International Journal of Scientific Research in Computer Science and Engineering **Research Paper**
Vol.5, Issue.6, pp.54-57, December (2017) **E-ISSN:** 2320-7639

Peer 2 Peer System Using Sort

V. V.Sharma [1*], R. B. Wagh [2]

[1*]Computer Engineering, R.C.Patel Institute of Technology, North Maharashtra University, Shirpur, India
[2] Computer Engineering, R.C.Patel Institute of Technology, North Maharashtra University, Shirpur, India

**Corresponding Author: vickyvsharma1989@gmail.com*

Available online at: www.isroset.org

Received: 16/Nov/2017, Revised: 28/Nov/2017, Accepted: 20/Dec/2017, Published: 31/Dec/2017

***Abstract*—** Peer 2 peer system act as both clients as well as server. This system exposes them to malicious activity. Without central server this system can share their files between them easily. To decrease the attacks of malicious peer the system builds trust between each other. A good peer always gives fair recommendations after uploading authentic files. Both service as well as recommendation attacked performed by malicious peer. Both service based attack as well as recommendation based attack are detect by Self Organizing Trust Model (SORT). To learn trust information of other peer, Peer send query to other peer that interacted in past. Any peer wants to download or upload file from another peer. So peer get recommendation from other node, Peer decides that the node is good or malicious based on recommendation. Peer does not interact with node if it is found malicious but also separate the malicious node from the network. If node found good peer then both can interact with each other. A separate history of interactions for each acquaintance is stored by peer.

***Keywords*—**peer to peer system, trust, management, reputation, security

I. INTRODUCTION

Peer-to-peer systems rely in work together to achieve a task. A peer-to-peer system exposes them to malicious activity due to the open nature. Mitigate attack of malicious peer due to a trust relationships between peers. This paper presents distributed algorithms so peer can make trust on other peers based on past interaction and recommendations. Local information helps peers to create their own trust network in their proximity and peer don't try to learn global trust information. Trustworthiness not only in providing services but also giving recommendations are measured by two contexts of trust, service, and recommendation contexts.

Interactions and recommendations between peers are evaluated based on importance, recentness, and their satisfaction parameters[2].A file sharing application show that the proposed model can reduce attacks on 16 different malicious behavior models due to this peer were able to form trust relationship in their proximity and isolate malicious peer. Malicious activity is a threat for security of P2P systems. Peers can provide both a more secure environment and creating long-term trust relationships among peers by reducing risk and uncertainty in future P2P interactions. In malicious environment, establishing trust in an unknown entity is difficult. Need of metrics to represent trust in computational models because trust is a social concept and hard to measure with numerical values. In most cases, Classifying peers as trustworthy or untrustworthy is not sufficient. Peers can be ranked according to trustworthiness if metrics should have precision. Interactions with a peer provide certain information and feedbacks might contain deceptive information to measure trust among peers.

A central server is a preferred way to store and manage trust information in the presence of an authority. Management of trust information is reliant for the structure of P2P network. Managing trust is a problem of particular importance in peer-to-peer environments where one frequently encounters unknown agents [2].The central server securely stores trust information and defines trust metrics. Peer store and mange trust information about each other because there is no central server in most P2P, Existing methods for trust management that are based on reputation focus on the semantic properties of the trust model, In this paper an approach that addresses the problem of reputation-based trust management at both the data management and the semantic level [3],[4]. Trust information management is depend to the structure of P2P network. In peer to peer environment when one frequently meet unknown agents there is a problem to managing trust. Rely on a central databases or require maintaining global knowledge they don't scale at each agent to provide data on earlier interactions. By computing an agents reputation from its former interactions with other agents, We employ at both levels not only scalable data structures but also algorithms that require both no central control as well as allow assessing trust. Managing trust relationships in p2p systems have no well defined methods. The Distributed hash table based approaches are suited for structured p2p networks only. P2p nature collapse due to some of the existing methods introduce central authority in p2p networks. Complex and very large data structures that represent a kind of global knowledge about the whole network must keep by every agent.

Based on past interactions and recommendations, distributed algorithms enable a peer to reason about trustworthiness of other peers. Peers create their own trust network by using local information and do not try to learn global trust information. Establishing trust relations among peers, Self-Organizing Trust model (SORT) that aims to decrease malicious activity in a P2P system. In SORT, in beginning each peer are stranger to another peer and become acquaintance after providing a service e.g upload a file. Peer chooses a trust strangers when it has no acquaintance. If stranger are equally trustworthy, an acquaintance is always preferred them. Using peer's service is an interactions as abased on weight, recentness of the interaction and satisfaction of the requester. Peer get feedback from an acquaintance .Recommendation which based on recommender's trust worthiness. Recommender's own experience about peer not only the information collected from the recommender's acquaintances but also recommender's level of confidence in the recommendation. If less trustworthiness of the recommender because of low value in evaluation this all are depend on the low level of confidence. Three trust mertices are defined by SORT. Recommendations calculate reputation metric while deciding about strangers and new acquaintances. Reputation decreases its importance as experience with an acquaintance increases. Both are primary metrics Service trust and recommendation trust to measure trustworthiness in the service and recommendation contexts, respectively.

While selecting service provider service trust is used and at the time of requesting recommendations recommendation trust metric is important. To calculate the reputation metric, recommendations are based on the recommendation trust metric.

The organization of the paper is as follows, Section I contains the survey on peer to peer system using self organizing trust model, Section II contain the related works on p2p system,Section III contain the methodology of p2p using SORT model,Section IV contain the conclusion & the future work to improve the performance in p2p system.

II. RELATED WORK

Sinju and Felsy et al. [5] proposed that downloading a file is an interaction. Uploader means a file sharing by peer. Abdul-rahman and Hailes [6] evaluate not only trust in a discrete domain as an aggregation of direct experience but also recommendations of other parties. Test to measure recommendation accuracy they define semantic distance. Yu and Singh's model propagates the trust information through referral chains. Referrals are the primary method of developing trust in the others. Mui et al. [7] propose a statistical model based on trust, reputation, and reciprocity concepts. Reputation is propagated during multiple referral chains. Jøsang et al. [8] 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. [9] introduce an algorithm to classify users and assign them roles based on trust relationships. Building trust relationships and uncertain evidences are evaluated with second-order probability as well as Dempster - Shaferian framework.

In e-commerce platforms like eBay, Amazon, depends on building trust method widely used by reputation systems. New customers used previous customer feedback information for shopping which is collected by central authority. Despotovic and Aberer [10] point out that trust-aware exchanges can increase economic activity since some exchanges may not happen without trust. Yu et al. [11] and Tran et al. [12] propose techniques based on the observation that there are rarely trust relationship with real users otherwise fake entities generally have many trust relationships among each other. There are extra challenges occurs by compare e-commerce platforms with P2P Trust models systems. P2p trust model have no central authority so malicious peers have more opportunities to attack. Hoffman et al. [13] discuss five common attacks in P2P trust models: self-promoting, white-washing, slandering, orchestrated, and denial of service attacks. They point out that defense techniques in trust models are dependent to P2P system architecture. Decentralized and efficient access to trust information provided by a DHT structure.

In Aberer and Despotovic's trust model [3], peers report their complaints by using P-Grid [14]. There are complaint about peer if it does not assumed as trustworthy. Eigentrust and Peer trust evaluate a recommendation based on trustworthiness of the recommender. Recoomender's trustworthiness helps to Eigentrust and Peer trust to evaluate a recommendation. SORT instead of considering information from all acquaintances, having trust holder's feedback like authentic and public opinion.To make decisions peers develop their own trust networks is better than considering global trust information, local trust information. If there are enough neighbors then A reputation query is sent to them otherwise the query is flooded to network. Some neighbors have a query which is send randomly to them,so others Reputation query traffic is reduces by comparing with flooding approach and gossiping. In SORT, Peers send reputation queries to each other if only if they have interacted in past otherwise no quries send to peers, it helps decrease network traffic.

III. Methodology

Peer Creation

In SORT, peer are strangers to each other at the beginning, after providing a service peers becomes an acquaintance to each other. Trust stranger chosen by peer if that peer have no acquaintances. To understand SORT, then it is necessary to implement a peer to peer file sharing simulation.

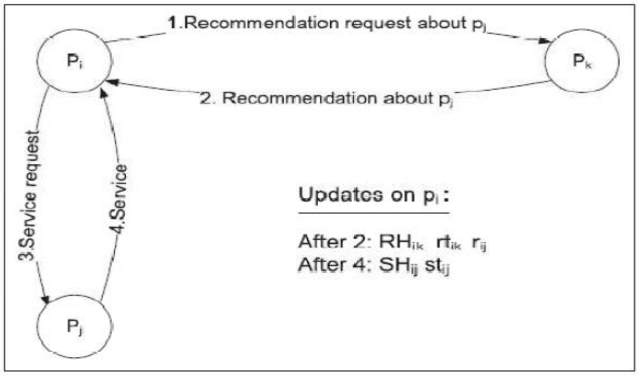
1.Recommendation request about p_j
P_i
P_k
2. Recommendation about p_j
3.Service request
4.Service
Updates on p_i :
After 2: RH_{ik} rt_{ik} r_{ij}
After 4: SH_{ij} st_{ij}
P_j

Fig 1.operations when receiving a recommendation & having an interaction.

Upload Process

Any peer upload a file and it is update to all other peer. File contain name, up-loader name with IP address stored continuously. So if any peer need that can download at any time it easily.

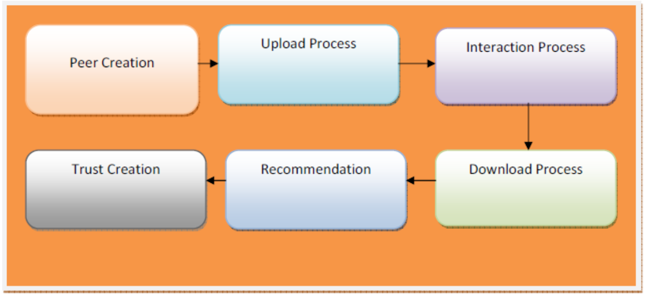

Fig 2.block diagram for trust creation.

Interaction Process

Peer cannot directly download any file before download a file that peer must request for that file to the up-loader with full details e.g. file name etc. The up-loader receive request and then starts the process. If the up-loader sends the file, then the file can downloaded only by the requested peer. No peer can download the file without up-loader permission.

Recommendation Model

The recommendation to other peers is depend on the service or up-loader. A peer may act good service provider but may be a bad recommender or vice versa. SORT uses different tasks such as service and recommendation, past interactions and recommendation's history information stored histories to assess competence and integrity of acquaintances. Information collected from the recommender's acquaintances, and the recommender's level of confidence in the recommendation. The following algorithm helps in SORT.

IV. Conclusion and Future Scope

In this paper a peer can develop a trust network in its nearness due to presence of trust model for peer to peer. Relation with good peers separate malicious peer around itself. To measure capability of peers not only in providing services but also in giving recommendations two contexts of trust, service and recommendation are defined. This implemented work delivers better security for peer to peer system. Interactions and recommendations are measured with satisfaction, time and bandwidth. This method satisfies on earlier methods. In future trust can enhance security and effectiveness of systems but does not solve all security problems. SORT can be modified to various P2P systems, If interactions are demonstrated correctly.

In this paper, SORT useful to reduce malicious peer attacks but may not be more effective in hypocritical cases. GenTrust may be more effective to reduce malicious attacks in hypocritical cases.

References

[1] Ahmet Burak Can and Bharat,"A Self-Organizing Trust Model for Peer-to-Peer Systems"IEEE Trans.Dependable and Secure Computing,vol 10, No.1, 2013.

[2] J. U. Duncombe, "Infrared navigation—Part I: An assessment of feasibility," IEEE Trans. Electron Devices, vol. ED-11, pp. 34-39, Jan. 1959

[3] Aberer.K and Despotovic.Z "Managing Trust in a Peer-2-Peer Information System" Proc. 10th Intl Conf. Information and Knowledge Management (CIKM), (2001),.

[4] Kamvar.S, Schlosser.M, and Garcia-Molina.H,,The (Eigentrust) Algorithm for Reputation Management in P2P Networks" Proc. 12th World Wide Web Conf. (WWW), ,(2003).

[5] R.S.Sinju and C.Felsy, " Managing Trust Relationship in Peer to Peer System" vol.2,Issue-2,pp-29-36,April-June 2014.

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

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

[8] 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.

[9] E. Terzi, Y. Zhong, B. Bhargava, Pankaj, and S. Madria, "An Algorithm for Building User-Role Profiles in a Trust Environment," Proc. Fourth Int'l Conf. Data Warehousing and Knowledge Discovery (DaWaK), vol. 2454, 2002

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

[11] H. Yu, M. Kaminsky, P.B. Gibbons, and A. Flaxman, "Sybilguard: Defending against Sybil Attacks via Social Networks," ACM

SIGCOMM Computer Comm. Rev., vol. 36, no. 4, pp. 267-278, 2006.

[12] N. Tran, B. Min, J. Li, and L. Subramanian, "Sybil-Resilient Online Content Voting," Proc. Sixth USENIX Symp. Networked Systems Design and Implementation (NSDI), 2009.

[13] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A Survey of Attack and Defense Techniques for Reputation Systems," ACM Computing Surveys, vol. 42, no. 1, pp. 1:1-1:31, 2009.

[14] 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.

Authors Profile

Mr.R. B. Wagh passed B.E from Amravati University, Amravati and Master of Enginnering from RGPV University,Bhopal,India. He is currently pursuing Ph.D. and currently working as Associate Professor in Department of Computer Engineering in R.C.Patel Institute of Technology,Shirpur,India.He has published more than 30 research papers in reputed International journals.

Mr V. V. Sharma passed Bachelor of Engineering in 2012 from North Maharashtra University, Jalgaon and pursuing Master of Engineering from North Maharashtra University, Jalgaon . His area of interest is JAVA , Soft Computing. He is presently a PG student at R.C. Patel Institute of Technology, Shirpur