International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161

Available at http://inpressco.com/category/ijcet

Research Article

Study of Trust Management Approaches in Peer to Peer System

Santosh Suresh Padwal[A*] and G.P. Bhole[A]

[A]Veermata Jijabai Technological Institute, Mumbai - 400 019, India.

Accepted 10 July 2014, Available online 01 Aug 2014, **Vol.4, No.4 (Aug 2014)**

Abstract

In a peer-to-peer (P2P) network, every machine plays the role of client and server at the same time. In P2P system, one of the most important issues is trust management. P2P systems 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 four trust models based on various approaches such as by policies, by reputation etc. Currently most of models for trust management are based on reputation. There are many models which works under above mentioned approaches out of these we have studied Eigen trust, SORT, Global Trust model and NICE. We have also compared four trust models in P2P systems. The comparison is based on the benefits and their properties.

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

1. Introduction

Peer to Peer systems rely on collaboration of peers to accomplish tasks. Peers need to trust each other for successful operation of the system. A malicious peer can use the trust of others to gain advantage or harm. Feedbacks from peers are needed to detect malicious behavior. Since the feedbacks might be deceptive, identifying a malicious peer with high confidence is a challenge (Ahmet Burak Can 2013).Determining trustworthy peers requires a study of how peers can establish trust among each other. Long-term trust information about other peers can reduce the risk and uncertainty in future interactions .Interactions and feedbacks provide a means to establish trust among peers (Chen Ding, Jussi Kangasharju 2012). In this section, we will cover some background knowledge regarding Peer to Peer Networks, trust management and techniques to manage trust in Peer to Peer Networks.

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 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.

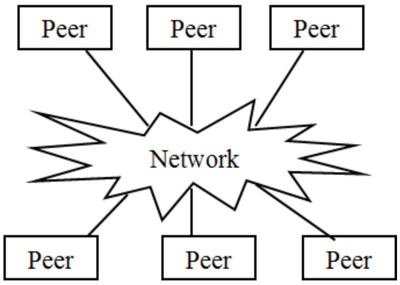


Fig. 1 P2P overlay topology

System Models

P2P networks are organized as overlay topologies on top of the underlying network topologies and are formed by peers connecting to each other in either a structured or unstructured manner. Since P2P networks are fault-tolerant, not susceptible to single-point-of-failure and required to cater to a transient population of nodes, P2P

*Corresponding author: **Santosh Suresh Padwal** overlay topologies are multiply-connected broadly; there are 3 classes of P2P systems (Chen Ding).

1. *Unstructured networks* - Unstructured peer-to-peer networks do not impose a particular structure on the overlay network by design, but rather are formed by nodes that randomly form connections to each other Because there is no structure globally imposed upon them. Unstructured networks are easy to build and allow for localized optimizations to different regions of the overlay. This is highly robust network where dynamically entry or exit of new nodes can be done.
2. *Structured networks* - In structured peer-to-peer networks the overlay is organized into a specific topology, and the protocol ensures that any node can efficiently search the network for a resource, even if the resource is extremely rare.
3. *Hybrid models* -Hybrid models are a combination of peer-to-peer and client-server models. A common hybrid model is to have a central server that helps peers find each other. Spotify is an example of a hybrid model. There are a variety of hybrid models, all of which make trade-offs between the centralized functionality provided by a structured server/client network and the node equality afforded by the pure peer-to-peer unstructured networks. Currently, hybrid models have better performance than either pure unstructured networks or pure structured networks because certain functions, such as searching, do require a centralized functionality but benefit from the decentralized aggregation of nodes provided by unstructured networks.

Application

- These Peer to Peer networks efficiently uses in various applications such as BitTorrent, DistriBrute, Private File Sharing, Real-time communications such as Skype, Adobe Flash Player, YaCy Search Engine.
- Distributed Processing In a P2P system, distributed processing share the computing power of their nodes(Chen Ding, Ankur Gupta 2011).

2. Motivation

Peer to Peer systems rely on collaboration of peers to accomplish tasks. Peers need to trust each other for successful operation of the system. A malicious peer can use the trust of others to gain advantage or harm. Feedbacks from peers are needed to detect malicious behavior. Since the feedbacks might be deceptive, identifying a malicious peer with high confidence is a challenge (Ahmet Burak Can 2013). Determining trustworthy peers requires a study of how peers can establish trust among each other. Long-term trust information about other peers can reduce the risk and uncertainty in future interactions.

These issues have motivated substantial research on trust management in P2P networks. Trust management is a successful approach that helps to maintain overall credibility level of the system as well as to encourage honest and cooperative behavior. The intuitive motivation of trust management is as follows. Since in P2P system there is no central authority that can authenticate and guard against the actions of malicious peers, it is up to the peer to protect itself and to be responsible for its own actions. Consequently, each peer in the system needs to somehow evaluate information received from another peer in order to determine the trustworthiness of both the information as well as the sender. This can be achieved in several ways such as relying on direct experiences or acquiring reputation information from other peers. Particularly trust management systems are classified into three categories, reputation-based trust systems, policy-based trust systems, and social network-based trust systems.

Based on the above mentioned approach adopted to establish and evaluate trust relationship between peers, trust management in P2P system can be classified into 3 categories i.e. credential and policy-based trust management, reputation-based trust management, and social network-based trust management as shown in Figure 2.

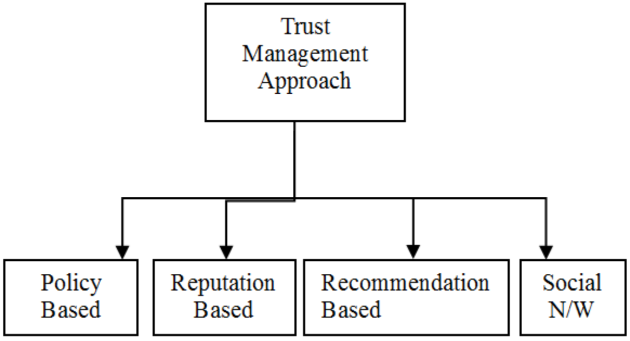


Fig. 2 Approaches in Trust management

There are many models under this approaches out of which we are considering 4 models to study. Eigentrust uses transitivity of trust which allows a peer to calculate global trust values of other peers. Trust of some base peers helps to build trust among all other peers. A recommendation is evaluated according to the credibility of recommender. PeerTrustdefines community and transaction context parameters in order to address application specific features of interactions. SORT (Ahmet Burak Can 2013) trust model is newly proposed reputation based trust model which has fair approaches to form a trust among peers. These models used by many application of file sharing and distribute processing. These four approaches are mentioned in brief in following section.

1. Policy-based Trust Management Systems

In credential and policy-based trust management systems, peers use credential verification to establish a trust relationship with other peers . Since the primary goal of such systems is to enable access control, their concept of trust management is limited to verifying credentials and restricting access to resource according to application-defined policies.

Policymaker is a trust management system that facilitates the development of security features including privacy and authenticity for different kinds of network applications. It provides each peer with local control to specify its policies: using Policymaker a peer may grant another peer access to its service if the providing peer can determine that the requesting peer's credentials satisfy the policies. The policy-based access control trust mechanisms do not incorporate the need of the requesting peer to establish trust in the resource-owner; therefore, they by themselves do not provide a complete generic trust management solution for all decentralized applications.

2.2 Reputation-based Trust Management System

Trust management is any mechanism that allows establishing mutual trust. Reputation is a measure that is derived from direct or indirect knowledge on earlier interactions of peer , and it is used to access the level of trust an agent puts into another agent. Thus, reputation-based trust management is one specific form of trust management. (Chen Ding)

Reputation-based trust management systems on the other hand provide a mechanism, by which a peer requesting a resource may evaluate the trust in the reliability of the resource and the peer providing the resource. Examples of such systems include SPORAS and HISTOS, XRep, NICE, DCRC/CORC, EigenRep, etc. Peers in such systems establish trust relationships with other peers and assign trust values to these relationships. Trust value assigned to a trust relationship is a function of the combination of the peer's global reputation and the evaluating peer's perception of that peer.

Abdul-Rahman et al. proposed a decentralized approach to trust management and a recommendation protocol to compute trust related information. Each entity has its own trust relationship database. They make use of different trust categories, a scale of trust values on recommendations and direct trust values. In order to get a recommendation, an entity sends recommendation requests to its trusted recommenders. Results from different paths are collected and averaged. Each path is computed based on recommender trust value of recommenders and recommended trust value returned.

NICE is a platform for implementing cooperative applications over the Internet. It works in a purely decentralized fashion and each peer stores and controls data that benefits itself. Applications based on NICE barter local resources in exchange for access to remote resources. NICE provides three main services: resource advertisement and location, secure bartering and trading of resources, and distributed trust evaluation. NICE uses two trust mechanisms to protect the integrity of the cooperative groups: trust-based pricing and trust-based trading limits. One of the main contributions of the NICE approach is the ability of good peers to form groups and to isolate malicious peers.

Reputation based Trust management has been implemented in large scale. EigenRep and DMRep contribute more on proposing a computational model of trust and P2PRep and XRep that focus on the security concerns of reputation-based systems.

2.3 Social Network-based Trust Management Systems

Social network-based trust management systems utilize social relationships between peers when computing trust and reputation values. In particular, these systems form conclusions about peers through analyzing a social network that represents the relationships within a community. Other examples of such trust management systems include Regret that identifies groups using the social network, and Node Ranking that identifies experts using the social network.

2.4 Recommendation based Trust Management Systems

Recommendation based trust management in which peers takes the recommendation from other peers before take the service. Eigentrust and Peertrust evaluate a recommendation based on trustworthiness of the recommender. (Ahmet Burak Can 2013)

3. Existing Trust Models in Peer to Peer System

There are many trust models, some are noted as follows 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*** complaints 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.

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 assign 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 change 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 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 untampered 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.

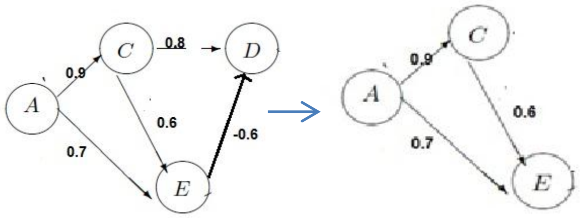


Fig3 A. directed graph with trust paths between peers .

At last peers are removed which are having negative feedback cookies.

Eigentrust

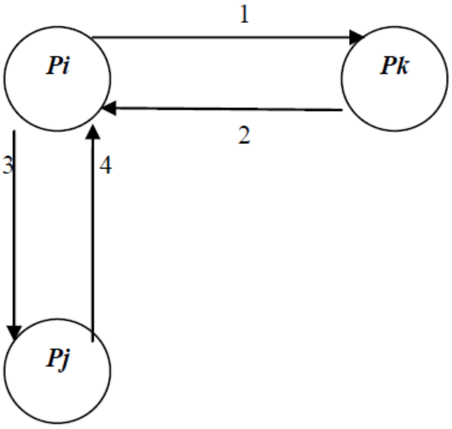
This is distributed algorithm to decrease the number of downloads of inauthentic files in a peer-to-peer file-sharing network that assigns each peer a unique global trust value, based on the peer's history of uploads. Eigen Trust model is designed for the reputation management of P2P system. The global 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 $C_{ij,}$ 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.

$$C_{i,j} = (Max(Si,j))/\sum Max(Si,j)$$

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. (Li Xiong and Ling Liu). This Eigentrust is meant for protection from inauthentic file accessment in peer to peer interaction.

SORT

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 **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 th eir 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.

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. (Ahmet Burak Can 2013)

4. Comparison of the Trust algorithms

There are some algorithms which have been proposed for reputation-based trust management in P2P systems. In this section, let's to examine the differences among them. There are many approaches which can be compared relatively(Hai Ren 2012).

Table 1 Different Approaches of trust management

Approaches	Significance
Policy-based	Use credential verification to establish a trust relationship with other peers but no peer's capability is considered
Reputation-based	Mutual Trust by reputation is a measured that is derived from direct or indirect knowledge on earlier interactions.
Social Network-based	Utilize social relationships between peers when computing trust and reputation values
Recommendation based	Trust is only maintained by the recommendations by other peers.

Table 2 Different Techniques in trust management

Model	Significance
SORT	Uses Reputation and recommendation based approach, Trust Values on the basis of service and recommendations
EIGENTRUST	Uses Reputation based approach and accordingly trust values are evaluated
NICE	Use of cookies which tells negative and positive feedback of peer.
Global Trust Model	Mutual communication is required to a trust calculation and use of Binary Trust is maintained.

EigenTrust scheme is proposed by Kamvaret al., 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.

Finally 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.

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

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

Chen Ding, Chen Yueguo, Cheng Weiwei(2012), E-Book Of Trust Management in P2P Systems.

Jussi Kangasharju(2011), E-Book OfIntroduction Peer-to-Peer Networks.

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

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

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

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

Li Xiong and Ling Liu(2004), PeerTrust :Supporting reputation based trust model, *IEEE Knowledge and engineering* vol. 16 no. 7 pp. 843-857.

K. Aberer, Z. Despotovic (2001) Managing Trust in a Peer-2-Peer Information System, *In Proc. of the IX International Conference on Information and Knowledge Management*, Atlanta, Georgia.