ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

A Survey on Trust Model in Peer-to-Peer Networks

Pradnya Bhirud, Prof.Avinash Shrivas

ME Student, Dept. of Computer, Vidyalankar Institute of Technology, Mumbai University, Maharashtra, India

Assistant Professor, Dept. of Computer, Vidyalankar Institute of Technology, Mumbai University, Maharashtra, India

ABSTRACT: Security is one of the most critical constraints for the expansion of peer-to-peer networks. In a peer-to-peer (P2P) network, every machine plays the role of client and server at the same time. In peer-to-peer networks, one of the most important issues is trust management. Peer-to-peer networks rely on other peers to accomplish the tasks. Peers need to trust each other for successful operation of the system. While communicating in between peers trust formation is very important to take service from the unknown resource. In this paper, we study trust models based on various approaches like reputation, service and recommendation.

KEYWORDS: Peer-to-peer networks; trust; reputation; security; recommendation.

I. INTRODUCTION

With the increasing availability of high bandwidth Internet connections and low price of computers, peer-to-peer (P2P) networks have become very popular in resource sharing and exchange. There are no fixed clients and servers. Any node could be a client or a server [7].

A peer-to-peer network is a type of decentralized and distributed network architecture in which individual nodes in the network act as both suppliers and consumers of resources, in contrast to the centralized client–server model where client nodes request access to resources provided by central servers [5]. In this network, tasks are shared amongst multiple interconnected peers who make a portion of their resources directly available to other network participants, without the need for centralized coordination by servers [1]. Below figure provides a conceptual representation of the P2P overlay topology. In this, every machine plays the role of client and server at the same time. Although a P2P network has a number of advantages over the traditional client-server model in terms of efficiency and fault-tolerance, additional security threats can be introduced. Users and IT administrators need to be aware of the risks from propagation of malicious code, the legality of downloaded content, and vulnerabilities within peer-to-peer software [8].

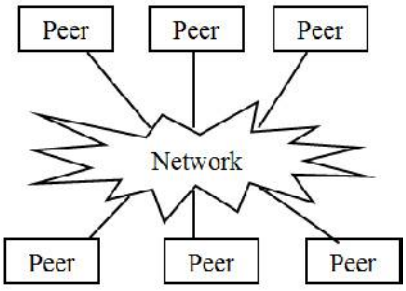

Fig. 1 P2P overlay topology

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

The rest of the paper is as follows. Section II briefs the considered Trust models EigenTrust, SORT, Self-Nominating Trust Modelfor the analysis. Section III represents the comparison of these trust model based on various approaches and the paper concludes with section IV.

II. LITERATURE SURVEY

Many types of research have been done to establish the trust model. We study trust models based on various approaches like reputation, service and recommendation.

2.1 EigenTrust [2]:

This is distributed algorithm to decrease the number of downloads of inauthentic files in a peer-to-peer file-sharing network that assigns each peer a unique global trust value, based on the peer's history of uploads. Eigen Trust model is designed for the reputation management of P2P system. The global reputation of each peer *i*is marked by the local trust values assigned to peer i by other peers, and it is weighted by the global reputation of the assigned peers. For normalizing local trust value *Cij*, the definition is as follow: *Sij*is meant for each peer enable to store the number satisfactory transactions it has had with peer *j*, and it is also meant for the number of unsatisfactory transactions it has had with peer.

$$C_{i,j} = (Max(S_{i,j}))/ \Sigma Max(S_{i,j})$$

Aggregating local trust Values, after normalizing local trust value, it is required to aggregate the normalized local trust values. In a distributed environment, one common way to do this is as follow: for the peer *i*will ask its acquaintances about their opinions about other peers. This EigenTrust is meant for protection from inauthentic file assessment in peer to peer interaction.

2.2SORT: A Self-Organizing Trust Model for Peer-to-Peer Systems [3]:

In this paper, Self-Organizing Trust Model can decrease malicious activity in a P2P system by establishing trust relations among peers in their proximity.Two contexts of trust, service, and recommendation contexts, are defined to measure trustworthiness in providing services and giving recommendations. Interactions and recommendations are evaluated based on importance, recentness, and peer satisfaction parameters.

In Self-Organizing Trust model that enables distributed algorithms that allows 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 recommendationcontexts are defined to measure trustworthiness in providing services and giving recommendations.

1. **Service trust metric**: Service trust metric is calculated on the basis of the reputation, satisfaction and the recommendation given by the other peers. A peer first calculates competence and integrity belief values for evaluating service provider's trustworthiness in the service context, using the information in its service history.
   - Competence belief: Average behavior in the past interactions is a measure of the competence belief.
   - Integrity belief: Level of confidence in predictability of future interactions is called integrity belief.
2. **Recommendation trust metric**: when peer pi collects the recommendation trust information of peer pj.Peers who have the direct interaction experiences with peer pj will send a feedback to peer pi.Peer pi aggregates these feedbacks to compute a recommendation trust metric of peer pj.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

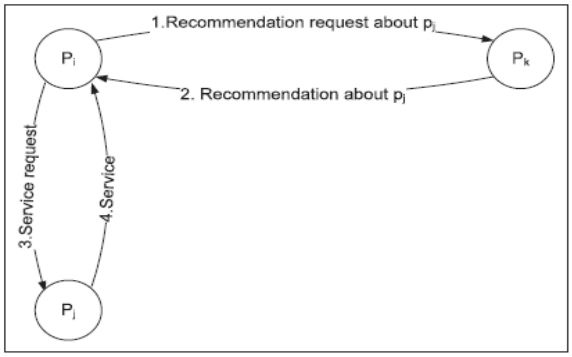

Fig. 2 Operations when receiving a recommendation and having an interaction

SORT models considerably behaves well by considering all the parameters like efficient trust calculation but this model has high computation cost due lot of calculation of metrics.

2.3 Self-Nominating Trust Model Based on Hierarchical Fuzzy Systems for Peer-to-Peer Networks [4]:

In this paper, present a self-nominating trust model based on Hierarchical Fuzzy Systems to quantify the activities of peers. Eight factors are integrated into the reputation evaluation process. In particular, three of them are Promising factor, four capability factors and one Security factor.

1. **Promising factors:** provided by resource holders to demonstrate their desires
    - Time to live:This factor can be promised and provided by the resource holder to identify its remaining (online) time before it leaves. The requester can estimate the task progress based on this factor.
    - Upload Speed: Upload Speed is the average time required for upload the file.
    - Content relevance:Spam and irrelevant files are not rare. Even an authentic and available file can be attached with annoying data such as unknown popup link or spam advertisement. Resource provider can declare the content relevance using this factor
2. **Capability factors:** recorded by requesters to identify the providers' service capability.
    - Bandwidth: Bandwidth determines a peer's ability for providing data transactions. A larger bandwidth provide more data transactions.
    - Online time rate:Due to the dynamic and autonomous nature of P2P networks, a peer can join and leave at any time. Online time rate is recorded to indicate the rate of peer's login time.
    - Download success rate:When a file downloaded from the peers, there is a chance of download failure. For that reason only successful downloads are the available for sharing. So we incorporate one new factor, download success rate factor. To calculate download success rate, we have to calculate the ratio of Number of success download and the number of failed download
    - File size:It indicates the size of the requested resource and the number of files included in the resource.
3. **Security factor:** The most important factor is malicious behaviorwhich is closely related to security threats in a P2P environment. The way of preventing malicious peers is to decrease their reputation level if they are undesirably elected as service providers.

The eight trust factors can be closely integrated into an output fuzzy variable (i.e., the local trust metric). There are 8 input fuzzy variables, 6 intermediate fuzzy variables, and 1 output fuzzy variable in the system. Finally compute the global trust metric by combining the local trust metric and the recommendation trust metric for improve the efficiency and security of P2P systems.

Self-nominating trust model based on Hierarchical Fuzzy Systems to improve the efficiency and security of P2P systems. Trust model can evaluate the trust in a comprehensive manner, where peers are promoted to share by identifying their sharing desires and transmission capabilities.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

III. COMPARISON OF TRUST MODEL BASED ON VARIOUS APPROACHES

There are some trust models based on various approaches which have been proposed in P2P systems. In this section, let's examine the differences among them.

Different Trust Models	Significance
EigenTrust	Uses Reputation based approach and accordingly trust values are evaluated
SORT	Uses Reputation and recommendation based approach, Trust Values on the basis of service and recommendations
Self-Nominating Trust Model	Uses Reputation based approach, Trust Values on the basis of reputation which calculated using fuzzy logic.

EigenTrust scheme is proposed by Kamvar [2], which can be used for evaluating the trust information provided by peers according to their trustworthiness. The core of the protocol is that, a special normalization process where the trust ratings held by a peer are normalized to have their sum equal to 1. Its shortcoming is that this normalization could occurs the loss of important trust information. For EigenTrust, the security issues are that: Firstly, the peer's current trust value must not be calculated by and reside at the peer itself. If it likes that, the peer can easily to be manipulated. Thus, we adopt a different peer in the network compute the trust value of a peer. Secondly, it will be in the interest of malicious peers to return wrong results when they are supposed to compute any peer's trust value. So, if in order to compute the trust value of one peer in the network, you will have to get more than one other peers [6].

SORT technique is trust management technique which gives the trust values to the peers on the basis of the service and recommendation of the peers. For Sort, the issue is that: Using trust information does not solve all security problems in P2P systems [3].

Self-nominating trust model based on Hierarchical Fuzzy Systems to improve the efficiency and security of P2P systems. The hierarchical fuzzy system was introduced to integrate eight factors with a low complexity. For Self-nominating trust model, the issue is that: Consider only reputation and recommendation module and not focused on the service module [4].

IV. CONCLUSION AND FUTURE WORK

We have studied trust models based on various approaches like reputation, service and recommendation out of which SORT model is quite better as compared to other models with respect to performance and accuracy but only 1 drawback is that 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. Self-nominating trust model based onHierarchical Fuzzy Systems to improve thesecurity of P2P systems but in this trust model consider only reputation and recommendation module and not focused on the service module. So, in Future work we combine these two trust model for better Performance.

REFERENCES

1. Santosh Suresh Padwal, G.P. Bhole, "Study of Trust Management Approaches in Peer to Peer System", International Journal of Current Engineering and Technology, Vol.4, Issue 4, pp.2439-2443, 2014.
2. Sepandar D. Kamvar, Mario T. Schlosse and Hector Garcia-Molina, "The EigenTrust Algorithm for Reputation Management in P2P Networks",WWW '03 Proceedings of the 12th international conference on World Wide Web, pp.640-651, 2003.
3. Ahmet Burak Can, and Bharat Bhargava, "SORT: A SelfORganizing Trust Model for Peer-to-Peer Systems",IEEE Transactions On Dependable And Secure Computing, Vol.10, Issue 1, pp.14-27, 2013.
4. Qiyi Han, Hong Wen, Ting Ma and Bin Wu, "Self-Nominating Trust Model Based on Hierarchical Fuzzy Systems for Peer-to-Peer Networks", IEEE/CIC ICCC 2014 Symposium on Privacy and Security in Commutations, pp. 199-203, 2014.
5. Yao Wang, JulitaVassileva, "Trust and Reputation Model in Peer-to-Peer Networks", P2P '03 Proceedings of the 3rd International Conference on Peer-to-Peer Computing, 2003.
6. Hai Ren, "Comparison of Trust Model in Peer to Peer System", TKK T-110.5290 Seminar on Network Security,2006.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

7. Peng Mu, Xianying Cheng, "Trust and reputation in file-sharing Peer-to-Peer systems", TDDC03 Projects, Spring 2004.
8. S John Bee, B.Ranjith, "SOT Model towards Peer to Peer System", International journal of computer engineering in research trends, Vol.1, Issue 6, pp.409-413,2014.

BIOGRAPHY

PradnyaBhirudis pursuing M.E (Comp Engg.) from Vidyalankar Institute of Technology, Mumbai University. She did her graduation B.E (Comp Engg.) from Mumbai University, Maharashtra.