A Trust Management for Peer 2 Peer Information Systems

Suraj Suryawanshi
(M. Tech. Computer Science and Engineering, Rajiv Gandhi Institute of Technology, Bengaluru)

Pavan Gujjar Panduranga Rao
(Research Scholar, CSSE Department, Andhra University, Vishakapatanam, Andhra Pardesh)

Abstract- Due to the open nature of P2P system exposes them to malicious activity. P2P system means computer in the system can act as both client and server. In a P2P network, the peers are computer systems which are connected to each other via the internet. Files can be shared directly between systems on the network without the need of a central server. Building trust relationships among peers can decrease the attacks of malicious peers. A good peer uploads reliable files and gives fair recommendations. A peer's trustworthiness is evaluated by considering provided services and given recommendations with service and recommendation contexts .A malicious peer performs both service and recommendation-based attacks. Uploading a virus infected (or) an inauthentic file is a service based attack. Self-Organizing Trust Model (SORT) detects the service based attack and recommendation based attack. If one peer wants to upload/download file from another peer means peer will send the query to peer that interacted in the past for learn the trust information of other peers. So, neighboring node will give the recommendation to peer. Based on the recommendation only Peer decides whether the node is good (or) malicious. Find the node is malicious node means peer will not interact with malicious node. Isolate the malicious node from the network. Find the node is good means peer interact with good pee Peer stores a separate history of interactions for each Acquaintance.. Experiments on file sharing application demonstrate that peers with the highest trust value are considered and build the trust model in their contiguity and insulate malignant peers.

Index Terms- Peer-to-peer systems, trust management, reputation, security.

I. INTRODUCTION

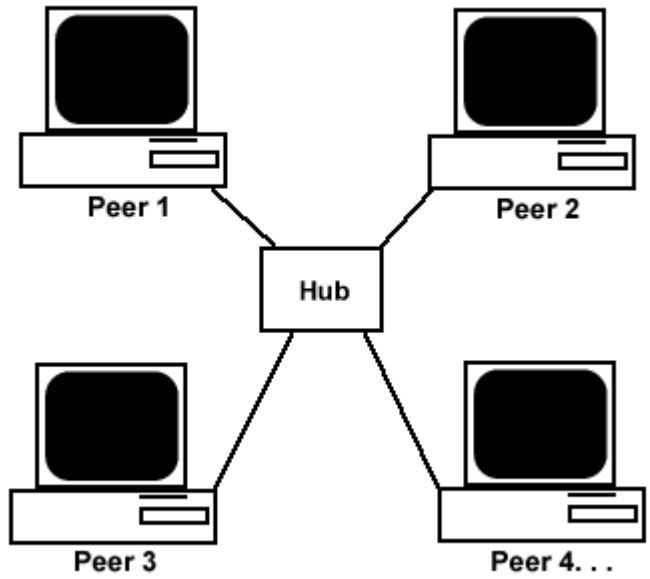
P2p computing is the sharing of computer resources and services by direct exchange between systems.[1]These resources and services include the exchange of information, processing cycles, cache storage, and disk storage for file.P2P computing takes advantage of existing computing power, computer storage and networking connectivity, allowing users to leverage their collective power to the 'benefit' of all. In peer to peer system Trust metrics defined on service and recommendation trust contexts help a peer to reason more precisely about capabilities of other peers in providing services and giving recommendations. If all peers are behave good, reputation of a peer is proportional to its capabilities such as network bandwidth, average online period and number of shared files. In a malicious network, service and recommendation-based attacks affect the reputation of a peer. Three individual attacker, three collaborator and three pseudo spoofer behaviors are studied. SORT mitigates service-based attacks in all scenarios. For individual attackers, hypocritical ones take more time to detect. Identification of collaborators usually takes longer than Identification of an individual attacker. Pseudo spoofers are more isolated from good peers after every pseudonym change. Since good peers get more acquaintances with time, they do not prefer to interact with strangers and leave pseudo spoofers isolated. Two types of collaborators present interesting behavior. Hypocritical collaborators use unfairly high recommendations and attract more good peers at the beginning. They can take advantage of SORT for their attacks. However, good peers eventually identify them and contain their attacks.

Interactions and recommendations are evaluated based on importance, recentness, and peer satisfaction parameters. Additionally, recommender's trustworthiness and confidence about a recommendation are considered while evaluating recommendations. Simulation experiments on a file sharing application show that the proposed model can mitigate attacks on 16 different malicious behavior models. In the experiments, good peers were able to form trust relationships in their proximity and isolate malicious peers. Peer to Peer (P2P) systems rely on collaboration of peers to accomplish tasks. Ease 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. However, establishing trust in an unknown entity is difficult in such a malicious environment. 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. Interactions and feedbacks of peers provide information to measure trust among peers. Interactions with a peer provide certain information about the peer but feedbacks might contain deceptive information. This makes assessment of trustworthiness a challenge. In the presence of an authority, a central server is a preferred way to store and manage trust information. 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 [2], [3]. Management of trust information is dependent to the structure of P2P network. Managing trust is a problem of particular importance in peer-to-peer environments where one frequently encounters unknown agents. Existing methods for trust management that are based on reputation focus on the semantic proper- ties of the trust model. They do not scale as they either rely on a central database or require maintaining global knowledge at each agent to provide data on earlier interactions. In this paper we present an approach that addresses the problem of reputation-based trust management at both the data management and the semantic level. We employ at both levels scalable data structures and algorithms that require no central control and allow assessing trust by computing an agentsreputation from its former interactions with other agents. There are no well defined methods for managing trust relationships in p2p systems. The DHT based approaches are only suited for structured p2p networks not for unstructured p2p networks. Some of the existing methods introduce central authority in p2p networks which may collapse p2p nature. Every agent must keep rather complex and very large data structures that represent a kind of global knowledge about the whole network.

This paper presents distributed algorithms that enable a peer to reason about trustworthiness of other peers based on past interactions and recommendations. Peers create their own trust network in their proximity by using local information available and do not try to learn global trust information.

Two contexts of trust, service, and recommendation contexts are defined to measure trustworthiness in providing services and giving recommendations. Self-Organizing Trust model (SORT) that aims to decrease malicious activity in a P2P system by establishing trust relations among peers in their proximity. 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, re commendation, is evaluated based on recommender‟s trust worthiness. It contains the recommender‟s own experience about the peer, information collected from the recommender‟sacquaintances, 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. SORT defines three trust metrics. Reputation metric is calculated based on recommendations. It is important when deciding about strangers and new acquaintances. Reputation loses its importance as experience with an acquaintance increases. Service trust and recommendation trust are primary metrics to measure trustworthiness in the service and recommendation contexts, respectively. The service trust metric is used when selecting service providers. The recommendation trust metric is important when requesting recommendations. When calculating the reputation metric, recommendations are evaluated based on the recommendation trust metric. One peer is marked as trusted by SORT and if it is turned OFF from network, there is a possibility to another malicious peer takes its position and act as trusted peer. This can be avoided by Auto Update Mechanism.



The simulation runs as cycles. Each cycle represents a period of time. Downloading a file is an interaction. A peer sharing files is called an uploader. A peer downloading a file is called a downloader. The set of peers who downloaded a file from a peer are called downloaders of the peer. An ongoing download/ upload operation is called a session. Simulation parameters are generated based on results of several empirical studies [6], [7] to make observations realistic. A file search request reaches up to 40 percent of the network and returns online uploaders only. A file is downloaded from one uploader to simplify integrity checking.

In trust routing in peer-to-peer systems using self-organizing trust model, 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 trust- worthiness. 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 inevaluation and

affects less the trustworthiness of the recommender.

In this paper structured p2p is implemented, because all the peers are organized into a clear logical overlay. Local view of trust is developed by its own based on the past interaction. Thus, good peers form dynamic trust groups in their contiguity and can isolate malignant peers. In novel trust, at the beginning of the process the peers are assumed to be strangers. Only after providing a service, a peer becomes an acquaintance of another peer e.g., file uploading. The peer chooses to trust strangers if it has no acquaintance. Each peer has a set of acquaintances, a subset of which is identified as its neighbors. Using a service of a peer is an interaction, which is evaluated based on priority, and recentness of the interaction, and contentment of the requester. An acquaintance's observation about a peer, recommendation, is calculated based on recommender's honesties. It contains the recommender's own experience about the peer, data collected from the recommender's acquaintances, and the recommenderconfidence level in the suggestion. If the confidence level is low, the recommendation has a low value in evaluation

II RESEARCH ELABORATIONS

In SORT, to evaluate interactions and recommendations better, importance, recentness, and peer satisfaction parameters 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.

A good peer uploads authentic files and gives fair recommendations. A malicious peer (attacker) performs both service and recommendation-based attacks. Four different attack behaviors are studied for malicious peers: naive, discriminatory, hypocritical, and oscillatory behaviors. A non-malicious network consists of only good peers. A malicious network contains both good and malicious peers. The satisfaction parameter is calculated based on following variables: The ratio of average bandwidth (AveBw) and agreed bandwidth (AgrBw) is a measure of reliability of an uploader in terms of bandwidth. The ratio of online (OnP) and offline (OffP) periods represents availability of an uploader.

Downloading a file is an interaction. A peer sharing files is called an uploader. A peer downloading a file is called a downloader. The set of peers who downloaded a file from a peer are called downloaders of the peer. An ongoing download/ upload operation is called a session. A good peer uploads authentic files and gives fair recommendations. A malicious peer (attacker) performs both service and recommendation-based attacks. Four different attack behaviors are studied for malicious peers: naive, discriminatory, hypocritical, and oscillatory behaviors. A non malicious network consists of only good peers. A malicious network contains both good and malicious peers.

SORT defines three trust metrics. Reputation metric is calculated based on recommendations. It is important when deciding about strangers and new acquaintances. Reputation loses its importance as experience with an acquaintance increases. Service trust and recommendation trust are primary metrics to measure trustworthiness in the service and recommendation contexts, respectively. The service trust metric is used when selecting service providers. The recommendation trust metric is important when requesting recommendations. When calculating the reputation metric, recommendations are evaluated based on the recommendation trust metric. Assume that pi wants to get a particular service. pj is a stranger to pi and a probable service provider. To learn pj‟s reputation, pi requests recommendations from its acquaintances. Assume that pk sends back a recommendation to pi. After collecting all recommendations, pi calculates rij. Then, pi evaluates pk‟s recommendation, stores results in RHik, and updates rtik. Assuming pj is trustworthy enough, pi gets the service from pj. Then, pi evaluates this interaction and stores the results in SHij, and updates stij. One peer is marked as trusted by SORT and if it is turned off from network, there is a possibility to another malicious peer takes its position and act as trusted peer. this can be avoided by the Auto update mechanism.

Metrics should have precision so peers can be ranked according to trustworthiness. Interactions and feedbacks of peers provide information to measure trust among peers. Interactions with a peer provide certain information about the peer but feedbacks might contain deceptive information. This makes assessment of trustworthiness a challenge.

Self-Organizing Trust model (SORT) that aims to decrease malicious activity in a P2P system by establishing trust relations among 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. 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. SORT defines three trust metrics. Reputation metric is calculated based on recommendations. It is important when deciding about strangers and new acquaintances. Reputation loses its importance as experience with an acquaintance increases.

Algorithm Design and Implementation

Algorithm 1 GETRECOMMENDATIONS(p_j)

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 $|rset| < \eta_{max}$ **do**
7: **for all** $p_k \in A_i$ **do**
8: **if** $th_{low} \leq rt_{ik} \leq th_{high}$ **then**
9: $rec \Leftarrow$ RequestRecommendation(p_k,p_j)
10: $rset \Leftarrow rset \cup \{rec\}$
11: **end if**
12: **end for**
13: $th_{high} \Leftarrow th_{low}$
14: $th_{low} \Leftarrow th_{low} - \sigma_{rt}/2$
15: **end while**
16: return $rset$

Service trust and recommendation trust are primary metrics to measure trustworthiness in the service and recommendation contexts, respectively. The service trust metric is used when selecting service providers. The recommendation trust metric is important when requesting recommendations. When calculating the reputation metric, recommendations are evaluated based on the recommendation trust metric.

Creating trust relationship is based upon two contexts of trust. They are Service Context, Recommendation Context. The service trust metric is used when selecting service providers. The recommendation trust metric is important when requesting recommendations. When pi searches for a particular service, it gets list of service providers. Considering a file sharing application, primary download a file from either one or multiple uploaders. With multiple uploaders, checking integrity is a problem since any file part downloaded from an uploader might be inauthentic.. Assume that pi wants to get a particular service. pj is a stranger to pi and a probable service provider. To learn pj‟s reputation, pi requests recommendations from its acquaintances. Assume that pk sends back a recommendation to pi. After collecting all recommendations, pi calculates rij. Then, pi evaluates pk‟s recommendation, stores results in RHik, and updates rtik.Assuming pj is trustworthy enough, pi gets the service from pj. Then, pi evaluates this interaction and stores the results in SHij, and updates stij.

III CONCLUSION

We have identified the question to be addressed when trying to and a solution to the problem of trust assessment based on reputation in a decentralized environment. 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. 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

REFERENCES

[1] AhmetBurakCan and Bharat Bhargava(2013),‟A Self-Organizing Trust Model for Peer-to-Peer Systems‟IEEE Trans.Dependable and Secure Computing,vol 10,No.1.

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

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

[4] SelcukA.A ,Uzun.E, and Pariente.M.R(2004), „A Reputation-Based Trust Management System for P2P Networks‟ Proc. IEEE/ACM Fourth Int‟l Symp. Cluster Computing and the Grid (CCGRID).

[5] Zhou. R, Hwang. K, and Cai. M(2008), „Gossiptrust for Fast Reputation Aggregation in Peer-to-Peer Networks‟ IEEE Trans. Knowledge and Data Eng., vol. 20, no. 9.

[6] Abdul-Rahman. A and Hailes.S(2008), „Supporting Trust in Virtual Communities‟ Proc. 33rd Hawaii Int‟l Conf. System Sciences (HICSS).

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

[8] S. Marsh, “Formalising Trust as a Computational Concept,” PhD thesis, Dept. of Math. And Computer Science, Univ. of Stirling, 1994.

[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] R. Zhou, K. Hwang, and M. Cai, “Gossip trust for Fast Reputation Aggregation in Peer-to-Peer Networks,” IEEE Trans. Knowledge and Data Eng., vol. 20, no. 9, pp. 1282-1295, Sept. 2008.

AUTHORS

First Author –Suraj Suryawanshi has received his B.E degree in Computer Science and Engineering from STJIT College of Engineering, VTU University in 2011.he is pursuing M.Tech in Computer Science and Engineering from Rajiv Gandhi Institute of Technology, Bengaluru.
E-mail: ss120344@gmail.com

Second Author – Pavan Gujjar PandurangaRao Research scholar ,CSSE Department ,Andhra university Vishakapatanam, Andhra pradesh