ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 1, ISSUE 6, DECEMBER 2014, PP 409-413

SOT Model towards Peer to Peer System

[1] S JOHN BEE , [2] B.RANJITH

[1] M.Tech Research Scholar, Priyadarshini Institute of Technology and Science for Women
[2] HOD-CSE, Priyadarshini Institute of Technology and Science for Women

Abstract:

In a peer-to-peer (P2P) network, each device assumes the part of Client and server in the meantime. In P2p framework, a standout amongst the most essential issues is trust administration. P2P frameworks depend on different companions to finish the undertakings. Companions need to trust one another for fruitful operation of the framework. While imparting in the middle of companions trust development is paramount to take administration from the obscure asset. In this paper we think over for four trust models focused around different methodologies, for example, by approaches, by notoriety and so forth. Presently a large portion of models for trust administration are focused around notoriety. There are numerous models which meets expectations under aforementioned methodologies out of these we have examined Eigen trust, SORT, Worldwide Trust model and NICE. We have likewise analyzed four trust models in P2P frameworks. The examination is focused around the profits and their properties.

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

1. INTRODUCTION

Peer systems accomplish tasks by relying on collaboration. P2P systems are exposed to security threats, due to lack of central authority and dynamic in nature. In case of secure environment, building up of trust relationship can reduce the risk and reliable in future interactions. The fundamental challenges for peer-to-peer (P2P) systems is to manage the risks involved in interaction and collaboration with priory unknown and potentially malignant agents. In case of malignant environment, establishing trust is a most difficult task. Moreover, trust is a social phenomenon i.e. firm belief in the reliability and difficult to measure with numeric values. Benchmarks are needed to symbolize trust. Ranking of peers is necessary so that trustworthiness can be displayed based on metrics defined.

The measurement of trust depends on interactions and feedbacks of peers. Interactions with a peer provide specific information but feedbacks might contain illusive information. Peer to peer is a decentralized network architecture in which each peer can act as a server for sharing of resources. P2P systems can be classified into two groups: unstructured and structured. In unstructured P2P, a limited number of connections are maintained by each peer to other neighboring peers in the network. Searching in an unstructured P2P environment leads to flooding queries in the network. In structured P2P systems, a hash function is used in order to couple keys with objects. To hold the relevant objects, distributed hash table (DHT) is used to route key-based queries efficiently to peers.

Peer to Peer System

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. 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.

Below figure provides a conceptual representation of the P2P overlay topology. In this, every machine plays

ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 1, ISSUE 6, DECEMBER 2014, PP 409-413

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. Security and preventative measures should be implemented to protect from any potential leakage of sensitive information and possible security breaches.

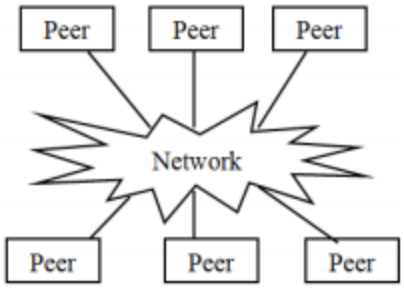


Fig. 1 P2P overlay topology

In this paper structured p2p is implemented, because all the peers are organized into a clear logical overlay. A novel trust model is proposed that intent to decrease malignant activity in a P2P system by establishing trust relations among peers in their contiguity. 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 recommender's confidence level in the suggestion. If the confidence level is low, the recommendation has a low value in evaluation. Novel defines three trust metrics. Reputation metric represents the belief in the system and allows parties to build trust, or the degree to which one party has confidence in another within the context of a given purpose or decision and is calculated based on recommendations. The service trust metric is used for selection of service providers. The recommendation trust metric is needed when requesting recommendations. When calculating reputation metric, recommendations are evaluated based on recommendation trust metric.

2. RELATED WORK

Trust model creation based on following trust principles such as,
a) Trust is content-dependent.
b) Negative and positive belief is supported.
c) Trust is based on past experience.
d) Information exchange through recommendation.
e) Different opinions of all the agents are considered.
f) Recommendations may increase or decrease the trust level [2].
Reputation is the opinion of the public towards a person or organization or resources. In p2p, reputation represents the opinions nodes and expectation about an agent's behavior based on data or observations of its past behavior. In this, the users rate he reliability of parties they deal with, and share this data with their peers. Reputation trust identifies the malicious responses from benign ones by using reputation of peers provided by them.Peer" s past transaction are stored in trust vectors, which are of constant-length, binary vector of l bit i.e. (8, 16, 32). A 1 bit represents an honest transaction; 0 represents a dishonest one.

Reputation-based trust management properties:
a) No central coordination. No central database.
b) No peer has a global view of the system.
c) Global behavior emerges from local interactions.
d) Peers are autonomous.
e) Peers and connections are unreliable.
Two types of ratings are performed;
1. Trust rating
2. Distrust rating

Peer to peer information sharing environments are increasingly gaining acceptance on the internet as they provide an infrastructure in which the desired information can be located and downloaded while

ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351
INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 1, ISSUE 6, DECEMBER 2014, PP 409-413

preserving the anonymity of both requestors and providers. Reputation sharing is done based on a distributed polling algorithm by which resource requestors can assess the reliability of perspective providers before initiating the download; also it keeps the current level of anonymity of requestors and providers, as well as that of the parties sharing their view on other's reputation [7]. In absence of central database, manage trust in a peer-to-peer network is tedious, which is based on binary trust values, i.e., a peer is either trustworthy or not. In case a dishonest transaction occurs, the peers can forward their complaints to other peers. To store the complaints in a peer-to-peer network, special data structures namely the P-Grid are needed to be designed [8]. An agent uses own experiences when building trust and does not consider information of other agents [9]. Each peer stores its own reputation using signed certificates. This approach eliminates the need for reputation queries, but it requires a public-key infrastructure [10].

An algorithm is introduced to classify users and assign them roles based on trust relationships [11]. Reputation systems are vulnerable to incorrect and false feedback attacks. Thus feedback ratings must be based on goal criteria [12].Trust and distrust metrics are defined. A nonzero distrust value lets an agent to distinguish an untreated user from a new user [13]. Reputation is been used 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 [14]. A history of interactions is stored and considers ratings and recentness of interactions when evaluating trust. Number of interactions with a peer is a measure of confidence about the peer [15].

3. EXISTING TRUST MODELS IN PEER TO PEER SYSTEM

There are many trust models, some are noted as follows like,Global Trust, NICE, EIGENTRUST, SORT. (Chen Ding,Jussi Kangasharju 2010, Hai Ren 2012)

Global Trust Model

This model is based on binary trust. In other words, an agent could be either trustworthy or not. The transactions are performed by the agents, and each of them t (p, q) can be performed correctly or not. If there is one agent p cheating within a transaction, the agent will become from the global perspective untrustworthy. For distributing the information about transactions agent, these information is forwarded by agents to other agents. In this model, it is assumed that the trust exists and malicious behavior is just exceptions. If there is a malicious behavior of q, an agent is able to file a complaint c(p,q). Firstly, let's consider a simple situation. If there are two agents' p and q, they interact with each other very well. After for a while, another agent r, which wants to get the trustworthiness of p and q. As p, it is cheating, but q is honest. After their interaction, the complaint about p will be filed by q that is pretty fair. On the other side, p will also do the similar thing as q does, so that to hide its misbehavior. To an outside observer r, it cannot distinguish whether p is honest or q is honest, it is very hard for r to tell the truth. There is another new trouble for P continues to cheat. p is a cheater which can be distinguished in the following way.

Assume that, p is cheating in another interaction with s. Then, agent r will detect that p complaint about q and s. In contract, both q and s all complaint about p. So we can get a conclusion, p is the cheater. Generalizing the above idea by the below equation:

$$T(p) = \{|c(p,q)|q \in P\}| \times |\{c(q,p)|q\ 2 \in P\}$$

The higher values of T(p), the trustworthy of p is lower.

4. NICE MODEL

In order to determine good peers in P2P system, and establish steady cooperation with other peers, NICE model is inspired in this background. This model is used to guard against malicious peers. Each peer at the ends of an interaction, creating a cookie with feedback about the other peer assigns it. The signed cookies are exchange among them. If the transaction is successful, the value of the cookie is positive, otherwise, the value is negative.

NICE model differs other models lively. For other models, it is required for them to be in charge of the requestor is trusted. For NICE model, if one peer wants to request a certain data or other things. The peer can just show the provider with a cookie signed by the provider itself. The validity of the cookies provided will be justified by the provider. If the cookie is right, then, it is regarded as a evidence of the requestor peer's

ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 1, ISSUE 6, DECEMBER 2014, PP 409-413

trustworthiness. Positive cookies will be exchanged by interacting peers; negative cookies are retained by the peer that creates it. To guarantee the negative cookies are unhampered and available to other peers in the system. To

Avoid any other attacks perpetrated by colluding peers; the peers will create robust cooperative groups with other good peers. In this way, every peer has a preference list of good peers, and maintaining it based on the past interaction history. At last peers are removed which are having negative feedback cookies.

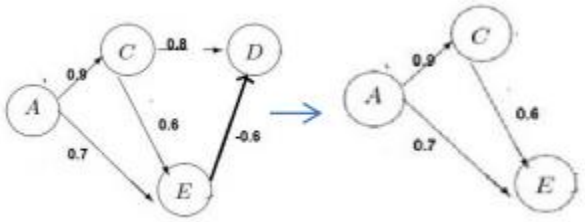


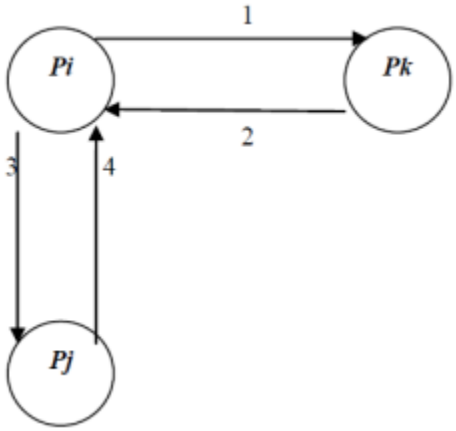
Fig 2 Directed graph with trust paths between peers.

Eigentrust

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

5. SOT

Self-Organizing Trust model that enables distribute 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 recommendation contexts are defined to measure trustworthiness in providing services and giving recommendations. Service trust is calculated on the basis of the reputation, satisfaction and the recommendation given by the other peers. Self-Organizing Trust model that aims to decrease malicious activity in a P2P system by establishing trust relations among peers in their proximity. (Ahmet Burak Can 2013)



1 Recommendation request about Pj

2 Recommendation of Pj

3 Service Request

4 Service

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. SOT 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. (Ahmet Burak Can 2013)

6. CONCLUSION

In P2P systems, it is important to detect the malicious peers and harmful resources before a peer starts downloading. Reputation-based trust management is

used to promote honest and cooperative behaviors, and thus the overall credibility of the P2P network can be maintained at an expected level. 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. 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. We have studied various approaches and models for trust management 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 it has high computational and communicational cost.

REFERENCES

[1]Ahmet Burak Can, and Bharat Bhargava, (2013) SORT: A SelfORganizing Trust Model for Peer-to-Peer Systems,IEEE Transactions On Dependable And Secure Computing, Vol. 10, No. 1.

[2]Chen Ding, Chen Yueguo, Cheng Weiwei(2012), E-Book Of Trust Management in P2P Systems.Jussi Kangasharju(2011), E-Book OfIntroduction Peer-toPeer Networks.

[3] Gupta(2011). Peer-To-Peer Networks And Computation:Current Trends And Future Perspectives,Computing And Informatics, Vol. 30, 559–594

[4]Stefan Saroiu, P. Krishna Gummadi, Steven D.Gribble(2013) A Measurement Study of Peer-to-Peer File Sharing Systems Dept. of Computer Science and Engineering, Univ. of Washington, Seattle, WA, 98195-2350

[5]Loubna Mekouar(2005) Reputation-based Trust Management in Peer-to-Peer File Sharing Systems,University of Waterlo IEEE Consumer Communications and Networking Conference (CCNC)

[6].Hai Ren(2006), Comparison of Trust Model in Peer to Peer System, Helsinki University of Technology, TKK T-110.5290 Seminar on Network Security.

[7] 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.

[8] 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.

[9] S. Marsh, Formalising Trust as a Computational Concept.PhD thesis, Department of Mathematics and Computer Science,University of Stirling, 1994.

[10] B. Ooi, C. Liau, and K. Tan, "Managing trust in peer-topeer systems using reputation-based techniques," in Proceedings of the 4th International Conference on Web Age Information Management, 2003.

[11] 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.

[12] 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.

[13] 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.

[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] B. Yu, M.P. Singh, and K. Sycara, "Developing Trust in Large- Scale Peer-to-Peer Systems," Proc. IEEE First Symp.Multi-Agent Security and Survivability, 2004.