International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 3, Issue 8, August 2014 **ISSN 2319 - 4847**

A Self-ORganizing Trust Model with Peer Acquaintance

S. V. Shirke[1], R. S. Chaure[2]
[1]University of Pune, P. k. technical campus, Chakan, Pune, India
[2]University of Pune, P. k. technical campus, Chakan, Pune, India

Abstract

In this paper problem with system is 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. So we solve this issue in our proposed system, here we assign particular id to peer node which maintain by server. So if that node goes out of network, still when it again attach to network whole data information loaded to that node so we can get trustworthiness. Open nature of peer-to-peer systems exposes them to malicious activity. Building trust relationships among peers can mitigate. In the experiments, good peers were able to form trust relationships in their proximity and isolate malicious peers. Peers are equal in computational power and responsibility. There are no privileged, centralized, or trusted peers to manage trust relationships. Peers occasionally leave and join the network. A peer provides services and uses services of others. For simplicity of discussion, one type of interaction is considered in the service context, i.e., file download. 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.

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

1. INTRODUCTION

Peer-to-peer (P2P) systems rely on collaboration of peers to accomplish tasks of performing malicious activity is a threat for security of P2P systems. Creating long-term trust relationships among peers can provide a more secure environment by reducing risk and uncertainty in future P2P interactions. Furthermore, trust is a social concept and hard to measure with numerical values. Metrics are needed to represent trust in computational models. Classifying peers as either trustworthy or untrustworthy is not sufficient in most cases. Metrics should have precision so peers can be ranked according to trustworthiness. A trust query is either flooded to the network or sent to neighborhood of the query initiator. Generally, calculated trust information is not global and does not reflect opinions of all peers. The presence of an authority, a central server is a preferred way to store and manage trust information, e.g., eBay. The central server securely stores trust information and defines trust metrics. Since there is no central server in most P2P systems, peers organize themselves to store and manage trust information about each other [1], [2]. Management of trust information is dependent to the structure of P2P network. In distributed hash table (DHT)- based approaches, each peer becomes a trust holder by storing feedbacks about other peers . Global trust information stored by trust holders can be accessed through DHT efficiently. In unstructured networks, each peer stores trust information about peers in its neighbourhood or peers interacted in the past . A peer sends trust queries to learn trust information of other peers. A trust query is either flooded to the network or sent to neighborhood of the query initiator. Generally, calculated trust information is not global and does not reflect opinions of all peers. 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. No a priori information or a trusted peer is used to leverage trust establishment. Peers do not try to collect trust information from all peers. Each peer develops its own local view of trust about the peers interacted in the past. In this way, good peers form dynamic trust groups in their proximity and can isolate malicious peers. Since peers generally tend to interact with a small set of peers [7], forming trust relations in proximity of peers helps to mitigate attacks in a P2P system. In SORT, peers are assumed to be strangers to each other at the beginning. A peer becomes an acquaintance of another peer after providing a service, e.g., uploading a file. If a peer has no acquaintance, it chooses to trust strangers. An acquaintance is always preferred over a stranger if they are equally trustworthy. Using a service of a peer is an interaction, which is evaluated based on weight (importance) and recentness of the interaction, and satisfaction of the requester. 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. No a priori information or a trusted peer is used to leverage trust establishment. Peers do not try to collect trust information from all peers. Each peer develops its own local view of trust about the peers interacted in the past. In this way, good peers form dynamic trust groups in their proximity and can isolate malicious peers. Since peers generally tend to interact with a small set of peers, forming trust relations in proximity of peers helps to mitigate attacks in a P2P system. In SORT, peers are assumed to be strangers to each other at the beginning. A peer becomes an acquaintance of another peer after providing a service, e.g., uploading a file. If a peer has no acquaintance, it chooses to trust strangers. An acquaintance is always preferred over a stranger if they are equally trustworthy. Using a service of a peer is an interaction, which is evaluated based on weight (importance) and recentness of the interaction, and satisfaction

of the requester. An acquaintance's feedback about a peer, recommendation, is evaluated based on recommender's trustworthiness. It contains the recommender's own experience about the peer, information collected from the recommender's acquaintances, and the recommender's level of confidence in the recommendation. If the level of confidence is low, the recommendation has a low value in evaluation and affects less the trustworthiness of the recommender. An acquaintance's feedback about a peer, recommendation, is evaluated based on recommender's trustworthiness. It contains the recommender's own experience about the peer, information collected from the recommender's acquaintances, and the recommender's level of confidence in the recommendation. If the level of confidence is low, the recommendation has a low value in evaluation and affects less the trustworthiness of the recommender. In next section II we are presenting the literature survey over the various methods presented for SORT. In section III, the proposed approach and its system block diagram is depicted. In section IV we are presenting the current state of implementation and results achieved. Finally conclusion and future work is predicted in section V.

2. LITERATURE REVIEW

Several researchers have done the Annotating Search Results from Web Databases Following are some of them, K. Aberer and Z. Despotovic, [1] in this paper they have identified the questions to be ad- dressed when trying to find a solution to the problem of trust assessment based on reputation management in a decentralized environment. They have introduced and analyzed a simple, yet robust method that shows that a solution to this problem is feasible. Having introduced our approach, allows us to provide a more detailed comparison to related approaches. A.A. Selcuk, E. Uzun, and M.R. Pariente,[3] in this paper the open and anonymous nature of a P2P network makes it an ideal medium for attackers to spread malicious con- tent. In this paper, they describe a reputation-based trust management protocol for P2P networks where user s r ate the reliability of Parties the y deal with, and share this in- formation with their peer s. The protocol helps establishing trust among good peer s as well as identifying the malicious ones J. Kleinberg, [4] in this paper Algorithmic work in different settings has considered the problem of routing with local information; see for example the problem of designing compact Routing tables for communication networks and the problem of robot navigation in an unknown environment. Our results are technically quite different from these; But they share the general goal of identifying qualitative e properties of net works that Makes routing with local information tractable, and offering a model for reasoning about Effective routing schemes in such networks. S. Kamvar, M. Schlosser, and H. Garcia-Molina,[2] in this paper presented a method to minimize the impact of malicious peers on the performance of a P2P system. The system computes a global trust value for a peer by calculating the left principal eigenvector of a matrix of normalized local trust values, thus taking into consideration the entire system's history with each single peer. We also show how to carry out the computations in a scalable and distributed manner. In P2P simulations, using these trust values to bias download has shown to reduce the number of in- authentic files on the network under a variety of threat scenarios. Furthermore, rewarding highly reputable peers with better quality of service incents non-malicious peers to share more files an d to self-police their own file repository for inauthentic files. In e-commerce platforms, reputation systems are widely used as a method of building trust, e.g., eBay, Amazon, and Epinions. A central authority collects feedbacks of past customers, which are used by future customers in shopping decisions. Resnick et al. [17] discuss that ensuring long-lived relationships, forcing feedbacks, checking honesty of recommendations are some difficulties in reputation systems. Despotovic and Aberer [18] point out that trust-aware exchanges can increase economic activity since some exchanges may not happen without trust. Jsang et al. [19] indicate that reputation systems are vulnerable to incorrectAnd bogus feedback attacks. Thus feedback ratings must be based on objective criteria to be useful. Dellarocas [20] proposes controlled anonymity and cluster filtering methods as countermeasures to unfairly high/low ratings and discriminatory seller behavior attacks. Yu and Singh [21] present a weighted majority algorithm against three attacks on reputation: complementary, exaggerated positive/negative feedbacks. Guha et al. [22] use trust and distrust concepts in a discrete domain. Their results on Epinions web site's data show that distrust is helpful to measure trustworthiness accurately. Reputation systems are vulnerable to sybil attacks [23], where a malicious entity can disseminate bogus feedbacks by creating multiple fake entities. To defend against Sybil attacks, Yu et al. [24] and Tran et al. [25] propose techniques based on the observation that fake entities generally have many trust relationships among each other but they rarely have relationships with real users. Some trust models use signed credentials to store trust information. Ooi et al. propose that each peer stores its own reputation using signed certificates. When a peer needs to know about a stranger, it requests certificates of the stranger. NICE uses signed cookies as a proof of good behavior. Peers dynamically form trust groups to protect each other. Peers in the same group have a higher trust in each other. Trust-based pricing and trading policies help to protect integrity of groups. Using signed credentials eliminates the need for reputation queries but ensuring validity of trust information in credentials is a problem. If a peer misbehaves after collecting good credentials, it is hard to revoke credentials without using a central authority. Furthermore, a public-key infrastructure is generally needed. How to evaluate interactions and how to define trust metrics are important problems in trust models. Wang and Vassileva [11] propose a Bayesian network model which uses different aspects of interactions on a P2Pfile sharing application. Victor et al. [12] define trust and distrust metrics. A nonzero distrust value lets an agent to distinguish an untrusted user from a new user. A lattice structure with trust and knowledge axis is used to model various trusting conditions. Swamynathan et

al. [13] decouple trust metric son service and recommendation contexts to assess trust-worthiness better. Creating contexts of trust can be helpful to address issues in various domains. Gupta et al. [14] use reputation as a currency. A central agent issues money to peers in return for their services to others. This money can be used to get better quality of service. Bhargava et al. [15] discusses trading privacy to gain more trust in pervasive systems. In another interesting study, Virendraetal. [16] Use trust concept in mobile ad-hoc networks to establish keys among nodes and group nodes into domains. Trustworthiness is measured according to lost and misrouted packets. Trust establishment phases are defined for starting up new nodes, maintaining trust of old peers, and reestablishing trust in malicious nodes. In SORT, to evaluate interactions and recommendations better, importance, recentness, and peer satisfaction Para-meters are considered. Recommender's trustworthiness and confidence about recommendation are considered when evaluating recommendations. Additionally, service and recommendation contexts are separated. This enabled us to measure trustworthiness in a wide variety of attack scenarios. Most trust models do not consider how interactions' are rated and assume that a rating mechanism exists. In this study, we suggest an interaction rating mechanism on a file sharing application and consider many real-life parameters to make simulations more realistic

3. PROPOSED ALGORITHM

1. $\mu_{rt} \Leftarrow \frac{1}{|A_i|} \sum_{p_k \in A_i} rt_{ik}$
2. $\sigma_{rt} \Leftarrow \frac{1}{|A_i|} \sqrt{\sum_{p_k \in A_i} (rt_{ik} - \mu_{rt})^2}$
3. $th_{high} \Leftarrow 1$
4. $th_{low} \Leftarrow \mu_{rt} + \sigma_{rt}$
5. $rset \Leftarrow \emptyset$
6. while $\mu_{rt} - \sigma_{rt} \leq th_{low}$ and $|rset| < \eta_{max}$
for all $p_k \in A_i$ do
if $th_{low} \leq rt_{ik} \leq th_{high}$ then
$rec \Leftarrow (p_k, p_j) rset \Leftarrow rset \cup \{rec\}$
end If
end for
$th_{high} \Leftarrow th_{low}$
$th_{high} \Leftarrow th_{low} - \sigma_{rt} / 2$
end while
7. return rset.

4. EXPERIMENTAL ANALYSIS

Objectives of Experiments: Experiments will be performed to understand how SORT is successful in mitigating attacks on a file sharing application. Distribution of trust metrics will be examined to understand if malicious peers are isolated from other peers. If a malicious peer is successful in a scenario, the reasons will be investigated. How recommendations are (or not) helpful in correctly identifying malicious peers is a question to be studied.

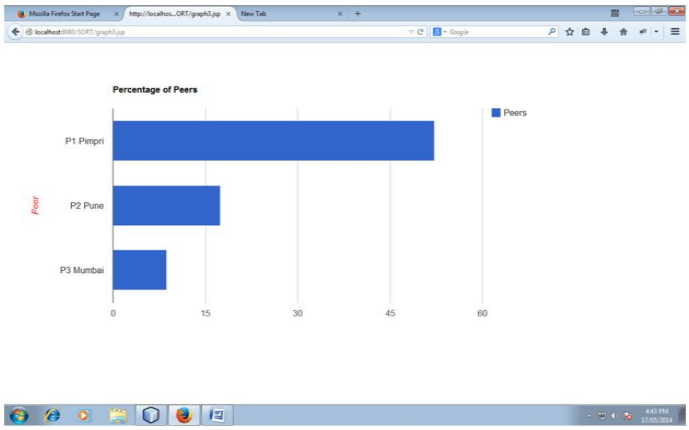

Fig.1 Peer wise user feedback percentage

In this section we has output screen of work done.fig1 shows output screen for the percentage of peer which has show peer wise user feedback percentage.

5. CONCLUSION AND FUTURE WORK

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. 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. Defining application specific context of trust and related metrics can help to assess trustworthiness in various tasks

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] 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.
[3] 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.
[4] J. Kleinberg, "The Small-World Phenomenon: An Algorithmic Perspective," Proc. 32nd ACM Symp. Theory of Computing, 2000.
[5] 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.
[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] 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.
[9] Z. Despotovic and K. Aberer, "Trust-Aware Delivery of Composite Goods," Proc. First Int'l Conf. Agents and Peer-to-Peer Computing, 2002.
[10] B. Yu and M.P. Singh, "Detecting Deception in Reputation Management," Proc. Second Int'l Joint Conf. Autonomous Agents and Multiagent Systems, 2003.
[11] Y. Wang and J. Vassileva, "Bayesian Network Trust Model inPeer-to-Peer Networks," Proc. Second Workshop Agents and Peer-to-Peer Computing at the Autonomous Agents and Multi Agent Systems Conf. (AAMAS), 2003.
[12] 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.
[13] G. Swamynathan, B.Y. Zhao, and K.C. Almeroth, "Decoupling Service and Feedback Trust in a Peer-to-Peer Reputation System," Proc. Int'l Conf. Parallel and Distributed Processing and Applications(ISPA), 2005.
[14] M. Gupta, P. Judge, and M. Ammar, "A Reputation System for Peer-to-Peer Networks," Proc. 13th Int'l Workshop Network and Operating Systems Support for Digital Audio and Video (NOSSDAV),2003.
[15] S. Staab, B. Bhargava, L. Lilien, A. Rosenthal, M. Winslett, M.Sloman, T. Dillon, E. Chang, F.K. Hussain, W. Nejdl, D. Olmedilla,and V. Kashyap, "The Pudding of Trust," IEEE Intelligent Systems, vol. 19, no. 5, pp. 74-88, 2004.
[16] M. Virendra,M. Jadliwala, M. Chandrasekaran,and S. Upadhyaya, "Quantifying Trust in Mobile Ad-Hoc Networks," Proc.IEEE Int'l Conf. Integration of KnowledgeIntensive Multi-AgentSystems (KIMAS), 2005.
[17] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, "Reputation Systems," Comm. ACM, vol. 43, no. 12, pp. 45-48, 2000.
[18] Z. Despotovic and K. Aberer, "Trust-Aware Delivery of Composite Goods," Proc. First Int'l Conf. Agents and Peer-to-Peer Computing, 2002.
[19] 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.
[20] C. Dellarocas, "Immunizing Online Reputation Reporting Systems Against Unfair Ratings and Discriminatory Behavior," Proc. Second ACM Conf. Electronic Commerce (EC), 2000.

[21] B. Yu and M.P. Singh, "Detecting Deception in Reputation Management," Proc. Second Int'l Joint Conf. Autonomous gents and Multiagent Systems, 2003.
[22] R. Guha, R. Kumar, P. Raghavan, and A. Tomkins, "Propagation of Trust and Distrust," Proc. 13th Int'l Conf. World Wide Web (WWW), 2004.
[23] J. Douceur, "The Sybil Attack," Proc. First Int'l Workshop Peer- o- Peer Systems (IPTPS), 2002.
[24] 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.
[25] N. Tran, B. Min, J. Li, and L. Subramanian, "Sybil-Resilient nline Content Voting," Proc. Sixth USENIX Symp. Networked Systems Design and Implementation (NSDI), 2009.

AUTHOR

S. V. Shirke received the B.E. degree in Computer Engineering from University of Pune in Cummins College of Engineering for women. During 2009-2012 and pursuing M.E. degrees in Computer Engineering from University of Pune in P. K. Technical Campus.

R. S. Chaure assistant professor P. K. Technical Campus, Chakan, Pune.