DSORT-A Dynamic Self-ORganizing Trust Model for Peer to Peer Systems

Manju John(Author)
Computer Science and Engineering
MES College of Engineering
Kuttippuram

Dr.Govindaraj.E (Author)
Computer Science and Engineering
MES College of Engineering
Kuttippuram

***Abstract*—Peer to peer network (P2P) is a type of decentralized and distributed network architecture. Trust management in P2P networks encourages resource sharing among well-behaved peers and detect selfish or malicious peers to provide a more secure environment by reducing risk and uncertainty in the P2P interactions. In a distributed infrastructure without centralized server for authority, providing security mechanism is more complicated than in server-centric solutions. Therefore security issues are one of the major challenges that need to be carefully analyzed and addressed. A mechanism was developed here to decrease malicious activity in the peer to peer network system by establishing trust relations among peers in their proximity. Each peer develops its own local view of trust about the peers interacted in the past and share its acquaintance history with the peers in its peer list. Also a novel load-balancing method is proposed based on calculation of workload present at different service providers. Simulation results indicate that this model efficiently distribute workload among the service providing agents under stable condition.**

Keywords—peer-to-peer computing; reputation system; trust management; recommendation trust,security

I. INTRODUCTION

Peer-to-peer (P2P) systems are driving a major paradigmshift in the era of distributed computing.In a P2P infrastructure, the traditional distinction between clients and back-end (or middle tier application) serversis simply disappearing. Every node of the system acts therole of a client and a server. A P2P system can be characterized by a number of properties: no central coordination, nocentral database, no peer has a global view of the system, global behavior emerges from local interactions, peers areautonomous, and peers and connections are unreliable.

Trust management in P2P system is used to detect malicious behaviors 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.

Reputation-based trust management is one specific form of trustmanagement. Reputation-based trust management systems on the other hand provide amechanism, by which a peer requesting a resource may evaluate the trust in thereliability of the resource and the peer providing the resource.Sharing knowledge between peers is one ofthe ways to make at least some trust among peers.

We propose a Dynamic Self-ORganizing Trust model (DSORT) that aims to decrease malicious activity in a P2P system by establishing trust relations among peers in their proximity. 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 and share its acquaintance history with its own acquaintances. Also a novel load-balancing method is proposed based on calculation of workload present at different service providers. . In this way, good peers form dynamic trust groups in their proximity and can isolate malicious peers.

Outline of the paper is as follows: Section 2 discusses the related 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.

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 Despotovic’s trust model [1], peers report their complaints by using P-Grid. A peer is assumed as a trustworthy unless there are complaints about it. However, preexistence of trust among peers does notdistinguish 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 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 peer's 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 calculationadaptive on P-Grid. While transaction context parameteraddresses application dependent factors, communitycontext parameter addresses P2P community related issuessuch 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 utilizingpower nodes, feedback aggregation speed, and globalreputation accuracy are improved.

GossipTrust [6] defines a randomized gossiping protocolfor efficient aggregation of trust values. A query is randomlyforwarded to some neighbors instead of all neighbors.Comparing to flooding approach, gossiping reduces reputationquery 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 [7]for BitTorrent 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.

III. Dynamic Self organizing trust model for peer to peer networks

A peer may be a good service provider but a badrecommender or vice versa. Thus, SORT [8] considers providingservices and giving recommendations as different tasks and defines two contexts of trust: service and recommendationcontexts. Information about past interactions and recommendationsare stored in separate histories to assesscompetence and integrity of acquaintances in these contexts.SORT defines three trust metrics. Reputation metric iscalculated based on recommendations. It is importantwhen deciding about strangers and new acquaintances.Reputation loses its importance as experience with anacquaintance increases. Service trust and recommendationtrust are primary metrics to measure trustworthiness in theservice and recommendation contexts, respectively. Theservice trust metric is used when selecting serviceproviders. The recommendation trust metric is importantwhen requesting recommendations. When calculating thereputation metric, recommendations are evaluated basedon the recommendation trust metric.

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 was 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 abouta peer, recommendation, is evaluated based on recommender'strustworthiness. It contains the recommender's own experienceabout the peer, information collected from the recommender'sacquaintances, and the recommender's level of confidence inthe recommendation. If the level of confidence is low, therecommendation has a low value in evaluation and affects lessthe trustworthiness of the recommender.

If a peer p_i downloads a file from another peer p_j, it is aninteraction for p_i and no information is stored on p_j. If p_i hadat least one interaction with p_j, p_j is an acquaintance of p_iOtherwise; p_j is a stranger to p_i. Assume that pi wants to geta particular service and p_j is a probable service provider. Inorder to maintain trust all over the network the peer p_i shouldcommunicate only with the peers having trust value greaterthan 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 pi about p_j is updated.
- If p_j is a stranger, to learn p_j's reputation, p_i requests recommendations from its acquaintances. Assume that p_k is an acquaintance of p_i and sends back a recommendation trust value to p_i. After collecting all recommendations, p_i calculates reputation trust value and compares it with the threshold value. If p_j is trustworthy enough, pi gets the service from p_j and based on the service, service trust value of p_i about p_j and recommendation trust value of p_i about p_j are updated.

In proposed method,using SORT we firstcompute the trust of peers who respond to a transactionrequest and then we select the agent with the highest trustvalue. However, in this scenario, the agent with the highesttrust value will have immense workload while other capableagents with slightly lower reputation will have considerably less workload. The problem that will arise from this disproportionate allocation of workload is that the qualityof service will fall greatly due to the heavy workload presentat the highly trusted agents. So, a load-balancing algorithmis required for sustaining good service quality.

A. Load Balancing Algorithm

```
1. If peer j is a trusted one for peer i, check whether peer j's load is greater than certain threshold;
    A. If load is less than threshold,
        a. Assign peer j as an uploader;
        b. Increment its load by 1;
    B. Otherwise,
        a. Consider an another peer k, a trusted peer of i;
        b. Assign k as i and goto 1;
```

For selecting a best service provider, initially we select an uploader with highest trust value. Then check whether the load of that particular peer is greater than a certain threshold. If not, select that peer as a service provider and increments its load by one. Otherwise select another peer having next highest value of trust. Then repeat the loop until we select a service provider or no more service providers exist.

And also to maintain trust all over the network every node which moves to a new location or come across a new neighbor, or changes its vicinity is supposed to exchange the "acquaintance history" with other nodes.

IV. Implementation Results

Dynamic Self ORganizing Trust Model is developed using ns2 simulator by considering bittorrent protocol as a base protocol. Trust values are calculated based on the equations specified. 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 bandwidth utilization, packet delivery ratio, number of packet drops and load present at each node.

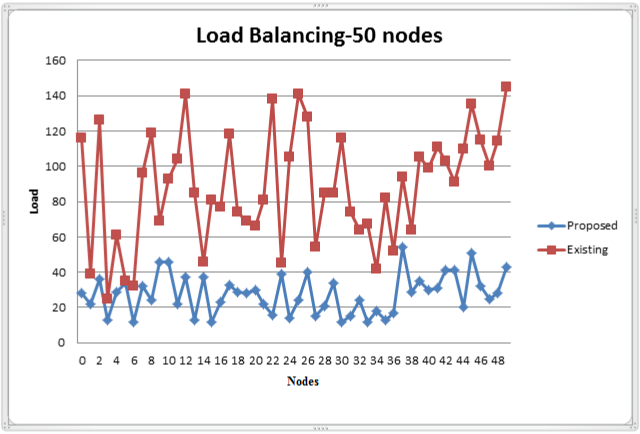

Fig. 1. Load balancing

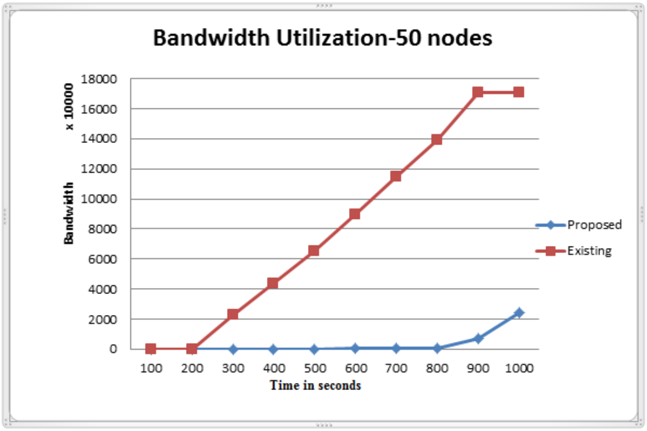

Fig. 2. Bandwidth Utilization

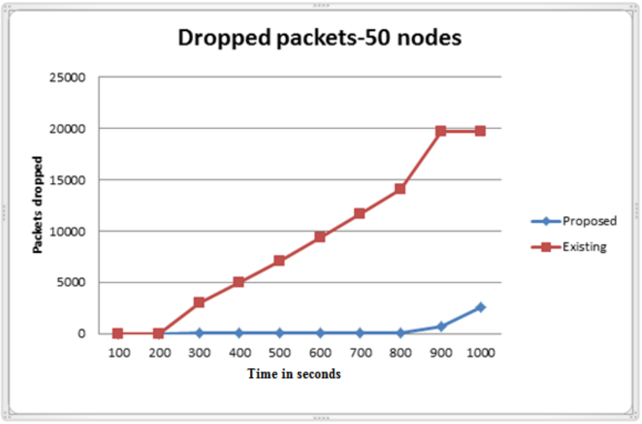

Fig. 3. Number of dropped packets

Graphical results show that comparing to the existing trust management systems,number of dropped packets during transmission are very less in D-SORT. Also it is seen that the load-balancing methodcan successfully distribute workload among the agents without compromising performance. The download rate with D-SORT might be slightly less than other methods. In most of the trust management systems, uploadersare selected based on their network bandwidth. An uploader with the higher bandwidth is always preferred. In D-SORT, 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.

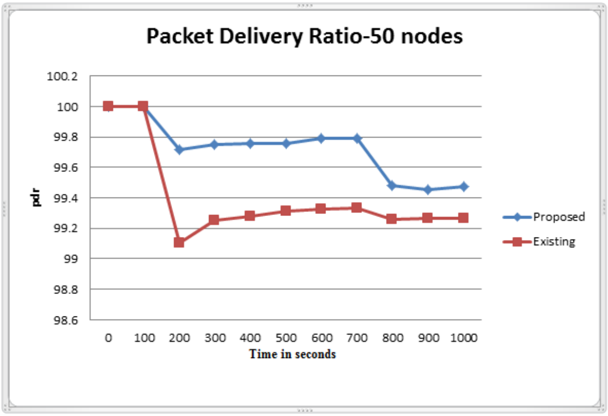

Fig. 4. Packet delivery ratio

V. CONCLUSION

Open nature of peer-to-peer systems exposes them to malicious activity. Reputation-based trust management is used topromote honest and cooperative behaviors, and thus the overall credibility of the P2Pnetwork can be maintained at an expected level.Various methods for trust management in peer to peer systems have been compared. Each methodhas its own merits and demerits.

In SORT, instead of considering global trust information, local trust information is enough to make decisions as peers develop their own trust networks.But one aspect which is slowly becoming critical for the proper maintenance of service quality is the appropriate distribution of workload among the trusted service providers. Thus a method, Dynamic-SORT is proposed which consider load balancing among service providers for distributing workload among service providers is proposed and to maintain trust throughout the network, every node exchange its acquaintance history with every other node.

Using trust information does not solve all securityproblems in P2P systems but can enhance security andeffectiveness of systems. Main overhead of the proposed method comesfrom the reputation queries. Before starting a download session,a peer sends reputation queries to learn about each uploader.

It gets back recommendations from its acquaintances.Since a peer obtains more acquaintanceswith time, the average number of recommendation requestsfor a query increases for a while. And also this method does not work in extra malicious environment. These issues might be studied as a future workto extend the trust model.

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 ntl World Wide Web Conf. (WWW 07), 2009.