International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

Maintaining Trust Relationships between Peer – To – Peer Systems

Kiran P[1]& Dr. K.S.Vijaya Simha [2]

[1] PG Scholar, Dept of CSE, Krishna Murthy Institute Of Technology & Engineering, Hyderabad, Telangana

[2] Professor, Dept of CSE, Krishna Murthy Institute Of Technology & Engineering, Hyderabad, Telangana

ABSTRACT

Maintaining trust among peer-to-peer systems is a problem, Open nature of peer-to-peer systems exposes them to malicious activity. Building trust relationships among peers can mitigate attacks of malicious peers. This paper presents an automated trust model which takes into consideration peers past interaction and recommendations to choose trustworthy peer. While evaluating trustworthiness parameters like importance, recentness and peer satisfaction is taken into consideration. Recommenders' trustworthiness and confidence about a recommendation are also considered while evaluating recommendations. We have implemented access control technology in the P2P file sharing system and for that we have used symmetric encryption with shared secrete key. Proposed automated trust model can mitigate attacks on different malicious behavior models

An interaction is evaluated based on importance, recentness and three parameters: satisfaction, weight, fading effect, when evaluating recommendation, recommender's trustworthiness and confidence level about the information provided are also considered. 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.

Keywords—trustworthiness; Peer-to-peer; recommendations

I. INTRODUCTION

In present situations, security is considered as one of the most critical parameter for the acceptance of any networking technology. Basically a network uses the client-server model to perform any task. A peer-to-peer is a type of network in which the nodes act as both the client and server. This model of network arrangement is differs from client-server model where communication made to and from any node [1]. A peer-to-peer network depends on the collaboration of nodes to perform the tasks Peer to peer system contain both type of peers like good peers and also malicious peers. We need to classify the both type of peers by creating long-term relationships among peers. Peers can provide a more secure environment by reducing risk and helps in future peer to peer interactions. However, establishing trust in an unknown peer is difficult in such a malicious environment. Furthermore, trust is a social concept and hard to measure with numerical values. 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 [14].

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. In the existing system, a central server is used to store and manage trust information, for example, eBay [7]. The central server securely stores trust information and defines trust metrics but lot of problems could happen. Since there is no central server in most peer to peer systems, peers organize themselves to store and manage trust information. Systems work on collaboration of peers to accomplish tasks. Peer to peer system contain both type of peers like good peers and also malicious peers. We need to classify the both type of peers by creating long-term relationships among peers. Peers can provide a more secure environment by reducing risk and helps in future peer to peer interactions. However, establishing trust in an unknown peer is difficult in such a malicious environment. Furthermore, trust is a social concept and hard to measure with numerical values. Classifying peers as either trustworthy or untrustworthy is not sufficient in most cases [14].

Each peer develops its own local view of trust about the peers interacted in the past. In this way, good peers form trust groups in their proximity and can isolate malicious peers. Since peers generally tend to interact with small set of peers, forming trust relations in proximity of peers helps to mitigate attacks in a peer to peer system. In computational model metrics are used to represent trust. Peers are classified as trustworthy or untrustworthy and also ranked according to their trustworthiness. An automated trust model that aims to improve security in P2P system by establishing trust relations among peers in their proximity. Each peer develops its own view of trust about the peers with whom he interacted in the past. In this way good peers form dynamic trust groups and can isolate malicious peers. At the beginning, peers are assumed to be strangers to each other and become an acquaintance of another after providing a service, e.g. download a file. If peer has no interaction in the past, it chooses to trust strangers [2].

Using a service of a peer is an interaction, which is evaluated based on weight (importance), recentness of the interaction and satisfaction of the requester. An acquaintances feedback about a peer, recommendation is evaluated based on recommender's trustworthiness. It contains the recommenders own experience about the peer, information collected from the recommenders acquaintances, and the recommenders 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. 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 [3, 4]. 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.

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.

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

Since there is no central server in most P2P systems, peers organize themselves to store and manage trust information about each other [5]. Management of reliable information is based on the structure of P2P network. Managing trust is a problem of particular importance in peer-to-peer environments where one frequently encounters unknown agents.

II. EXISTING SYSTEM

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 certain information about the peer but feedbacks might contain deceptive information [13, 15]. This makes assessment of trustworthiness a challenge. The main problem with existing system is centralized server it is used to store and manage the information about peers. Every time peer need to ask server for which peer is to be selected for next interaction so it takes lot of time and bandwidth wastage [6]. If server got failure then all the information about the peers could be lost. Survive methods for reliable management that are based on reputation focus on the semantic proper- ties of the reliance 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 [7]. We employ at both levels scalable data structures and algorithms that require no central control and allow assessing trust by computing an agents

Reputation 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. The present 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 [9]. 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 [10]. If a peer has no acquaintance, it chooses to trust strangers. Expressing trust or distrust per peer allows hit predict between any two people in the network with high accuracy. Result of their experiment shows that distrust is helpful to measure trustworthiness accurately. J. Douceur explained

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

'the Sybil attack' to reputation system are vulnerable to sybil attack, where malicious peers gives bogus feedbacks by creating multiple fake entities. To overcome Sybil attack, Yu et al. as well as Tran et al. propose system which is based on the observation that fake entities and have many trust relationships among each other but they rarely have relationships with real users [11].

Decentralized network have more challenges comparing to centralized platform. Due to lack of central authority malicious peers have more attack opportunities in P2P system. Attacks like self promoting, white-washing, slandering, orchestrated and denial of service attacks in P2P trust model are discussed by Hoffman et al. In network peer is assumed as trustworthy unless there are complaints against it [12]. In Aberer and Despotovic's trust model, peer reports their complaints using P-Grid. Eigentrust uses transitivity of trust to calculate global trust values stored on content addressable network i.e. CAN. L. Xiong and L. Liu's peer trust defines transaction and community context parameters to make trust calculations adaptive on PGrid. Both Eigentrust and Peertrust evaluate a recommendation based on trustworthiness of the recommender.

All peers are assumed to have antivirus software so they can detect infected files Four different cases are studied to understand effects of trust calculation methods under attack conditions: **No trust.** Trust information is not used for uploader selection. An uploader is selected according to its bandwidth. This method is the base case to understand if trust is helpful to mitigate attacks.

No reputation query. An uploader is selected based on trust information but peers do not request recommendations from other peers. Trust calculation is done based on SORT equations but reputation (r) value is always zero for a peer. This method will help us to assess if recommendations are helpful.

SORT: 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.

Flood reputation query: SORT equations are used but a reputation query is flooded to the whole network. This method will help us to understand if getting more recommendations is helpful to mitigate attacks.

III. PROPOSED SYSTEM

In this proposed system we use the recommendation metric, service trust metric to decide the trustworthiness of peers. Fig 1 shows architecture of Peer2Peer environment. Assume that Peer1 wants to access the particular service.Peer3 is a stranger to peer1 (because at beginning each peer is stranger to each other) and a service provider. Peer1 sends recommendation request from its acquaintances (P2 is said to be acquaintance of P1,if P1 had at least one interaction with P2 otherwise it is said to be stranger). Suppose that peer2 sends a back recommendation to peer1. Peer 1 collects all the recommendations from peers and computes reputation value r.

After this, peer1 computes peer2's recommendation and stores result, and updates recommendation trust about peer2.Considering peer3 is trustworthy enough, peer1 gets service from peer3. Then peer1 evaluates this interaction and computes quality of service and assigns a

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

satisfaction value for interaction. Old interaction's importance decreases as new interaction happens. The fading effect parameter notes this issue and forces peer to stay consistent in the future interactions.

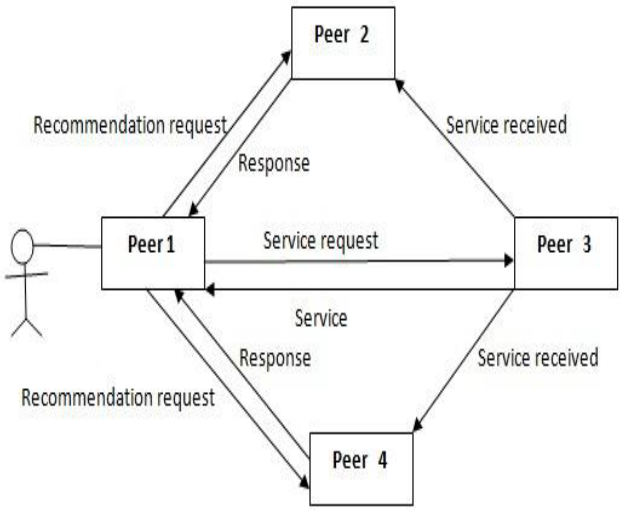

Figure 1: System Architecture

Service trust metric: The service trust metric has been used to evaluate the trustworthiness of trusted third party. To evaluate the trustworthiness of trusted third party, a peer calculates the competence belief and integrity belief values using the information in the service history. The competence belief defines how well a trusted third party satisfied the needs of the peers in past interactions. If a trusted third party completes all interactions perfectly then the competence belief value set to be 1. Otherwise, the value lies in 0<=1 according to the completion of interaction. Consistency is also important as well as competence. That has been obtained by evaluating integrity belief. Integrity belief value is an approximation. That has been evaluated from interactions. If the trusted third party maintains its level of expectation from requester then the value set to be 1. Otherwise, the value lies between o<=1 according to the satisfaction. These two values competence beliefs and integrity belief are calculated by using the weight, recentness and satisfaction values. This process has been done for all the trusted third parties and the values are stored in service history. From the service history a third party with the highest trust value is taken as a trusted third party to get recommendations.

Reputation trust metric: The reputation trust metric calculates the trustworthiness of a stranger based on past interactions. To calculate the reputation value, a reputation query will send to peers. The reputation query collects the recommendations from its trusted third party and the maximum number of recommendations collected through reputation query. There is high threshold value has been set to recommendation trust value. It starts to collect recommendations from its highly trusted third party. Likewise, it collects recommendations from all the trusted third party. If the maximum recommendations are received, then the process will be stopped.

After collecting the recommendations the reputation value has been calculated. Additionally competence and integrity belief values also calculated when a peer needs more trustworthiness about a peer. These values are taken from service history. While this, an own experience is considered.

When the threshold value of service history is equal to the maximum size of service history, then the trusted third party has high level experience about a stranger.

Recommendation trust metric: Recommendation trust metric is also used in evaluating the trustworthiness of a stranger. The recommendation trust value evaluated to

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

calculate the trustworthiness of a stranger by recommendation from trusted third party. After calculating the recommendation trust metric, a recommendation value of recommender is updated. Three parameters namely weight, satisfaction, and recentness of trusted third party are used to calculate the recommendation trust value. The recommendations are stored in a recommendation history. To calculate the satisfaction value the requester compares the reputation value, competence belief value, the integrity belief value provided by trusted third party with values in the history. If these values are equal, then the satisfaction value set to be 1. The weight calculated by service history size. If the history is large, then the maximum value is set to the weight. To provide more trustworthiness competence belief and integrity belief are considered. These values are taken from service history of appropriate peer. After getting all the values a requester calculates the reputation value. Then, the requester evaluates the trusted third parties recommendations trust value and stores the results in service history. If the stranger is trustworthy enough, a requester gets service from the stranger. Getting service is done as follow. First, the recommendation request has been sent to trusted third party. The trusted third party receives a request and sends a recommendation about a stranger. Then, the service request will send to a stranger to get the service. Interactions, opinion and service trust values are stored in a history.

Selecting service provider: After calculating the trustworthiness, the peer selects the service provider to get the needed service. When requesting a particular service there may be several service providers. To select one of the service providers some values are considered. First, the peer which had the highest service trust value has been selected as the service provider. If the peers had equal service trust values, then the peer which had a larger history size is selected to be a service provider. If history size is also equal, the peer which had a higher competence belief value is selected to be a service provider. If this value also equal, then the bandwidths of the peers are compared. If the bandwidth also equal, then any one of the peers has been selected randomly as a service provider from the list of service providers.

IV. CONCLUSION

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. Interactions and recommendations are considered with satisfaction, time and bandwidth. This implemented work provided better security for peer to peer system. This system provides better result compare to earlier methods. In future using trust information does not solve all security problems in P2P systems but can enhance security and effectiveness of systems.

REFERENCES

[1] A.A. Seluk, E. Uzun, and M.R. Pariente, "A Reputation-Based trust Management System for Peer to peer Network," Proc. IEEE/ACM Fourth Int'l Symp. Cluster Computing and the Grid(CCGRID), 2004.

[2] R. Zhou, K. Hwang, and M. Cai, "Gossiptrust for Fast Reputation Aggregation in Peer to peer Network," IEEE Trans. Knowledge and Data Eng., vol.20,no.pp. 1282-1295,Sept.2008.

[3] J . Kleingberg, "The Small-World Phenomenon: An Algorithmic Perspective," Proc. 32nd ACM Symp. Theory of Computing, 2000.

[4] S . Saroiu, P. Gummadi, and S. Gribble, "A Measurement Study of peer to peer File sharing Systems," Proc. Multimedia Computing and Networking,2002.

[5] 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.

[6] 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, Pg.No.843 to Pg.No.857, 2004.

[7] 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.

[8] R. Guha, R. Kumar, P. Raghavan, A. Tomkins, "Propagation of Trust and Distrust, " Proc. 13th Int. Conf. World Wide Web (WWW), 2004.

[9] J. Douceur, The Sybil Attack," Proc. First Intl Workshop Peer-to- Peer Systems (IPTPS), " 2002.

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

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

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

[13] S.Song, K. Hwang, R. Zhou, and Y.-K. Kwok, "Trusted P2P Transactions with Fuzzy Reputation Aggregation," IEEE Internet Computing, vol. 9, no. 6, pp. 24-34, Nov.-Dec. 2005.

[14] 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.

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