ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Novel Design and Implementation of Self Organizing Trust Model for Peer - Peer Systems

E. Latha
M.Tech,
Dept of Software Engineering (SE),
Vinuthna Institute of Technology & Sciences.

T. Moulika
Asst. Professor,
Dept of Software Engineering (SE),
Vinuthna Institute of Technology & Sciences.

Abstract:

This paper discusses about novel design and implementation of self organizing trust model for peer – peer systems using integrated technologies like trust model, p2p systems, self organizing, novel design and implementation etc.

Keywords: Trust Model, P2P Systems, Self Organizing, Novel DESIGN.

I.INTRODUCTION AND LITERATURE SURVEY:

The popularity and wide spread usage of peer-to- peer (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 Foster- Lyapunov Theorem which ensures the stability of a based policies as well as maximum weight schedules are 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 controlledMarkov chain if a Lyapunov function with negative expected drift is shown to exist. More specifically, the throughput optimal backpressure-

4. Loss of packets when the data is transmitted

5. Peers can't collect Global information

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

II NOVEL DESIGN AND IMPLEMENTATION:

Figure 1 below provides usecase diagram of this novel design and implementation. Figure 2 below provides class diagram of this novel design and implementation. Figure 3 below provides sequence diagram of this novel design and implementation.

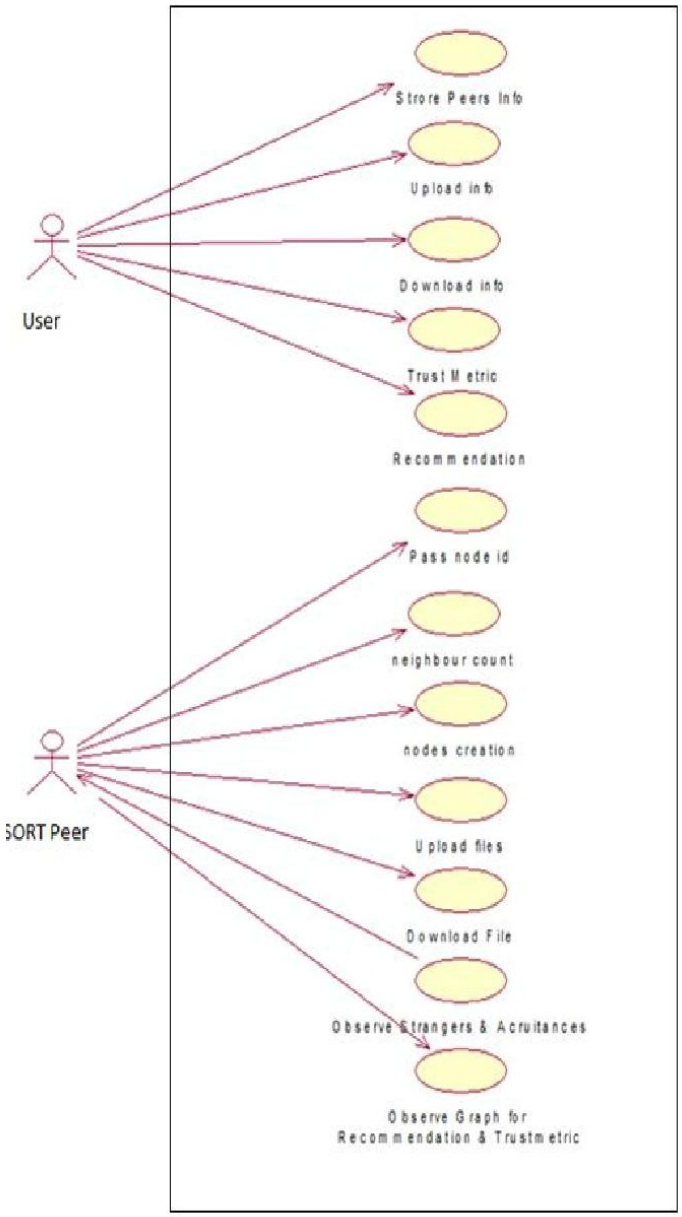

Figure 1 usecase diagram

Proposed System:

We propose a Self-ORganizing Trust model (SORT) that aims to decrease malicious activity in a P2P system by establishing trust relations among peers in their proximity.

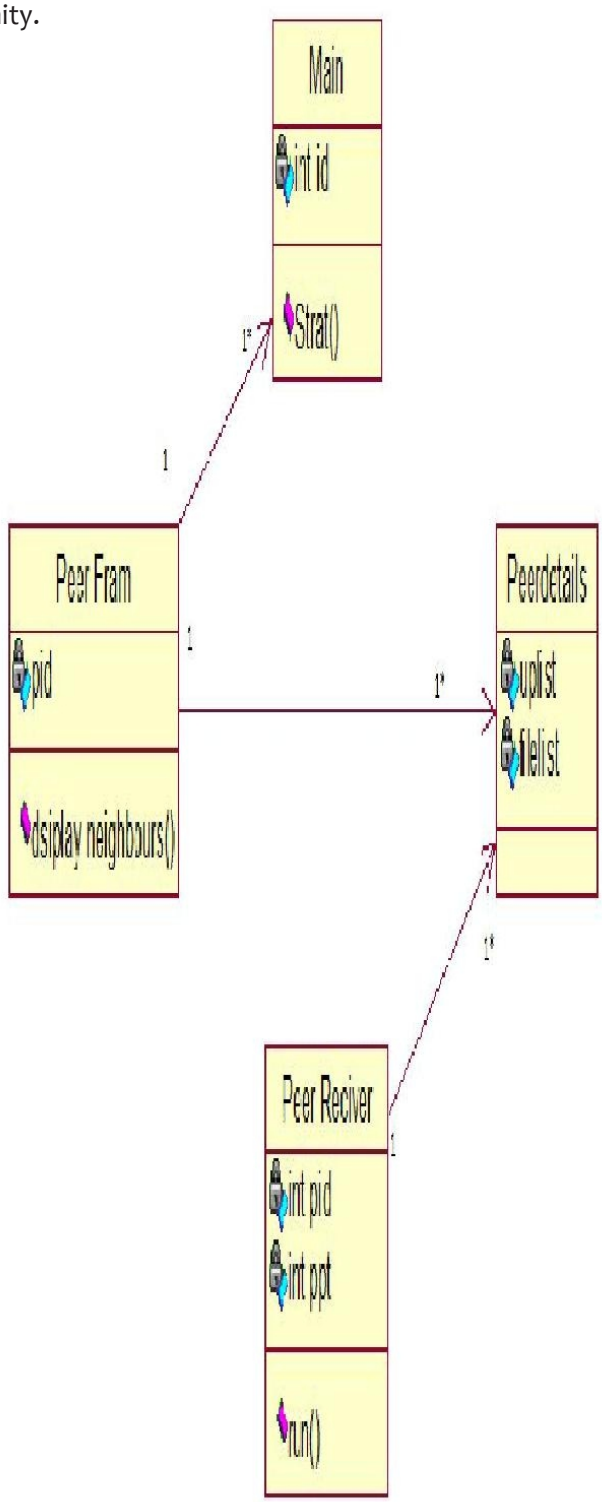

Figure 2 class diagram

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

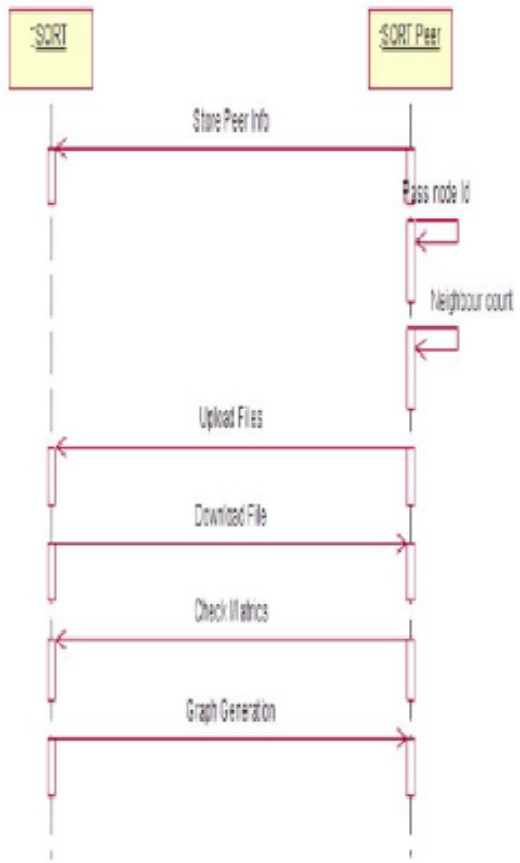

Figure 3 sequence diagram

Figure 4 Peer Information

Figure 4 provides execution screen shot for peer information. Figure 5 provides execution screen shot for recommendation. Figure 6 provides execution screen shot for trust metric. Figure 7 provides execution screen shot for final recommendation.

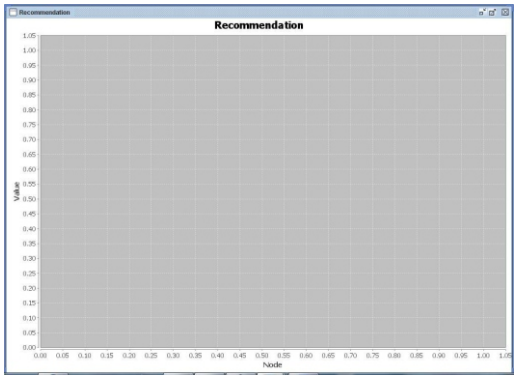

Figure 5 Recommendation

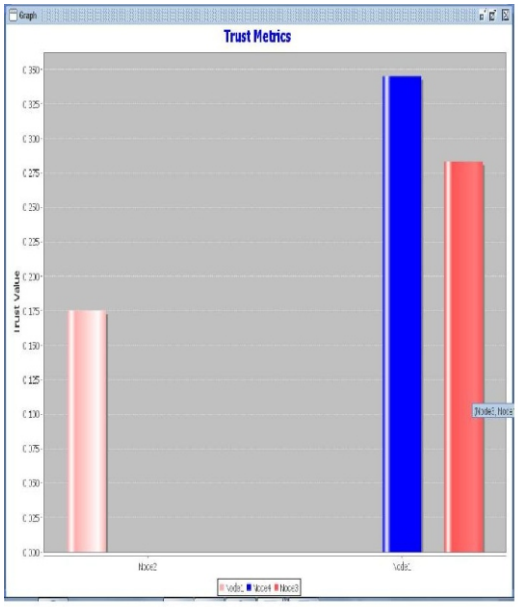

Fig: 6 Trust Metric

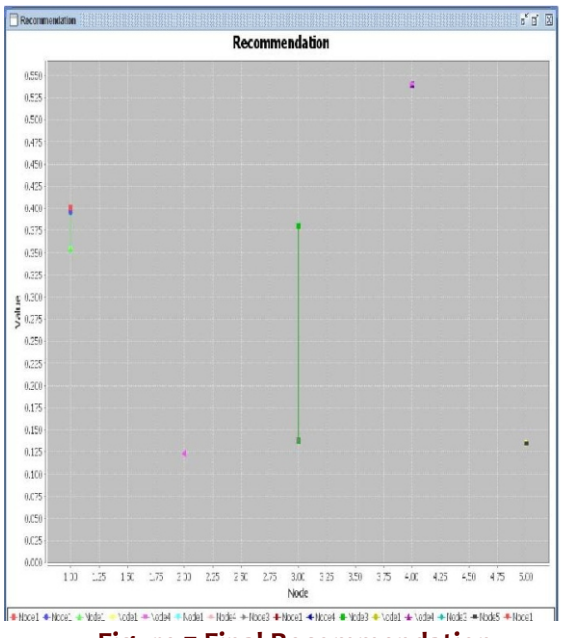

Figure 7 Final Recommendation

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Conclusion :

The 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 recommender's own experience, information from its acquaintances, and level of confidence in the recommendation. These parameters provided us a better assessment of trustworthiness. Individual, collaborative, and pseudonym changing attackers are studied in the experiments.Damage of collaboration and pseudospoofing is dependent to attack behavior. Although recommendations are important in hypocritical and oscillatory attackers, pseudospoofers, and collaborators, they are less useful in naive and discriminatory attackers. SORT mitigated both service and recommendation-based attacks in most experiments. However, in extremely malicious environments such as a 50 percent malicious network, collaborators can continue to disseminate large amount of misleading recommendations. Another issue about SORT is maintaining trust all over the network. 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. Using trust information does not solve all security problems in P2P systems but can enhance security and effectiveness of systems. If interactions are modeled correctly, SORT can be adapted to various P2P applications. e.g., CPU sharing, storage networks, and P2P gaming.

Future Enhancements:

Peer-to-peer (P2P) systems, peers often must interact with unknown or unfamiliar peers without the benefit of trusted third parties or authorities to mediate the interactions. A peer will need reputation mechanisms to incorporate the knowledge of others to decide whether to trust another party in P2P systems. This paper discusses the design of reputation mechanisms and proposes a novel distributed reputation mechanism to detect malicious or unreliable peers in P2P systems.

It illustrates the process for rating gathering and aggregation and presents some experimental results to evaluate the proposed approach. Moreover, it considers how to effectively aggregate noisy (dishonest or inaccurate) ratings from independent or collusive peers using weighted majority techniques. Furthermore, it analyzes some possible attacks on reputation mechanisms and shows how to defend against such attacks.

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]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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[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.

[11]Software Engineering By Pressmen.

[12]S. Marsh, "Formalising Trust as a Computational Concept," PhD thesis, Dept. of Math. and Computer Science, Univ. of Stirling,1994.

[13]A. Abdul-Rahman and S. Hailes, "Supporting Trust in Virtual Communities," Proc. 33rd Hawaii Int'l Conf. System Sciences (HICSS), 2000.

[14] B. Yu and M. Singh, "A Social Mechanism of Reputation Management in Electronic Communities," Proc. Cooperative Information Agents (CIA), 2000.

[15]L. Mui, M. Mohtashemi, and A. Halberstadt, "A Computational Model of Trust and Reputation for E-Businesses," Proc. 35thHawaii Int'l Conf. System Sciences (HICSS), 2002.

[16]Unified modeling language by Gradybooh.

[17]A. Jøsang, E. Gray, and M. Kinateder, "Analysing Topologies of Transitive Trust," Proc. First Int'l Workshop Formal Aspects in Security and Trust (FAST), 2003.

E. Terzi, Y. Zhong, B. Bhargava, Pankaj, and S. Madria, "An Algorithm for Building User-Role Profiles in a Trust Environment,"

[18]L. Mui, M. Mohtashemi, and A. Halberstadt, "A Computational Model of Trust and Reputation for E-Businesses," Proc. 35thHawaii Int'l Conf. System Sciences (HICSS), 2002.

[19]Y. Zhong, "Formalization of Dynamic Trust and Uncertain Evidence for User Authorization," PhD thesis, Dept. of Computer Science, Purdue Univ., 2004.

[20]D.H. McKnight, "Conceptualizing Trust: A Typology and E-Commerce Customer Relationships Model," Proc. 34th Ann. Hawaii Int'l Conf. System Sciences (HICSS), 2001.

[21]P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, "Reputation Systems," Comm. ACM, vol. 43, no. 12, pp. 45-48, 2000.

[22]Z. Despotovic and K. Aberer, "Trust-Aware Delivery of Composite Goods," Proc. First Int'l Conf. Agents and Peer-to-Peer Computing, 2002.

[23]A. Jøsang, R. Ismail, and C. Boyd, "A Survey of Trust and Reputation Systems for Online Service Provision," Decision Support Systems, vol. 43, no. 2, pp. 618-644, 2007.

[24]C. Dellarocas, "Immunizing Online Reputation Reporting Systems Against Unfair Ratings and Discriminatory Behavior," Proc. Second ACM Conf. Electronic Commerce (EC), 2000.

[25]B. Yu and M.P. Singh, "Detecting Deception in Reputation Management," Proc. Second Int'l Joint Conf. Autonomous Agents and Multiagent Systems, 2003.

[26]R. Guha, R. Kumar, P. Raghavan, and A. Tomkins, "Propagation of Trust and Distrust," Proc. 13th Int'l Conf. World Wide