Volume 3, Issue 9, September 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# Survey on Large Scale Overlay for Query Processing in P2P Network

**Mamatha G**
M. Tech Student
Department of CSE
East West Institute of Technology
Bangalore, India

**Chandanraj B R**
Assistant Professor
Department of CSE
East West Institute of Technology
Bangalore, India

***Abstract- The scalability of a feedback aggregating overlay is the most fundamental requirement for large-scale P2P computing .In Peer-to-Peer (P2P) trust management feedback provides an efficient and effective way to build a reputation-based trust relationship among peers. In this paper, we proposed a scalable feedback aggregating (SFA) overlay for large-scale P2P trust evaluation. The local trust rating method is defined based on the time attenuation function, which can satisfy the two dynamic properties of trust. More importantly, based on the SFA overlay, an adaptive trustworthiness computing method can be defined the SFA-based trust model has greater adaptability and accuracy in handling various dynamic behaviors of peers. The SFA overlay is then proposed to strengthen the scalability of the feedback aggregation mechanism for large-scale P2P applications, but it can also reduce networking risk and improve system efficiency. We present a trust based content distribution for peer-to-peer overlay networks, which is built on the trust management scheme. The main concept is, before sending or accepting the traffic, the trust of the peer must be validated. The main concept is, before sending or accepting the traffic, the trust of the peer must be validated. Based on the success of data delivery and searching time, we calculate the trust index of a node. Then the aggregated trust index of the peers whose value is below the threshold value is considered as distrusted and the corresponding traffic is blocked.***

***Key terms- Scalability, Adaptability, Scalable feedback aggregating overlay, P2P trust management.***

## 1. Introduction

**Peer to peer** is an approach to computer networking where all computers share equivalent responsibility for processing data. Peer-to-peer networking (also known simply as *peer networking*) differs from client-server networking, where certain devices have responsibility for providing or "serving" data and other devices consume or otherwise act as "clients" of those servers. With the aid of this you can configure computers in peer to peer *workgroups* to allow sharing of files, printers and other resources across all of the devices. Peer networks allow data to be shared easily in both directions, whether for downloads to your computer or uploads from your computer. Due to the distributed nature of P2P systems there is no central point of attack but such kind of an architecture makes P2P networks very prone to malicious attacks by other peers like sending Trojans, Worms, Viruses, Fake files etc. Trust management is essential to overcome from the above attacks. Reputation systems provide a way for building trust through social control by utilizing community based feedback about past experiences of peers to help making recommendation and judgment on quality and reliability of the transactions. The challenge of building such a reputation based trust mechanism in a P2P system is to effectively cope up with various malicious behaviors of peers such as providing fake or misleading feedback about other peers. The most general mechanism of establishing trust among peers is using the reputation of the peers providing the resource. The users can rate the reliability of those peers with which they have dealt in the past. A peer requesting a resource can evaluate the trust ratings of the peer providing the resources using the reliability ratings of those peers which have dealt with the same peer in the past. The main challenge is the way to incorporate various contexts in building trust as they vary in different communities and transactions. Further, the effectiveness of a trust system depends not only on the factors and metrics for building trust, but also on the implementation of the trust model in a P2P system. Most existing reliable reputation mechanisms require a central server for storing and distributing the reputation information. It remains a challenge to build a decentralized P2P trust management system that is efficient, scalable, reliable, and secure in both trust computation and trust data storage and dissemination. Last, there is also a need for experimental evaluation methods of a given trust model in terms of the effectiveness and benefits. To promote availability and alleviate the worries of a large number of users, we must design the P2P ecosystem to be secure, trustworthy, and dependable. Trust management is especially necessary in commercial P2P applications, such as P2P file-sharing [1],trusted content delivery [2], pay per-transaction [3], etc.

## 2. Related Work

Ruichuan Chen et al [4] have proposed a unique poisoning-resistant security framework based on the idea that the only trusted sources to verify the integrity of the requested content would be the content providers. A content provider

 

publishes the information of his shared contents to a group of content maintainers self-organized in a security overlay, to present the mechanisms of availability and scalability. Hence a content requestor can confirm the integrity of the requested content from the associated content maintainers. They have devised a scalable probabilistic verification scheme, to further enhance the system performance. Thomas Repantis[5] have proposed a decentralized trust management middleware, based on reputation for unstructured, ad-hoc, peer-to-peer networks. In their middleware to requests for data or services, the reputation information of each peer is stored in its neighbors and piggy-backed on its replies. In self-organizing networks the lack of structure and the dynamic nature of the network are usually regarded as barriers in managing trust information. Their approach utilizes these characteristics to build a self organizing, non intrusive trust management infrastructure resistant to tampering and collusions.

Mujtaba Khambatti[6] have proposed an approach for trust management in P2P systems. They have established an optimistic role-based model for trust amongst peers and prove that it is scalable, dynamic, revocable, secure and transitive. Their proposed solution allows asymmetric trust relationships that can be verified by any peer in the system through a simple, low-cost algorithm. The authors have introduced a metric known as iComplex which combines a peer's trust value for each of its roles into a single, relative, probabilistic guarantee of trust. Finally, they have also discussed the no repudiation of peer relations and how their trust model allows peers to revoke relationships with malicious peers. Rahman and Hailes [7] proposed a method that can be implemented in P2P networks. This work is based on Marsh's model. Actually it is a kind of adaptation of Marsh's work to today's online environments. Some concepts were simplied (for example, trust can have only four possible values) and some were kept (such as situations or contexts). But the main problem with this approach is that every agent must keep rather complex and very large data structures that represent a kind of global knowledge about the whole network.In real word situations maintaining and updating these data structures can be a labourous and time consuming task. Also it is not clear how the agents obtain the recommendations and how well the model will scale when the number of agents grows. Xiong and Liu [8] presented an approach that avoids aggregation of the individual interactions. Their Peer Trust system computes the trustworthiness of a given peer as the average feedback weighted by the scores of the feedback originators. The limitation of this approach is that the computation convergence rate in large-scale P2P systems is not provided. The five factors used in their trust model must be retrieved with a heavy overhead.

The EigenTrust mechanism [9] aggregates trust information from peer by having them perform a distributed calculation approaching the eigenvector of the trust matrix over the peers. EigenTrust relies on good choice of some pre-trusted peers, which are supposed to be trusted by all peers. This assumption may be over optimistic in a distributed computing environment. The reason is that pre-trust peers may not last forever. Once they score badly after some transactions, the EigenTrust system may not work reliably.

## 3. System Design

The SFA overlay regards scalability as the first requirement of a trust system; i.e., our trust mechanism is scalable to serve a large number of peers in terms of convergence speed, extra overhead per peer, and so on. Additionally, using this trust evaluation mechanism, our trust system can partly mend the accuracy of the feedbacks evaluation with a small number of buddies.

### 3.1 Constraints

#### 3.1.1 A Scalable Feedback Aggregating Overlay

Based on a scalable perspective, we present the SFA overlay. Feedback is searched using the SFA instead of the polling based methods used in previous works. Not only can this strengthen the scalability of feedback aggregation mechanism for large-scale P2P applications, but it can also reduce risk and improve system efficiency.

#### 3.1.2 An Innovative Local Trust Rating Method Based on Time Attenuation Function

The dynamic property of trust creates the greatest challenge in measuring trustworthiness. In this paper, we propose an innovative computing method for LTD based on the time attenuation function, which can satisfy two social properties of trust: the dynamics and time-based attenuation.

#### 3.1.3 An Adaptive Weight Allocation Method for GTD Calculation

Many previous studies have used subjective means to assign various weights for trust factors. The adaptability of these models has limitations. Based on the human cognitive process, we use a novel self-feedback mechanism to integrate peers' local trust scores into the overall trust evaluation. This mechanism can overcome the effect of the rigidity of assigned weights on the overall trust perception and evaluation. A Risk-Probabilistic-Based Method to Combat Raters' Misbehavior in P2P networks, some raters may be misbehaving peers (e.g., colluding cheaters). They may exaggerate the positive or negative ratings, or offer testimonies that are outright false. Focusing on this issue and based on the risk probabilistic model in economics, we propose a feasible method to combat raters' misbehavior or at least make raters' misbehavior costly.

#### 3.1.4 A Pretty Good Privacy (PGP)-Based Signature Mechanism to Support Identity-related Issues

Identity support is probably the most crucial element in a security and trusted service system. However, P2P systems lack infrastructure services to support public key cryptographic mechanisms that rely on a trusted CA. We adopt a PGP-based signature mechanism to support identity-related issues in a fully self-organized manner, which can better meet the identity-related issues in the SFA overlay. We also design the key techniques to be simple in implementation over pure P2P networks, so that the mechanism can be incorporated into the existing P2P overlay network.

### 3.1 System Architecture

The fundamental role of our trust system is to monitor the behaviors of other entities and collect, aggregate, and distribute feedback.The architecture of the trust management system we have developed is depicted in. Trust decision-

 

making module (TDM) is deployed at each peer by a special software agent. It comprises three core components: trust context collector (TCC), trust information processor (TIP), and trust context emitter (TCE). TCC is used to gather feedback from FRs. TIP uses the related algorithms to calculate an aggregated representation of a peer's trustworthiness. TCE makes the results available to other requesting peers.

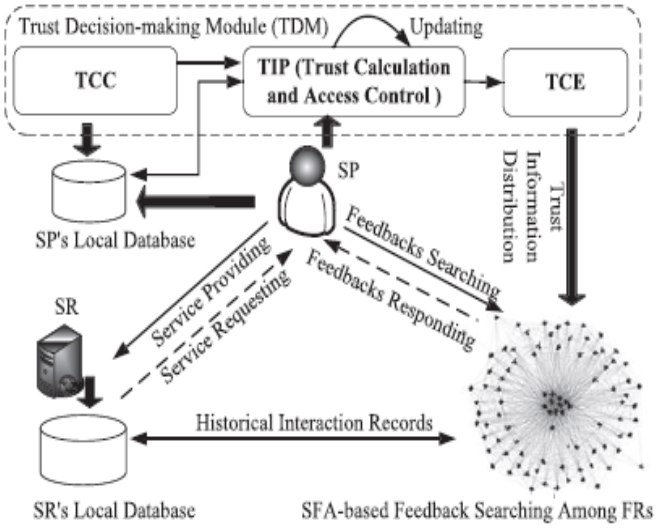


**Fig 1 System Architecture**

**3.3 Pseudo Code**

**3.1 Pseudo code Query Processing and Cache**

```
Wait for Query Request
    If (Request Received)
      Select The Node for Query  Distribution
      Send Pack to The Surrounding Nodes
If(Check for Cached Data)
     Store The Data to Database for Caching
Else
     Pass The Data To The Requester
```

**3.2 Pseudo Code for Multicasting on Overlay Network**

```
Join  The Overlay Network
  Load  The Query
     Request For Transfer
If(Joining Successful)
     Multicast The Data to All The Nodes
Else
     Retry Joining
```

**3.3 Modules**

- Overlay Creation Module
- Data Aggregation Module
- Routing Table Manager Module
- Query Manager Module
- Certificate Manager Module

Overlay Creation Module: This Overlay Network is built on top of the peer network that provides one to many communication and one to one communication.

Data Aggregation Module: This module aggregates the data from all the intermediate nodes and have their results in temporary cache.

Routing Table Manager Module: This module maintains a nodes Id and Local Trust Degree which gives the scalable feedback. It generates to construct the near reachable node via multicasting Query to all nodes.

Query Manager Module: The Module Broadcast a message to all the nodes via Multicast Query.

Certificate Manager Module: The trust based communication protocol using certificate management and hashing to authenticate the message.

## 4. Conclusion

Through our design we have analyzed that the SFA overlay, which not only can significantly enhance the scalability of the trust system, but can also reduce the risk and improve system efficiency.Combining trust management with intrusion detection to address the concerns of sudden and malicious attacks.we intend to deploy related algorithms in a practical decentralized setting to observe the effectiveness of proposed trust techniques where many registry peers exchange among each other information about users, and services' quality data.

 

**References**

[1] M. Ripeanu, I. oster, and A. Iamnitchi, "Mapping the Gnutell Network: Properties of Large-Scale P2P Systems and Implications for System Design," IEEE Internet Computing, vol. 6, no. 1, pp. 50-57, Sept. 2002.

[2] S. Saroiu, K.P. Gummadi, R.J. Dunn, S.D. Gribble, and H.M. Levy,"An Analysis of Internet Content Delivery Systems," Proc. Fifth Symp. Operating Systems Design and Implementation (OSDI '02),pp. 86-90, 2002.

[3] L. Liu and W. Shi, "Trust and Reputation Management," IEEE Internet Computing, vol. 14, no. 5, pp. 10-13, Sept./Oct.2010.

[4] Ruichuan Chen, Eng Keong Lua, Jon Crowcroft, Wenjia Guo, Liyong Tang, Zhong Chen, "Securing Peer-to-Peer Content Sharing Service from Poisoning Attacks", pp. 22-29, 8th International Conference in p2p computing, IEEE, 2008.

[5] Thomas Repantis Vana Kalogeraki, "Decentralized Trust Management for Adhoc Peer to Peer Networks", ACM, MPAC: Vol.182, Proceedings of the 4th international workshop on Middleware for Pervasive and Ad-Hoc Computing (MPAC 2006), USA.

[6] Mujtaba Khambatti, Partha Dasgupta, Kyung Dong Ryu, "A Role-Based Trust Model for Peer-to- Peer Communities and Dynamic Coalitions", Second IEEE International Information Assurance Workshop (IWIA'04), pp. 141-154, April 2004.

[7] A. Abdul-Rahman and S. Hailes: Supporting Trust in Virtual Communities Proceedings of the 33rd Hawaii International Conference on System Sciences, 2000.

[8] L. Xiong and L. Liu, "PeerTrust: Supporting Reputation based Trust for Peer-to-Peer Electronic Communities", IEEE Trans. Knowledge and Data Engineering, Vol.16, No.7,2004, pp. 843-857.

[9] S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The Eigentrust Algorithm for Reputation Management in P2P Networks", ACM WWW'03, Budapest, Hungary, May 2003.

 