ISSN 2277-3061

A Self-Orgnizing Model for Peer-to-Peer Systems using Trust Relations

Sourabh S.Mahajan , S.K.Pathan
PG student, Computer Department
Smt. Kashibai Navale College of Engineering, Pune.
Email id : m.sourabh@rocketmail.com
Assistant Professor, Computer Department
Smt. Kashibai Navale College of Engineering, Pune
Email id : spathan@sinhagad.edu

ABSTRACT

Peer-to-Peer systems enables the interactions of peers to accomplish tasks. Attacks of peers with malicious can be reduced by establishing trust relationship among peers. In this paper we presents algorithms which helps a peer to reason about trustworthiness of other peers based on interactions in the past and recommendations. Local information is used to create trust network of peers and does not need to deal with global information. Trustworthiness of peers in providing services can be describedby Service metric and recommendation metric. Parameters considered for evaluating interactions and recommendations are Recentness, Importance and Peer Satisfaction. Trust relationships helps a good peer to isolate malicious peers.

Indexing terms/Keywords

Peer-to-peer systems; self organized network; trust relations; Service metric and recommendation metric.

Council for Innovative Research
Peer Review Research Publishing System

Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY

Vol. 14, No. 1

www.ijctonline.com , editorijctonline@gmail.com

LITERATURE REVIEW

There are different models are described related to the protection in peer to peer environment. Marsh [6] described a sociological foundations based trust model . An agent uses it's own experience to build trust relations without dealing with the information of other agents. Abdul-rahman and Hailes [7] considers trust in discrete domain as an integration of experience and recommendations of other parties. Yu and Singh's model [8] defines trust information through referral chains. Trust in other are developed by the method named as referral. Mui et al [9] developed statistical model based on trust, reputation, and reciprocity.

To build trust reputation systems are widely used in e-commerce. A central authority is used to collect past customer's feedback which is used by future customers in shopping decisions. There are more opportunities of attack in P2P trust model for malicious peers due to absence of central coordinator. Attacks in P2P trust model such as self promoting, white washing, slandering, orchestrated, and denial of service attacks discussed by Hoffman et al and they said that defense technique in trust models are dependant to P2P architecture. DHT structure provides decentralized approach and access to trust information in the structured P2P environment. A peer in Aberer and Despotovic's trust is treated as trustworthy unless there are complaints about it. In Eign trust [3], global trust values are calculated using trust transitivity. Peer trust [4] describes parameters such as transaction and community context for having trust calculation adaptive on P-grid. Transaction context parameters describes application dependant factors whereas community context parameter exposes P2P community related issues like creating incentives to have feedback. Eigntrust and Peertrust computes recommendations which is based on trustworthiness of the recommender.

Song et al [11] suggests a fuzzy logic trust model that performs same as Eigntrust [13] but with lower message overhead. There are two major steps performed by the fuzzy system: Local score calculation and Global reputation aggregation. In local score fuzzy operations are performed by peers on local parameters to create local score. Fuzzy logic is self adjusting and holds some uncertainties. Local trust scores which are collected from all peers are aggregated by fuzzy system in order to generate global reputation for each peers. Fuzzy inference is used by the system to get global reputation aggregation weights. Aggregation weights are determined by variables named peer's reputation, transaction date and transaction amount. In fuzzy trust system based on DHT, each peer maintains transaction record table and local score table. Transaction record table maintains transaction records with remote peers whereas local score table holds trusted score evaluated by remote peers.

Gnutella achieved reliability, scalability, performance with virtual network and routing mechanism. Gnutella survey determines characteristics of participating resources. It is decentralized mechanism and search protocol,which is used for the pupose of file sharing. Gnutella nodes named servants performs tasks related with server as well as client. Nodes accept queries from other servants, match it with local components and generate corresponding result. When nodes are attached to the network, nodes sends message to interact with each other where message can be broadcasted in the network or backpropogated .

INTRODUCTION

In peer to peer systems individual machine can communicate with each others and share resources without dealing the central coordinator. Building long term trust relationships provides more secure environment which reduces risk and uncertainty in the future. Metrics are required to describe trust in computational model. Trust among peers is measured based on the information provided by interactions and feedbacks of peers.

The systems such as eBay prefer the central server to store and manage trust information. In most P2P systems central authority is not present to deal with storing and managing trust information about each other [1], [2]. Structure of P2P systems resolves management of trust information. In approaches such as distributed hash table (DHT), feedback storing about other peers which made peer as trust holder [1], [3], [4]. Global trust information is accessed through DHT which is stored by trust holders. A peer sends queries for trust to know trust information of other peers. A query is either flooded to network or to neighbor of query initiator. If there is equality in trustworthiness then acquaintance is preferred over stranger. Using a service of a peer is said to be an interaction. It is computed based on recentness of the interaction, weight (importance). Recommendation, which is feedback of acquaintance, is computed based on trustworthiness of recommender. It involves the own experience about the peer of recommender, information from recommender's acquaintances, and recommender's level of confidence. The recommendation has a low value if level of confidence is low, which affects less the trustworthiness of recommender.

SORT defines two context of trust: service and recommendation trust. In these contexts, separate histories are maintained to store information about past interactions and recommendations in order to assess competence and integrity of acquaintances. There are three trust metrics: Reputation metric-It is computed based on recommendations. It considers to be prime when deciding about strangers and new acquaintances. Service trust metric and Recommendation trust metrics are considered in order to measure trustworthiness in the service context and recommendation contexts. Service providers are selected based on service trust metric, whereas recommendation trust metric is used when requesting recommendations. Recommendations are computed based on recommendation trust metric in order to compute reputation metric. SORT deals with the service based attacks as well as recommendation based attacks. SORT describes, good peer can protect themselves against peers with malicious intents without using global trust information, and instead it uses local trust to assess trustworthiness of other peers.

ISSN 2277-3061

PROPOSED SCHEME

The proposed peer to peer system enables peer to secure access of data and services. 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.

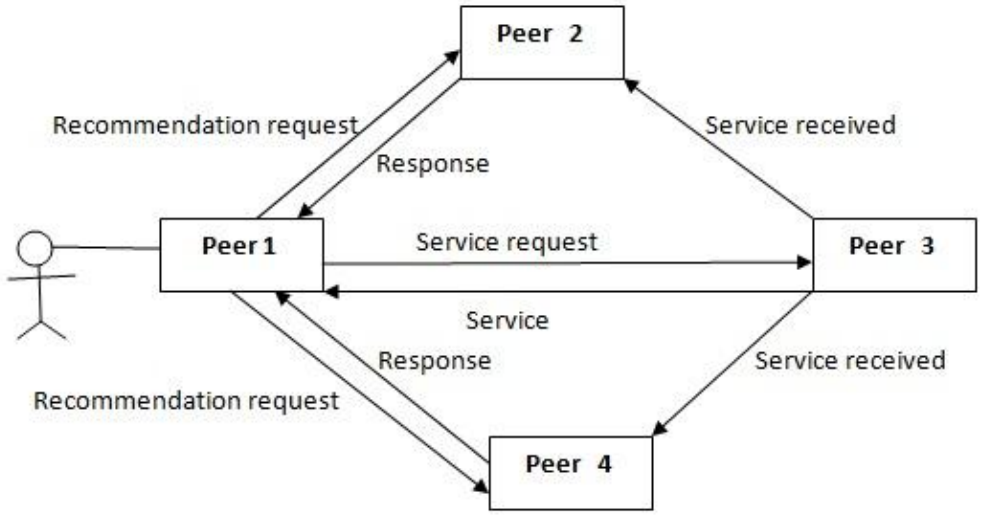

Fig. 1 Architecture of Peer2Peer System

Peer1 sends recommendation request from it's 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 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.

Selection of service provider

Suppose peer Pi searches for a particular service, it gets a list of service providers. Considering a file sharing application, pi may download a file from either one or multiple uploaders. Service provider selection is done based on service trust metric, service history size, competence belief, and integrity belief values. When pi wants to download a file, it selects an uploader with the highest service trust value. If service trust values are equal, the peer with a larger service history size (sh) is selected to prioritize the one with more direct experience.

Model of Attacker

There are two possible attacks named service-based and recommendation based attacks. Uploading a virus infected or an inauthentic file is a service-based attack. Giving a misleading recommendation intentionally is a recommendation-based attack. A servicebased attack can be detected immediately since a virus infected or an inauthentic file can be recognized after the download. However, it is hard for a peer to determine a recommendation-based attack if the peer's own experience conflicts with a recommendation. 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 nonmalicious network consists of only good peers. A malicious network contains both good and malicious peers. If malicious peers do not know about each other and perform attacks independently, they are called as individual attackers.Individual attackers may attack each other.

Attack behaviors are as follows:

1. **Naïve**: The attacker always uploads infected/ inauthentic files and gives unfairly low recommendations about others .

2.**Discriminatory**: The attacker selects a group of victims and always uploads infected/inauthentic files to them.It gives unfairly low recommendations about victims. For other peers, it behaves as a good peer.

3. **Hypocritical**: The attacker uploads infected/iauthentic files and gives unfairly low recommendations with x percent probability . In the other times, it behaves as a good peer.

4. **Oscillatory**: The attacker builds a high reputation by being good for a long time period. Then, it behaves as a naive attacker for a short period of time. After the malicious period, it becomes a good peer again. If malicious peers know each other and coordinate when launching attacks, they are called as collaborators.

CONCLUSION AND FUTURE WORK

We have presented self orgnising trusted model for peer to peer networks. Trust relationship can developed by the peer with other peers. A good peer can easily isolate peers who have malicious intents.There are two prime contexts named Service context and recommendation context, defined to quantify peer's capabilities in order to provide services and giving recommendations. Parameters considered about interaction and recommendations are Fading effect, satisfaction, weight. We can compute number of trust recommendation given by peer as well as services taken by peer. Based on this, attacker modules calculate the attacks and give feedback about peer.Service based attacks and Recommendation based attacks are two possible attacks .In future we will reduce the storage overhead used to keep trust information.

REFERENCES

[1] K.Abererand Z. Despotovic,"Managing Trust in a Peer-2-Peer Information System," Proc. 10th Int'l Conf. Information and Knowledge Management (CIKM), 2001.

[2] 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.

[3] 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.

[4] L. Xiong and L. Liu, "Peertrust: Supporting Reputation-Based Trust for Peer-to-Peer Ecommerce Communities," IEEE Trans.

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

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

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

[9] 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.

[10] 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.

[11] 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.

[12] 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.

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

[14] 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.