ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

A Trust Management Scheme in Peer to Peer Systems

[I]Manju John, [II]Govindaraj.E
[I,II]Dept. of CSE, MES College of Engineering

Abstract
Trust management in P2P system is used to detect malicious behaviours and to promote honest and cooperative interactions. In this report, we first present a computational model that shows the relationships between peers based on trust . This model can be implemented in a real system to consistently calculate trust scores for each peer.Trust between direct neighbours can be calculated based on analysing earlier transactions of peers and if indirect neighbours trust is calculated based on recommendations or feedbacks. In this way each peer develops its own local view of trust about the peers interacted in the past .

Keywords
Peer-To-Peer Computing, Reputation System,Trust Management,Recommendation Trust,Security.

I. Introduction

PEER-to-peer (P2P) systems are driving a major paradigm shift in the era of distributed computing.In a P2P infrastructure, the traditional distinction between clients and backend (or middle tier application) servers is simply disappearing. Every node of the system acts the role of a client and a server. A P2P system can be characterized by a number of properties: no central coordination, no central database, no peer has a global view of the system, global behaviour emerges from local interactions, peers are autonomous, and peers and connections are unreliable.

Trust management in P2P system is used to detect malicious behaviours and to promote honest and cooperative interactions. Creating long-term trust relationships among peers can provide a more secure environment by reducing risk and uncertainty in future P2P interactions. Interactions and feedbacks of peers provide information to measure trust among peers. This makes assessment of trustworthiness a challenge. Trust management in P2P system can be classified into 3 categories : credential and policy-based trust management,social network-based trust management and reputation-based trust management. 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. 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.

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 agents, 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. We specially look into the area of reputation-based trust management systems. The basic problem related to reputation-based trust management in P2P networks is that information about transactions performed between peers (agents) is dispersed throughout the network so that every peer can only build an approximation of 'the global situation in the network'. Of course this is further complicated by the fact that agents storing and processing trust related data cannot be considered as unconditionally trustworthy and their eventual malicious behavior must be taken into account, too. Thus, reputation-based trust management is one specific form of trust management. 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.Sharing knowledge between peers is one of the ways to make at least some trust among peers.

Outline of the paper is as follows: Section 2 discusses therelated research. Section 3 explains the computational model of existing approach SORT. Section 4 presents the proposed method and section 5 presents simulation experiments and results. Section 6 summarizes the results and possible future work directions. Malicious peers have more attack opportunities in P2P trust models due to lack of a central authority. Researches are always being conducted to improve the accuracy and efficiency of the trust management in peer-to-peer systems. Some of the innovative approaches are described.

II. Literature Survey

Malicious peers have more attack opportunities in P2P trust models due to lack of a central authority.Researches are always being conducted to improve the accuracy and efficiency of the trust management in peer-to-peer systems. Some of the innovative approaches are described. On a structured P2P system, a DHT structure can provide decentralized and efficient access to trust information. In Aberer and Despotovics trust model [1], peers report their complaints by using P-Grid. A peer is assumed as trustworthy unless there are complaints about it. However, preexistence of trust among peers does not distinguish a newcomer and an untrustworthy one.

Eigentrust[2] uses transitivity of trust to calculate global trustvalues stored on CAN.The basic idea of secure algorithm 2 is that the trust value of one peer is computed by some other peers. Those peers are called mothers which are responsible for computing their daughters global reputation values. The reason for using more than one other peer to compute a peers reputation value is that some mothers may be malicious peers and they report false trust values for their daughters.

PeerTrust [4] defines transaction and community context parameters to make trust calculation adaptive on P-Grid. While transaction context parameter addresses application dependent factors, community context parameter addresses P2P community related issues such as creating incentives to force feedbacks

Power Trust [5] constructs an overlay network based on the Power law distribution of peer feedbacks. It dynamically selects small number of power nodes that are most reputable using a distributed ranking mechanism. A reputation system calculates the global reputation score of a peer by considering the feedback from all

other peers who have interacted with this peer. By using a random-walk strategy and utilizing power nodes, feedback aggregation speed, and global reputation accuracy are improved.
GossipTrust [6] defines a randomized gossiping protocol for efficient aggregation of trust values. A query is randomly forwarded to some neighbors instead of all neighbors. Comparing to flooding approach, gossiping reduces reputation query traffic.It uses the gossip protocol to aggregate reputation scores. It treats all opinions in gossip procedure with the same weight regardless of the sources of the opinions. A partially decentralized reputation-based TMS [8]for Bit- Torrent is presented which uses global trust scores to evaluate peers as well as their local trust scores. It uses the BitTorrent peers transactions for calculating local scores and the BitTorrent tracker to compute global trust scores.Peers calculate and assign local score to each other. Then peers send these local scores to the tracker. Tracker calculates global score of peers and find top 10 percent of peers. These 10 percent of peers determine global score of the other peers. Global scores return back to the peers.

A. Observation And Analysis

Table 1 compares the following reputation-based trust management systems in four technical aspects

III. Trust Management Scheme

In peer to peer systems, it is important to detect the malicious peers and harmful resources before a peer starts downloading. An efficient trust management scheme is developed and it maintains the overall credibility of the peer to peer network at an expected level.
In this trust management scheme, peers are assumed to be strangers to each other at the beginning. A peer becomes an acquaintance of another peer after providing a service, example, uploading a file. If a peer has no acquaintance, it chooses to trust strangers. An acquaintance is always preferred over a stranger if they are equally trustworthy. Using a service of a peer is an interaction, which is evaluated based on weight (importance) and recentness of the interaction, and satisfaction of the requester. An acquaintance's feedback about a peer, recommendation, is evaluated based on recommender's trustworthiness. It contains the recommender's own experience about the peer, information collected from the recommender's acquaintances, and the recommender's level of confidence in the recommendation. If the level of confidence is low, the recommendation has a low value in evaluation and affects less the trustworthiness of the recommender.

- If a peer pi downloads a file from an another peer p_j , it is an interaction for p_i and no information is stored on p_j . If pi had at least one interaction with p_j , p_j is an acquaintance of p_i. Otherwise, p_j is a stranger to p_i. Assume that p_i wants to get a particular service and p_j is a probable service provider. In order to maintain trust all over the network the peer p_i should communicate only with the peers having trust value greater than a certain threshold. Trust calculates here in two ways.
- If p_j is an acquaintance to p_i, then compare its service trust with the threshold value. If p_j is trustworthy enough, p_i gets the service from p_j and based on its own experience, service trust value of p_i about pj is updated. If p_j is a stranger, to learn p_j's reputation, pi requests recommendations from its acquaintances. Assume that p_k is an acquaintance of p_i and sends back a recommendation trust value to pi. After collecting all recommendations, p_i calculates reputation trust value and compare it with the threshold value. If p_j is trustworthy enough, p_i gets the service from p_j and based on the service, service trust value of pi about p_j and recommendation trust value of pi about pi are updated .

Table I : Performance Analysis

Trust Management System	P2P type	Local Trust Evaluation	Global Trust Evaluation	Data Management
DMRep	Structured	Binary Trust	Using complaints	PGrid
Eigen Trust	Structured	Sum of positive and negative ratings	Using pre-trusted peers	DHT (Distributed Hash Table)
Peer Trust	Structured	Normalized rating on each transaction	Calculates trust score using five factors	PGrid
Power Trust	Structured	Using Bayesian method	Using power nodes and LRW strategy	TON (Trust Overlay Network)
Gossip Trust	Structured and Unstructured	Using Bayesian method	Gossip based protocol	Bloom filter storage
TMS	Structured	Considers peer's co-operation with download and upload parameters	Using super peers	Bit-Torrent network
SORT	Structured and Unstructured	Considers both feedback and recommendations	-	Any

IV. Simulation Results

The trust model is developed using ns2 simulator by considering bittorrent protocol as a base protocol. There is a centralized tracker which controls the file transfer between the peers. Non trusted peers does not participate in the file transfer.The proposed method has been compared with existing method based on various parameters. Those parameters are packet delivery ratio and number of packet drops present at each node.

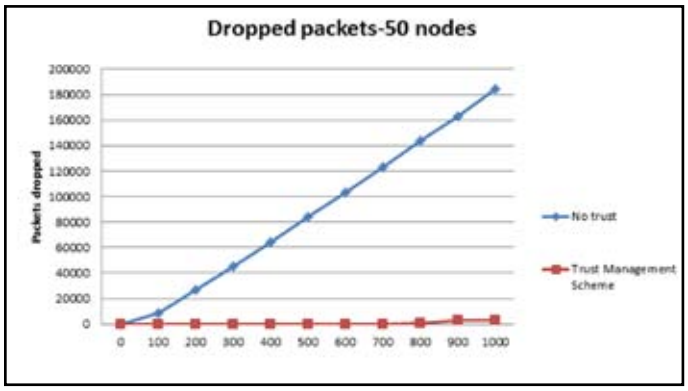

Fig. 1. Dropped packets

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

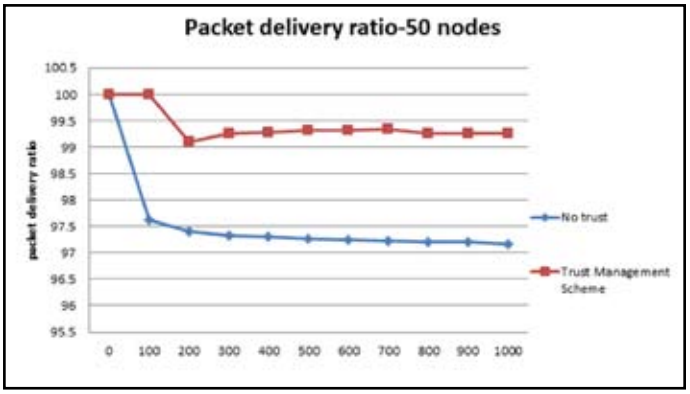

Fig. 2 : Packets delivery ratio

Graphical results show that comparing to the peer-to-peer networks with no trust, number of dropped packets during transmission are very less in new trust management scheme. The download rate of new trust management scheme mightbe slightly less than other methods. In most of the trust management systems, uploaders are selected based on their network bandwidth. An uploader with the higher bandwidth is always preferred. Here, selection is based on trustworthiness of uploaders. An acquaintance is always preferred over a stranger. Download rate might decrease due to this selection since an acquaintance with low bandwidth might be preferred over a stranger with high bandwidth.

V. Conclusion

Open nature of peer-to-peer systems exposes them to malicious activity. Building trust relationships among peers can mitigate attacks of malicious peers. Reputation-based trust management is used to pro- mote honest and cooperative behaviors, and thus the overall credibility of the P2P network can be main- tained at an expected level.Various methods for trust management in peer to peer systems have been compared. Each methods have its own merits and demer- its. A number of issues for future studies remain open. First, more extensive evaluation methods over wider parameters are needed. Second,lack of proper mechanism which consider the whole system state to balance loads. Thus, this issue needs more investigation in a future work.

References

[1] *K. Aberer and Z. Despotovic, "Managing Trust in a Peer-2-Peer Information System",Proc. 10th Intl Conf. Information and Knowledge Management (CIKM) 2002.*

[2] *S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The (Eigentrust) Algorithm for Reputation Management in P2P Networks",Proc. 12th World Wide Web Conf. (WWW) 2002.*

[3] *F. Cornelli, E. Damiani, S.C. Vimercati, S. Paraboschi, and P. Samarati,"A reputation-based approach for choosing reliable resources in peer-to-peer networks",In CCS02, Washington DC, USA 2002.*

[4] *L. Xiong and L. Liu, "Peertrust: Supporting Reputation-Based Trust for Peer-to-Peer Ecommerce Communities",IEEE Trans. Knowledge and Data Eng., vol. 16, no. 7, pp. 843-857 July 2004.*

[5] *R. Zhou and K. Hwang, "Powertrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing",IEEE Trans. Parallel and Distributed Systems, vol. 18, no. 4, pp. 460-473, Apr, 2007.*

[6] *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.*

[7] *Behrooz Shafiee Sarjaz Maghsoud Abbaspour, "BitTorrent using a new reputation-based trust management system",Springer Science+Business Media Sept. 2012.*

[8] *Ahmet Burak Can, Member, IEEE, and Bharat Bhargava, Fellow, IEEE, "SORT: A Self-ORganizing Trust Model for Peer-to-Peer Systems",IEEE Transactions on Dependable and Secure Computing, vol. 10, NO. 1, Feb. 2013.*

[9] *Ankur Gupta, "Peer-to-peer networks and computation: Current trends and future perspectives",Computing and Informatics, Vol. 30, 559594, 2011.*

[10] *Kevin Hoffman, David Zage, and Cristina Nita-Rotaru, "A Survey of Attack and Defense Techniques for Reputation Systems",Proc.16th Intl World Wide Web Conf. (WWW 07), 2009.*