ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Trustworthy Service Evaluation in Secure Self-Organizing Trust Model (SSORT) for Peer-To-Peer Service

Neetha Jose[1], Swapna.H[2]

M.Tech, Dept. of CSE, Marian Engineering College Trivandrum, Kerala, India[1]

Assistant Professor, Dept. of CSE, Marian Engineering College Trivandrum, Kerala, India[2]

ABSTRACT: Anonymous natures of the Peer-to-Peer networks are open to many malicious attacks. In a distributed environment without centralized server, providing security mechanism is more complicated than in central-server networks. Therefore security problems are one of the major challenges that need to be analysed, especially for decentralized systems. SORT (Self Organizing Trust Model) is used to isolate malicious peers by develops dynamic trust groups using the peers past information. Satisfaction, weight and fading effect are three parameters used to evaluate an interaction. Based on Service Trust Metric, Reputation Metric, and Recommendation Trust Metric are used to calculate trust metrics. In a Secure Self-Organizing Trust Model (SSORT), Sampling Scheme improves the performance of information collection from the acquaintances and that tries to determine the relevance of search results. By sampling, it avoids visiting all nodes in the vicinity of a peer and quickly collects information from the neighbourhood, thus improves the performance. In sampling process, it sends a query to one of its acquaintances randomly to select sample peers and evaluated acquaintances trustworthiness in the service history and to download a file from sample acquaintances. File sharing applications show that the SSORT can decrease misleading recommendation and maintaining trust all over the network in order to extend the trust. Using trust information's does not solve all security problems in P2P system but can improve security and effectiveness of the systems.

KEYWORDS: Trust management; Peer-to-Peer systems; Reputation system; Sampling approaches; Search process; SSORT; Query processing

I. INTRODUCTION

Peer-to-Peer (P2P) networks have many benefits over the client server approaches to data distribution. The central server defines trust metrics and manages trust information but in most P2P systems, peers organize themselves to manage trust metrics. The node have flexible roles and function at the same time as clients and servers. In a Self Organizing Trust Model (SORT) [16] is used to decrease malicious activity by establishing trust relations without using a priori information. Peers do not reflect opinions of all peers. In this way, good peers form dynamic trust groups about the peers interacted in the past and can isolate malicious activity. SORT defines three trust metrics. Service trust and recommendation trust are primary metrics to measure trustworthiness about the other peers. Service Trust Metric is used to calculated acquaintances trustworthiness in the service history. The recommendation trust metric is important when requesting recommendations. Reputation metric is calculated strangers trustworthiness based on recommendations. It is important when deciding about strangers and new acquaintances.

We propose a Secure Self-Organizing Trust Model (SSORT) that aims to efficiently collect information using sampling-based approaches. Random walks are used for a node to locate a resource. When a node wants to get a service, it sends a query to one of its acquaintances randomly and to search for good acquaintances based on the trustworthiness of the peer in the service context. Search method that tries to determine the relevance of search results by considering interactions. Random walks addressing topology maintains unstructured P2P networks, thus improves effectiveness and security of the system.

In SSORT offer performance improvements, via sampling, to the process of uniformly collecting information from past interactions. We introduce and analyse variants of these basic sampling schemes in which aim to minimize the total number of nodes in the network. We evaluate sampling in terms of accuracy and efficiency using real andsynthetic data. We show that basic sampling schemes can be utilized for a variety of strategies aiming to rank items

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

in a network, assuming that information for each peer in the network is available. The premise is that by collecting and analysing information from interactions of peers we can improve the accuracy of search results.

II. RELATED WORK

Malicious peers have more attack opportunities in P2P trust models due to lack of a central authority. A social mechanism of reputation management [1] aims at avoiding interaction with undesirable participants. Social mechanisms complement hard security techniques such as passwords and digital certificates. Social mechanisms are even more important when trusted third parties are not available. The recommendations by the personal agents [1] are based on a representation of how much the other parties can be trusted. The agents build and manage trust, to do so, the agents not only take into account the previous experiences of their users, but also communicate with other agents. Peer Trust [6] defines transaction and community context parameters to make trust calculation on P-Grid. In Aberer and Despotovic's trust model [2], peers report their complaints by using P-Grid mechanism [8]. It is an approach that addresses the problem of reputation-based trust management. A peer is assumed as trustworthy unless there are complaints about it. The principal advantage is that it has an efficient way of storing and retrieving trust data and does not flood every peer in the system with queries about other peers, thus limiting storage and bandwidth costs. Eigen Trust [5] uses transitivity of trust to calculate global trust values. In the distributed environment, peer i download a file from peer j, transaction as positive or negative. Peer i can store the number of satisfactory transaction with j sat (i,j) and number of unsatisfactory transactions with j unsat (i,j). Local trust value is the sum of the rating of the individual transactions. In order to aggregate local trust values, it is necessary to normalise them. It does not distinguish between a peer who not interact and who has poor experience.

Quantifying Trust [7] defines trust-domain model based security architecture for mobile ad-hoc networks ($MANET_S$) establish keys between nodes and defines trust metrics. To evaluate pair-wise trust as a combination of self trust and group trust and their model organizes nodes into trust-based clusters. This is also establishing trust in other parts of the network due to node mobility. It is used to design a comprehensive trust model for ad-hoc networks that can assure an admissible level of security through the use of trust. In PowerTrust system [11], a trust overlay network is build on the top of all peers in a P2P system. All peers evaluate each other, whenever a transaction takes place between a peer. Therefore all peers send local trust scores, these scores are input to the PowerTrust system. The system aggregates the local trust scores to calculate the global reputation score, which is the output of the PowerTrust system. The power-law findings in peer feedbacks, the Power Trust system [11] dynamically select a few power nodes that are most reputable by using a distributed ranking mechanism. The good reputation of power nodes is accumulated from the running history of the system. Like a democratic system, power nodes are dynamically replaceable, if they become less active or demonstrate unacceptable behaviour. GossipTrust system [12] computes global reputation scores of all nodes concurrently. GossipTrust is adapted to peer dynamics and robust to disturbance by malicious peers, the system as scalable, accurate, robust and fault-tolerant. These results are low aggregation overhead, storage efficiency, and scoring accuracy in unstructured P2P networks. Peers in NICE barter resources can be exchanging by transaction messages. A transaction message identifies sets of resources a principal is willing to barter. NICE is a platform for implementing cooperative distributed applications. Applications in NICE gain access to remote resources by bartering local resources. Transactions in NICE [10] consist of secure exchanges of resource certificates. These certificates can be redeemed for the named resources. Non-cooperative users may gain free access to remote resources by issuing certificates that they eventually do not redeem.

III. PROPOSED METHOD

A. *A SECURE SELF ORGANIZING TRUST MODEL (SSORT) FOR PEER TO PEER SYSTEM*

Peers are assumed to be strangers to each other at the beginning. After providing a service, e.g. uploading a file, a peer becomes an acquaintance of another peer. Creating long term trust relationships among peers can provide a more secure environment by reducing risk. By sampling avoid visiting all acquaintances nodes in services. It sends a query to one of its acquaintances randomly and select sample peers based on the randomwalks. And peer evaluated acquaintances trustworthiness in the service history and to download a file from sample acquaintances.
Based on these we focus on improving the performance of information collection in a network and make the following contributions:

- Sampling-based Schemes in a network quickly obtain sample of nodes in its acquaintances.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

- We introduce sampling schemes in which aim to minimize the total number of nodes in the network.
- We evaluate sampling-based algorithms in terms of accuracy and efficiency using real and synthetic data.

Sampling-Based Approaches

Random walks that obey tree structure. Let Dd (u) be the vicinity of a user u at depth d. Let G be a graph depicting connections between users in a network, where each node in the graph represents a user. This random walk procedure can be repeated n times to obtain a uniform random sample of the nodes in Dd (u) of size n. After we have done n independent random walks, we will have collected n leaves i.e., the set of n leaves is a random sample of the set of N nodes. Consider query q is submitted to a search engine by a user u. Search algorithm would try to personalize this result and collect information from u's network and use this information to rank the results according to acquaintances trustworthiness in the service history. Our research suggests methods for quickly collecting information from the acquaintances in a network when knowledge not available.

A random walk starts at user and ends either when a self-link is followed, a link that connects a node with itself or when a node in depth has been reached. As the random walk progresses, state information is maintained regarding previous walks and visited nodes that ensures the random walk obeys structural properties of a tree. Once a node has been reached it is selected to the sample.

IV. SIMULATION RESULTS

Secure Self ORganizing Trust Model (SSORT) is developed using real time systems. Trust values are calculated based on the equations specified. Non trusted peers are not participating in the file sharing application. The proposed method has been compared with existing method based on parameters. Those parameters are time and number of samples in the node (Sample size). In existing system, all acquaintances are selected for search method. But in the proposed method selects only samples. Graphical results show that comparing to the existing trust management systems, proposed sampling method takes lesser time for searching. Sampling approaches reduces the time require for searching compare to the existing method.

.

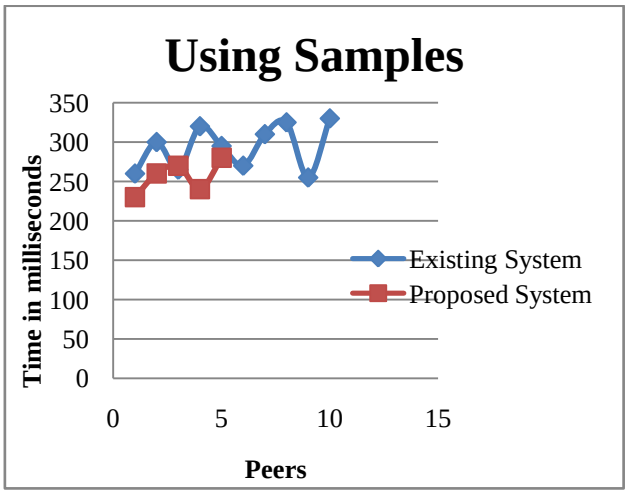

Fig.1. Time taken by two methods to search peers

The no. of peers by the existing method is large and it takes all acquaintances after providing services. Also it is seen that the number of peers taken by the proposed method is lesser than the existing method. Sampling scheme takes less sample nodes and hence use lesser time. Hence the proposed sampling method is efficient than the existing method, thus improved performance of the system.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

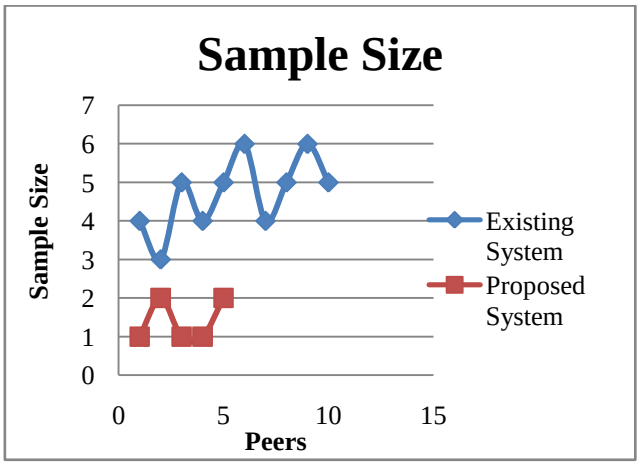

Fig.2. No. of peers taken by the existing and proposed sampling method

V. CONCLUSION AND FUTURE WORK

Open nature of peer-to-peer systems exposes them to malicious activity. Building trust relationships among peers can mitigate attacks of malicious peers. Reputation based trust management is used to promote honest and cooperative behaviours. Various methods for trust management in peer to peer systems have been compared. Structured network rely on a DHT structure to store trust information. Each peer becomes a trust holder of another peer, which is assumed to provide authentic global trust information. In a Secure Self-Organizing Trust Model (SSORT), improves the performance of information collection from the neighbourhood of the network. Using sampling approaches, Randomwalks quickly approximate the user's neighbourhood and minimize the total number of nodes in the network. It sends a query to one of its acquaintances randomly and select sample peers. And peer evaluated acquaintances trustworthiness in the service history and to download a file from sample acquaintances. In this way search method that tries to determine the relevance of search results by considering interactions in the service context and thus to improved performance. A number of issues in peer to peer systems for future studies remain open. First, more extensive evaluation methods over wider parameters are needed for trust computations, thus improve security. Second, robust methods are needed to avoid the malicious peers. Therefore, various contexts of trust can be defined to improve security of P2P systems. Another issue is maintaining trust all over the network. If a peer changes its point of attachment, it might lose a part of its trust network. Using trust information's does not solve all security problems but can enhance security and effectiveness of systems.

REFERENCES

1. B. Yu and M. Singh, "A Social Mechanism of Reputation Management in Electronic Communities," Proc. Cooperative Information Agents (CIA), 2000.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. M. Virendra, M. Jadliwala, M. Chandrasekaran, and S. Upadhyaya, "Quantifying Trust in Mobile Ad-Hoc Networks," Proc. IEEE Int'l Conf. Integration of Knowledge Intensive Multi-Agent Systems (KIMAS), 2005.
8. K. Aberer, A. Datta, and M. Hauswirth, "P-Grid: Dynamics of Self- Organization Processes in Structured P2P Systems," Peer-to-Peer Systems and Applications, vol. 3845, 2005.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

9. Z. Liang, and W. Shi, "PET: A PErsonalized Trust Model with Reputation and Risk Evaluation for P2P Resource Sharing," *Proc. 38th Ann.Hawaii Int'l Conf. System Sciences*, IEEE CS Press, 2005, pp. 201.2.
10. R. Sherwood, S. Lee, and B. Bhattacharjee, "Cooperative Peer Groups in Nice," Computer Networks, vol. 50, no. 4, pp. 523-544, 2006.
11. R. Zhou and K. Hwang, "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, Apr. 2007
12. 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.
13. P. Victor, C. Cornelis, M. De Cock, and P. Pinheiro da Silva, "Gradual Trust and Distrust in Recommender Systems," Fuzzy Sets Systems, vol. 160, no. 10, pp. 1367-1382, 2009.
14. K. Hoffman, D. Zage, and C. Nita-Rotaru, "A Survey of Attack and Defense Techniques for Reputation Systems," ACM ComputingSurveys, vol. 42, no. 1, pp. 1:1-1:31, 2009.
15. Behrooz Shafiee Sarjaz Maghsoud Abbaspour,"BitTorrent using a new reputation-based trust management system" , Springer Science+Business Media Sept. 2012
16. Ahmet Burak Can, Member, IEEE, and Bharat Bhargava, Fellow, IEEE, SORT: A Self- Organizing Trust Model for Peer-to-Peer Systems, IEEE Transactions on Dependable and Secure Computing, vol. 10, NO. 1, Feb. 2013.