PROFICIENT DATA TRUST MODEL FOR LARGE SCALE P2P WITH FEEDBACK AGGTEGATION

Mr.S.Annamalai M.E.+., Ms.A.UMA M.E.+., Ms.N.SATHYA M.E (CSE)*

**- Department of Computer Science and Engineering, PGPCET, Namakkal.*
+- Assistant Professor, Department of Computer Science and Engineering,
PGP College of Engineering and Technology, Namakkal

ABSTRACT

In Peer-to-Peer (P2P) trust management, feedback provides an efficient and effective way to build a reputation-based trust relationship among peers. There is no doubt that the scalability of a feedback aggregating overlay is the most fundamental requirement for large-scale P2P computing. However, most previous works either paid little attention to the scalability of feedback aggregating overlay or relied on the flooding-based strategy to collect feedback, which greatly affects the system scalability. A scalable feedback aggregating overlay for large-scale P2P trust evaluation. First, the local trust rating method is defined based on the time attenuation function, which can satisfy the two dynamic properties of trust. The SFA overlay is then proposed from a scalable perspective. Not only can the SFA overlay strengthen the scalability of the feedback aggregation mechanism for large-scale P2P applications, but it can also reduce networking risk and improve system efficiency. More importantly, based on the SFA overlay, an adaptive trustworthiness computing method can be defined.

This method surpasses the limitations of traditional weighting methods for trust factors, in which weights are assigned subjectively. Finally, the authors design the key techniques and security mechanism to be simple in implementation for the easy incorporation of the mechanism into the existing P2P overlay network. Through theoretical and experimental analysis, the SFA-based trust model shows remarkable enhancement in scalability for large scale P2P computing, as well as has greater adaptability and accuracy in handling various dynamic behaviors of peers.

Index Terms: P2P, Trust Management, Feedback Rating, Trust Model Processing, distributed hash table

I.INTRODUCTION

A distributed system is a decentralized network consisting of a collection of autonomous computers that communicate with each other by exchanging messages. These systems are scalable and fault tolerant, and they allow easy resource sharing, concurrent processing, and transparent operation. As the Internet's popularity grows, distributed applications such as e-commerce are becoming important. In addition, with the rapid development of network and communication technologies, new forms of distributed systems such as peer-to-peer (P2P) networks and mobile ad hoc networks—are quickly emerging. Trust is an important issue in distributed systems. Transactions in distributed systems can cross domains and organizations, and not all domains can be trusted to the same level. Even within the same domain, users' trustworthiness can differ. A flexible and general-purpose trust management system can maintain current and consistent trustworthiness information for the different entities in a distributed system. In e-commerce, for example, a trust management system lets a buyer and seller become acquainted with each other and estimate the risk of participating in a transaction, thus minimizing the loss. In P2P systems, where each entity acts as both client and server and is expected to contribute to the system, trust management can help reduce free riding, which can seriously degrade P2P system performance.

A major challenge for large-scale P2P systems is how to establish trust between different peers without the benefit of trusted third parties or authorities. Usually the peers don't have any pre-existing relationship and may reside in different security domains. Sometimes even when there are some authorities available, e.g., an authentication server or certification authority, it is inadvisable to assume that these authorities can monitor transactions and then declare the trustworthiness of different peers. The research of trust in security focuses on creating, acquiring, and distributing certificates.

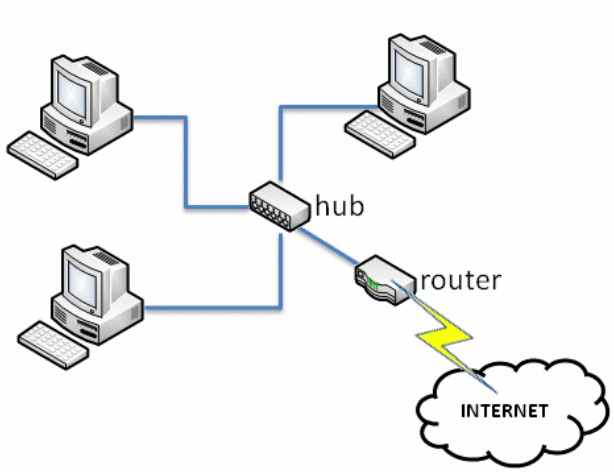

Fig 1. Peer-to-Peer Network

A conventional certificate chain, even if perfect and not compromised, would at best attest to the identity of the given party, but would not be able to guarantee that the given party is in fact trustworthy for a particular purpose at hand. Trust is a complex subject, and no unanimous definition of trust exists. The Merriam-Webster's Dictionary defines trust as "assured reliance on the character, ability,

strength, or truth of someone or something." Dictionary.com describes trust as the "firm reliance on the integrity, ability, or character of a person or thing." We define trust as the belief that an entity is capable of acting reliably, dependably, and securely in a particular case. Trust management entails collecting the information necessary to establish a trust relationship and dynamically monitoring and adjusting the existing trust relationship. The various models for describing trust and trust establishment in distributed systems include public-key cryptography, the resurrecting duckling model, and the distributed trust model.

II.RELATED WORKS

Metadata produced by members of a diverse community of peers tend to contain low-quality or even mutually inconsistent assertions. Trust values computed on the basis of users' feedback can improve metadata quality and reduce inconsistency, eliminating untrustworthy assertions. In this paper, we describe an approach to metadata creation and improvement, where community members express their opinions on the trustworthiness of each assertion. Our technique aggregates individual trustworthiness values to obtain a community-wide assessment of each assertion. We then apply a global trustworthiness threshold to eliminate some assertions to reduce the Meta database's overall inconsistency. The growing need of share and manage knowledge about data is strictly connected to the interest in studying and developing systems for generating and managing metadata.

Typically, metadata provide annotations specifying content, quality, type, creation, and spatial information of a data item. Though a number of specialized formats based on Resource Description Framework (RDF) are available, metadata can be stored in any format such as a text file, extensible Markup Language (XML), or database record. There are a number of advantages in using information extracted from data instead of data themselves. First of all, because of their small size compared to the data they describe, metadata are more easily shareable than data. Thanks to metadata share ability, information about data becomes readily available to anyone seeking it. Thus, metadata make data discovery easier and reduces data duplication. On the other hand, metadata can be generated by a number of sources (the data owner, other users, automatic tools) and May or may not be digitally signed by their author.

Therefore, metadata have non-uniform trustworthiness. To take full advantage of metadata, it is fundamental that (i) users are aware of each metadata level of trustworthiness;(ii) metadata trustworthiness is continuously updated, for example, based on the view of the user community. This is even more important when the original sources of metadata are automatic metadata generators whose error rates are not negligible, or when metadata are created via peer certifications, that is, via assertions by users that other users belong to a category or have a given property.

Peer-to-Peer (P2P) computing is widely recognized as a promising paradigm for building next generation distributed applications, ranging from large scale scientific applications to mobile ad hoc information sharing, by federating dispersed pools of geographically distributed resources under loosely coordinated control. However, the autonomous, heterogeneous, and decentralized nature of participating peers across multiple administrative domains introduces the challenge for resource sharing in such an environment: how to make the peers profitable in the decentralized resource sharing under the untrusted P2P environment. To address the problem, in this paper we present a self-policing and distributed approach by combining two models: PET, a Personalize Trust model, and M-CUBE, a multiple-currency based economic model, to lay a foundation for resource sharing in an untrusted P2P computing environment.

PET is a flexible trust model that can adapt to different requirements, and provides the solid support for the currency management in M-CUBE. With the help of the trust management and the merits of the economics, M CUBE provides a novel self-policing and quality-aware framework for the sharing of multiple resources, including homogenous and heterogeneous resources. We evaluate the efficacy and performance of this approach in the context of a real application, a peer to peer Web server sharing.

In peer-to-peer (P2P) systems, peers often must interact with unknown or unfamiliar peers without the benefit of trusted third parties or authorities to mediate the interactions. A peer will need reputation mechanisms to incorporate the knowledge of others to decide whether to trust another party in P2P systems. This paper discusses the design of reputation mechanisms and proposes a novel distributed reputation mechanism to detect malicious or unreliable peers in P2P systems. It illustrates the process for rating gathering and aggregation and presents some experimental results to evaluate the proposed approach. Moreover, it considers how to effectively aggregate noisy (dishonest or inaccurate) ratings from independent or collusive peers using weighted majority techniques. Furthermore, it analyzes some possible attacks on reputation mechanisms and shows how to defend against such attacks. This paper proposes a distributed reputation mechanism for P2P systems in general, e.g., multiagent systems (each peer is a software agent), and the web services (each peer is a web service provider), where binary ratings cannot accurately model a peer's experience of the quality of service (QoS) with other peers. This paper focuses on the design of reputation mechanisms on unstructured P2P systems, and does not consider structured P2P systems with Distributed Hash Tables. One reason is that DHTs are mainly designed for distributed storage systems, while the high turnover rate caused by frequent join and leave of peers in dynamic P2P systems causes significant overhead for DHTs.

III. PROPOSED METHODOLOGY

Ratings Generation: The ratings in existing approaches are binary. In the binary ratings, a peer rates the services from another peer as one of two values, commonly interpreted as either one (e.g., positive or satisfactory) or zero (e.g., negative, unsatisfactory). Binary ratings work pretty well for file sharing systems where a file is either the definitive correct version or is wrong, but cannot accurately model richer services in other settings such as web services and electronic commerce, where a boolean may not adequately represent a peer's experience of the quality of service (QoS) with other peers, e.g., the quality of products the peer sends and the expected delivery time. Our approach considers quality of service (QoS) as probabilistic ratings in the interval [0; 1] and focuses on how to aggregate these ratings.

Ratings Discovery: The polling algorithms for ratings discovery are based on Gnutella protocols, in which the requesting peer broadcasts the message to all other peers within the horizon of a given TTL (Time to Live). Polling processes waste much bandwidth and processing power since each peer queries all of its neighbors. Our approach applies a process of referrals through which peers help one another find witnesses. The process of referrals requires that any referrals.

Ratings Aggregation: Although some of the existing approaches consider the credibility's of voters (or witnesses) in the enhanced polling protocol, they don't consider how to effectively aggregate the noisy ratings in presence of dishonest or unreliable voters. We discuss different models of deception in the process of rating aggregation, e.g., complementary, exaggerated positive, and exaggerated negative, and study how to distinguish reliable peers from deceptive or unreliable peers. The focus of this paper is on minimizing the effect of ratings from these independent or collusive peers using weighted majority techniques.

High accuracy. To help distinguish reputable peers from malicious ones, the system should calculate the reputation scores as close to their real trustworthiness as possible.

Low overhead. The system should only consume limited computation and bandwidth resources for peer reputation monitory and evaluation.

Adaptive to peer dynamics. Peer joins and leaves an open P2P system dynamically. The system should adapt to this peer dynamics instead of relying on predetermined peers.

Robust to malicious peers. The system should be robust to various attacks by both independent and collective malicious peers.

Scalability: The system should be able to scale to serve a large number of peers in term of accuracy, convergence speed, and extra overhead per peer.

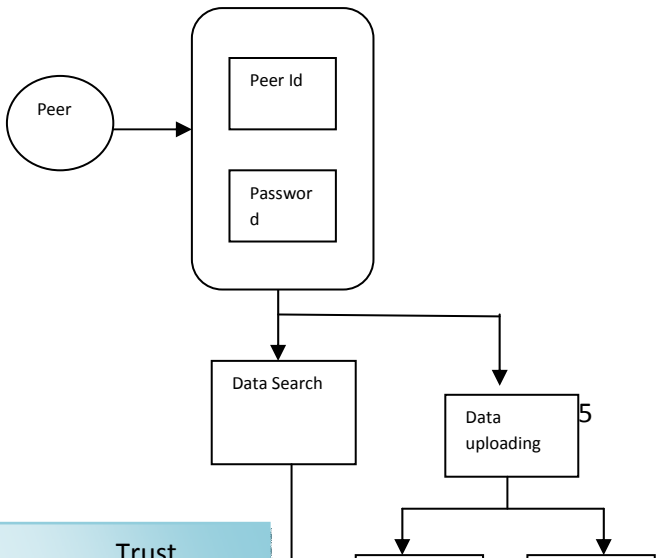

Fig 2.Architecture Diagram

IV. IMPLEMENTATION MECHANISM

Our overlay can be constructed in a Gnutella-based P2P network, with architecture similar to that of P2P, which is a pure P2P network for file exchange, and, more precisely, in the Gnutella architecture. The reason for focusing on a pure P2P network is that it is closest to the ideal structure of the peer-to-peer (P2P) spirit, where all participants have a uniform role. In the SFA overlay, each peer should hold a set of buddies, a subset of which is identified as its neighbors. In order to construct the SFA overlay on top of purely unstructured P2P networks, a data table (called buddy table) is applied in every peer's local database. Each peer (as an SP) maintains a buddy table. If another peer (as an SR) has direct interactions with it, then the LTD of the peer (SR) will be recorded in this table and the peer (SR) becomes a buddy of the SP. To manage online status of a peer, an item is added in each peer's buddy table. This item is called "online mark," when a peer (SR) joins the SFA overlay, the SP will set the SR's "online mark" as "yes." While a peer (SR) leaves the SFA overlay, the SP will set the SR's "online mark" as "no." Thus, the main items of the buddy table include the buddy's ID, LTD, online mark and other items.

V. CONCLUSION

In this paper, through a scalable perspective, the SFA overlay is presented, which not only can significantly enhance the scalability of the trust system, but can also reduce the risk and improve system efficiency. Meanwhile, based on the SFA overlay, an adaptive GTD computing method can be defined. This method surpasses the limitations of the existing approaches, where weights of the trust factors are assigned subjectively.

We are interested in combining trust management with intrusion detection to address the concerns of sudden and malicious attacks. Implementing and evaluating our proposed model on various P2P systems, such as distributed file sharing and P2P grid computing, is another direction for future research.

REFERENCES

- H. Li and M. Singhal, "Trust Management in Distributed Systems," Computer, vol. 40, no. 2, pp. 45-53, 2007.

- X. Li and X. Gui, "Research on Dynamic Trust Model in LargeScale Distributed Environment," J. Software, vol. 18, no. 6, pp. 1510-1521, 2007.
- F. Cornelli, E. Damiani, S.D.C. di Vimercati, S. Paraboschi, and P. Samarati, "Choosing Reputable Servents in a P2P Network," Proc. 11th Int'l World Wide Web Conf., pp. 376-386, 2002.
- E. Damiani, S.D.C. di Vimercati, S. Paraboschi, and P. Samarati, "Managing and Sharing Servants' Reputations in P2P Systems," IEEE Trans. Knowledge and Data Eng., vol. 15, no. 4, pp. 840-854, July/Aug. 2003.
- E. Damiani, S.D.C. di Vimercati, S. Paraboschi, P. Samarati, and F. Violante, "A Reputation-Based Approach for Choosing Reliable Resources in Peer-to-Peer Networks," Proc. Ninth ACM Conf. Computer and Comm. Security, pp. 207-216, 2002.
- R. Aringhieri, E. Damiani, S.D.C. di Vimercati, S. Paraboschi, and P. Samarati, "Fuzzy Techniques for Trust and Reputation Management in Anonymous Peer-to-Peer Systems," J. Am. Soc. for Information Science and Technology, vol. 57, no. 4, pp. 528-537, 2006.
- E. Damiani, S.D.C. di Vimercati, P. Samarati, and M. Viviani, "A WOWA-Based Aggregation Technique on Trust Values Connected to Metadata," Electronic Notes in Theoretical Computer Science, vol. 157, no. 3, pp. 131-142, 2006.
- L. Xiong and L. Liu, "Peer-Trust: Supporting Reputation-Based Trust in Peer-to-Peer Communities," IEEE Trans Data and Knowledge Eng., vol. 16, no. 7, pp. 843-857, July 2004.
- Z. Liang and W. Shi, "TRECON: A Trust-Based Economic Framework for Efficient Internet Routing," IEEE Trans. Systems, Man, and Cybernetics, Part A: Systems and Humans, vol. 40, no. 1, pp. 52-67, Jan. 2010.
- Z. Liang and W. Shi, "Enforcing Cooperative Resource Sharing in Untrusted Peer-to-Peer Environments," J. Mobile Networks and Applications, vol. 10, no. 6, pp. 771-783, 2005.
- B. Yu, M.P. Singh, and K. Sycara, "Developing Trust in Large- Scale Peer-to-Peer Systems," Proc. IEEE First Symp. Multi-Peer Security and Survivability, pp. 1-10, 2004.
- A.A. Selcuk, E. Uzun, and M.R. Pariente, "A Reputation-Based Trust Management System for P2P Networks," Int'l J. Network Security, vol. 6, no. 2, pp. 227-237, 2008.
- P. Dewan and P. Dasgupta, "P2P Reputation Management Using Distributed Identities and Decentralized Recommendation Chains," IEEE Trans. Knowledge and Data Eng., vol. 22, no. 7, pp. 1000-1013, July 2010.
- R. Zhou and K. Hwang, "Power-Trust: A Robust and Scalable

Reputation System for Trusted Peer-to-Peer Computing," IEEE Trans. Parallel and Distributed Systems, vol. 18, no. 5, pp. 460-473, Apr. 2007.

- R. Zhou, K. Hwang, and M. Cai, "GossipTrust for Fast Reputation Aggregation in Peer-to-Peer Networks," IEEE Trans. Knowledge and Data Eng., vol. 20, no. 9, pp.1282-1295, Sept. 2008.
- 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.
- 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.
- L. Liu and W. Shi, "Trust and Reputation Management," IEEE Internet Computing, vol. 14, no. 5, pp. 10-13, Sept./Oct. 2010.
- 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.
- X. Li, F. Zhou, and X. Yang, "Developing Dynamic P2P Trust Model Using Theory of Entropy-Based Multi-Source Information Fusion," Int'l J. Innovative Computing, Information and Control, vol. 7, no. 2, pp. 777-790, 2011.