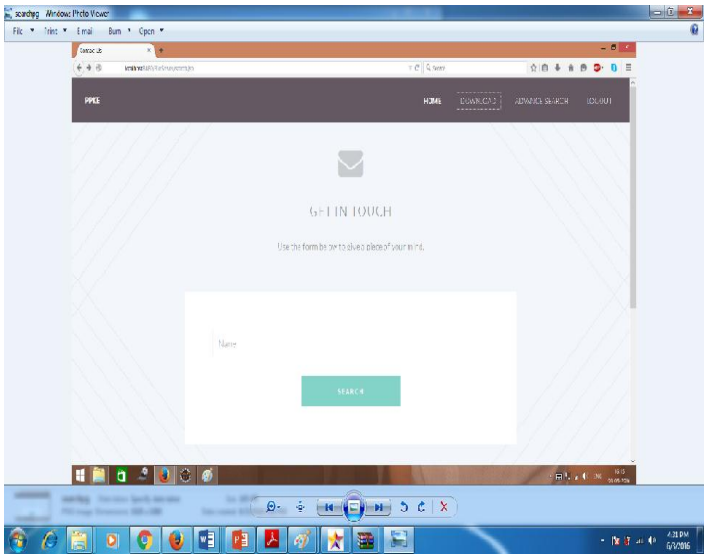

Fig 1. Main Menu

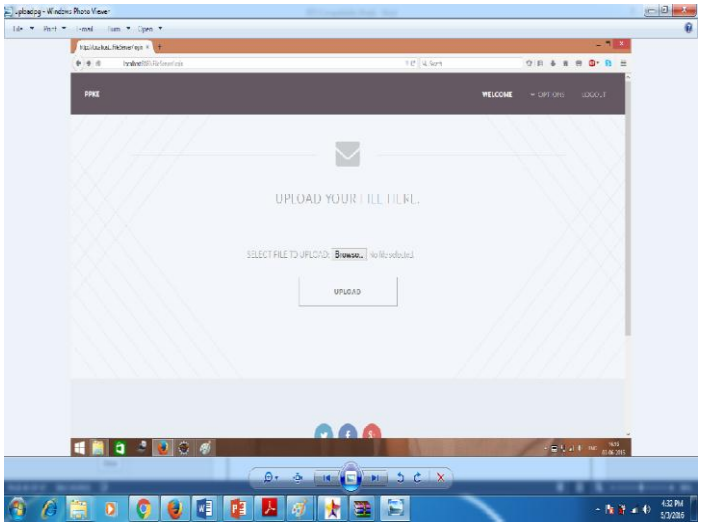

Fig 2. Uploading

IV. CONCLUSION

Today we are living in era of Information explosion, where need of data is increasing. Hence along with data integrity trustworthiness of its provider must be assessed. In current scenario only file integrity is evaluated. But with increase cyber-attack we must check its provider. In our current model we are doing verification based on Email based OTP further biometric verifications can be implemented. Also here we giving User ratings based on his performance in current network only and when new user is added to network, information about him is empty. As a future extension there can be a system which monitors user behaviour across internet and some basic feedback about user is added when he enters first time in network.

REFERENCE

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. F. Cornelli, E. Damiani, S.D.C. di Vimercati, S. Paraboschi, and P. Samarati, "Choosing Reputable Servents in a P2P Network," Proc. 11th World Wide Web Conf. (WWW), 2002.

3. 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.

4. 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.

5. A.A. Selcuk, E. Uzun, and M.R. Pariente, "A Reputation-Based Trust Management System for P2P Networks," Proc. IEEE/ACM Fourth Int'l Symp. Cluster Computing and the Grid (CCGRID), 2004

6. 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.

7. J. Kleinberg, "The Small-World Phenomenon: An Algorithmic Perspective," Proc. 32nd ACM Symp. Theory of Computing, 2000.

8. S. Saroiu, P. Gummadi, and S. Gribble, "A Measurement Study of Peer-to-Peer File Sharing Systems," Proc. Multimedia Computing and Networking, 2002.

9. M. Ripeanu, I. Foster, and A. Iamnitchi, "Mapping the Gnutella Network: Properties of Large-Scale Peer-to-Peer Systems and Implications for System Design," IEEE Internet Computing, vol. 6,no. 1, pp. 50-57, Jan. 2002.

10. S. Saroiu, K. Gummadi, R. Dunn, S.D. Gribble, and H.M. Levy, "An Analysis of Internet Content Delivery Systems," Proc. Fifth USENIX Symp. Operating Systems Design and Implementation (OSDI), 2002.

