AN OPPURTUNISTIC AND RELIABLE DATA ASSURANCE AMONG PEER-TO-PEER SYSTEMS

[1]Chejeti Rajitha, [2]Ch.Venkatrami Reddy

Dept of CSE, GITAM University, Hyderabad

Abstract-Peer-to-peer networks are mostly formed in random fashion without a good control on its topology. As the size of network grows, packets may have to travel through numerous links to reach far-end receivers. The longer the path, the higher the packet loss rate and longer transmission delay. This research is trying to find a better topology for multimedia data multicasting which makes the cumulated delay of the most-far-end user be tolerable and the packet loss be minimized. The problem is modeled as a MLDST problem, which is a NP-Complete problem. Unfortunately, P2P overlay networks are most formed freely without consideration of either balance of peer load or depth of the spanning tree. Furthermore, the popularity of error prone wireless links is increasing rapidly recently such that not only delay time, but also packet loss rate, must be taken into consideration. Whenever the size of the network grows enormously, number of long paths and overloaded peers, accompanying with long transmission delay and high packet loss rate, increases as well. We have also shown that error-correcting code and packet retransmission can help improve network stability by isolating packet losses and preventing transient congestion from resulting in PDM reconfigurations. Moreover, the overlay formation algorithm presented in this paper is oblivious to the physical network topology, and this may introduce considerable wide-area network traffic. It would be challenging to design an overlay formation algorithm aware of both the similarity of participating peers and the physical network topology.

Keywords:- *Anonymization, Communication Security, Trust, Response.*

I.INTRODUCTION

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. 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, e.g., making a small payment or signing a million-dollar purchase order. One challenge for a structured peer-to-peer storage system is to efficiently enforce stored contents availability in the face of node churn. One well known technique to address this issue is data replication. Number of existing structured storage systems enforce the leaf set (or successor) based replication approach. Recognizing the importance of trust in such communities, an immediate question to ask is how to build trust. There is an extensive amount of research focused on building trust for electronic markets through trusted third parties or intermediaries. However, it is not applicable to P2P e-commerce communities where peers are equal in their roles and are independent entities, thus no peers can serve as trusted third parties or intermediaries. The dynamic nature of peers poses challenges in the communication paradigm. The Overlay Nodes Management layer covers the management of peers, which include discovery of peers and routing algorithms for optimization. The Features Management layer deals with the security, reliability, fault resiliency, and aggregated resource availability aspects of maintaining the robustness of P2P systems. The

Services Specific layer supports the underlying P2P infrastructure and the application-specific components through scheduling of parallel and computation-intensive tasks, content and file management.

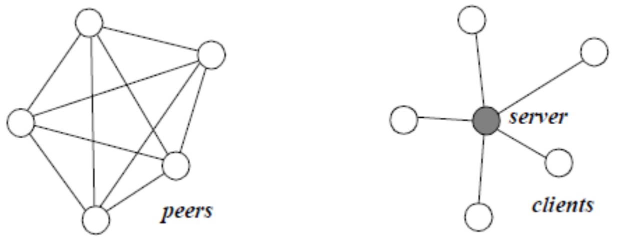

Figure.1. Simplified, High-Level View of Peer-to-Peer versus Centralized (Client-Server) Approach.

A peer gives some resources and obtains other resources in return. In the case

of Napster, it was about offering music to the rest of the community and getting other music in return. It could be donating resources for a good cause, such as searching for extraterrestrial life or combating cancer, where the benefit is obtaining the satisfaction of helping others. P2P is also a way of implementing systems based on the notion of increasing the decentralization of systems, applications, or simply algorithms. Conceptually, P2P computing is an alternative to the centralized and client-server models of computing, where there is typically a single or small cluster of servers and many clients (see Figure 1). In its purest form, the P2P model has no concept of server; rather all participants are peers.

Each peer maintains a small routing table consisting of its neighboring peers' Node IDs and IP addresses. Lookup queries or message routing are forwarded across overlay paths to peers in a progressive manner, with the Node IDs that are closer to the key in the identifier space. Although structured P2P networks can efficiently locate rare items since the key-based routing is scalable, they incur significantly higher overheads than unstructured P2P networks for popular content. Reputation systems provide a way for building trust through social control without trusted third parties. Most research on reputation-based trust utilizes information such as community-based feedbacks about past experiences of peers to help making recommendation and judgment on quality and reliability of the transactions. Community based feedbacks are often simple aggregations of positive and negative feedbacks that peers have received for the transactions they have performed and cannot accurately capture the trustworthiness of peers. In addition, peers can misbehave in a number of ways, such as providing false feedbacks on other peers. The challenge of building a trust mechanism is how to effectively cope with such malicious behavior of peers. Another challenge is that trust context varies from transactions to transactions and from communities to communities. In P2P systems peers form ratings of others that they interact with. To evaluate the trustworthiness of a given party, especially prior to any frequent direct interactions, the peers must rely on incorporating the knowledge of other peers— termed witnesses —who have interacted with the same party using reputation mechanisms. In our framework, each peer has a set of acquaintances, a subset of which are identified as its neighbors. The neighbors are the peers that the given peer would contact and the peers that it would refer others to. A peer maintains a model of each acquaintance. This model includes the acquaintance's reliability to provide high-quality services and credibility to provide trustworthy ratings to other peers.

The malicious peers could be independent: they give a bad rating of everyone else, or in a colluding group: they give good ratings of each other in the group and bad ratings of other peers. Here a bad rating could be an all-zero or a complementary rating. A good rating could be an all-one or an exaggerated positive rating. One example of a colluding group is that a single physical user generating multiple IDs

such as at least one of his IDs gets higher rating. In next section we show if reputation mechanisms can detect these two kinds of malicious peers or at least make the malicious attack costly.

II. BACKGROUND

A decentralized approach lends itself naturally to aggregation of resources. Each node in the P2P system brings with it certain resources such as compute power or storage space. Applications that benefit from huge amounts of these resources, such as compute-intensive simulations or distributed file systems, naturally lean toward a P2P structure to aggregate these resources to solve the larger problem. Distributed computing systems, such as SETI@Home, distributed.net, and Endeavours are obvious examples of this approach. By aggregating compute resources at thousands of nodes, they are able to perform computationally intensive functions. The incentive problem in P2P networks poses an obvious obstacle for P2P to be used as a distribution channel. Lacking incentives, free-riding will likely abound. There is recent growth of P2P literature from the computer science and economics perspective that address this problem. The most common solution is through a tit-for-tat protocol. While most of the research studying the free-riding problem in P2P networks focuses on direct and explicit incentives to encourage peers to share, analyze the possibility that users may share their content based entirely on self-interest. The intuition is that sharing will draw traffic away from other peers in the network to the sharing peer, thereby increasing the chance that the sharing peer will be able to get her desired content from other peers on the network. Thus, it is possible for a peer to increase her private utility through sharing. They propose to differentiate the quality of service provided to peers based on whether they share content. Significantly, they also find that it may not be socially optimal for all users to share their content, because the sharing cost is not justified by the potential benefit. In summary, in order to use P2P networks as a distribution channel, one should consider its similarity to public goods or club goods. However, the unique features of P2P networks also need to be taken into account. For example, the size of the endowment of resources in a P2P network varies based on how many peers contribute, which means that each peer who shares resources increases the size of the endowment to all other members. Peers have dual roles of being consumers of the P2P resources and providers as well. Over time, the same content can be distributed to many peers, which can potentially alter the quality and quantity of available resources and thereby the dynamics of user participation. A number of reputation systems and mechanisms are proposed for online environments and agent systems in general. Most of them assume the feedback is always given honestly and with no bias and paid little attention to handle the situation where peers may conspire to provide false ratings. A few proposals attempted to address the issue of quality of the feedbacks.

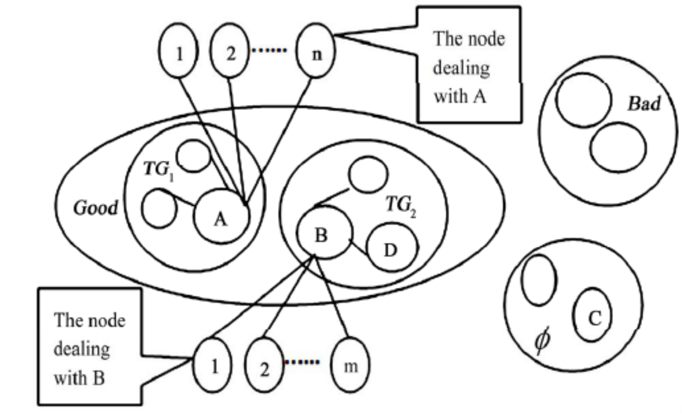

Figure.2. Network schematic of trust group-based

Nodes' departure has two ways: one is active departure, and the other is passive departure. Active departure can withdraw from the peer-to-peer actively when the node completes the transactions. If the node is also the administrator, before it leaves, it will choose the node with the highest credibility value in the group as administrator, and copy the information of the group to it. Passive departure happens when a node's credibility value is less than the credibility value of the group, and the administrator ejects it out of the trust group, and puts it into collection Bad. When a peer joins the system, the successor pointers of some peers need to be changed. It is important that the successor pointers are up to date at any time because the correctness of lookups is not guaranteed otherwise. The Chord protocol uses a stabilization protocol running periodically in the background to update the successor pointers and the entries in the finger table. The correctness of the Chord protocol relies on the fact that each peer is aware of its successors.

III. HYPOTHESIS

Delay is a significant factor in collaborative applications in a leased overlay network and is taken as a constrained metric of the presented algorithm. In addition, end-to-end delay is definitely used rather than average delay or total of the whole tree, because each user is mostly concerned to receive information from the source as soon as possible. Besides, inter destination delay variation is paid attention in this paper as well. It is an important factor in this situation. It is necessary that every participant to receive information from the source at the same time so that the fairness is guaranteed. There are several situations in which we need to limit the variation among the path delays by a certain given maximum bound. During a teleconference, it is important that a speaker is heard by all participants at the same time; otherwise, the communication may lack the feeling of an interactive face-to-face discussion. In the existing system of an authority, a central server is a preferred way to store and manage trust information, e.g., eBay. The central server securely stores trust information and defines trust metrics. Management of trust information is dependent to the structure of P2P network. In distributed hash table (DHT)- based approaches, each peer becomes a trust holder by storing feedbacks about other peers. Global trust information stored by trust holders can be accessed through DHT efficiently.

4.1.Basic Metric:

We first consider the basic form of the general metric by turning off the transaction context factor(T F (u,i)= 1) and the community context factor(α=1 and β=0)

$$T(u) = \frac{\sum_{i=1}^{I(u)} S(u,i) * Cr(p(u,i))}{2I(u)a}$$

This metric computes the trust value of a peer *u* by an average of the credible amount of satisfaction peer *u* receives for each transaction performed during the given period. The feedbacks in terms of amount of satisfaction are collected by a feedback system. Peer Trust model uses a transaction-based feedback system, where the feedback is bound to each transaction. The historical records of a peer's performance within a community can be an important factor for evaluation of trustworthiness of this peer in a consistent manner. When this is the case, the community context factor can be defined as the evaluation of the peer's historical behavior since the time when peer *u* enters the community. By assigning a proper weight, the past history of the peer can be taken into account but with a lower weight than the recent history. Let $I_h(u)$ denote the total number of transactions peer *u* has historically. If we only turn on the community context factor, and keep the transaction context factor off, we have the adaptive trust metric of the following form:

$$T(u) = \alpha * \frac{\sum_{i=1}^{I(u)} S(u,i) * Cr(p(u,i))}{2I(u)a} + \beta * \sum_{i=1}^{Ih(u)} S(u,i) * Cr(p(u,i))$$

Given an overlay network *G=(V,E)*, a source node s ε V, a multicast group $Z \leq V - s$, a link delay function *D*, a delay constraint (delay bound) Δ, a delay variation

tolerance δ, and an overall residual bandwidth-delay ratio *BD(T)*, the residual bandwidth, delay, and delay variation-bounded overlay routing problem can be

stated as follows: Find a multicast sub-network $T=(V_T ,E_T)$ $(T \leq G)$ rooted at *s* and spanning all nodes in *M*, such that for each node *j v* in *Z:*

$$Delay[s,v_j] = \sum_{e \in P(s,v_j)} D(e) \leq \Delta \, , \ \forall \ v_j \in Z$$

$$\left| \sum_{e \in P_T(s,v)} D(e) - \sum_{e \in P_T(s,u)} D(e) \right| \leq \delta \qquad \forall u,v \in Z$$

$$BD(T) = \sum_{e \in T} \frac{D(e)}{B(e)}$$ is minimized

All of the security, privacy, and trust issues discussed in the Structured P2P overlay network section applies to Unstructured P2P overlay networks. The ad-hoc nature of P2P systems also affects the way applications and systems are conceived. The fact that any system or user can disappear at time drives the design of these systems as well as user perceptions and expectations. In addition to the classical security issues of traditional distributed systems, P2P is distinguished by the importance of anonymity in certain applications and markets. Scalability, performance, fault resilience, and interoperability have similar importance for P2P as they have in traditional distributed systems.

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. We have also shown that error-correcting code and packet retransmission can help improve network stability by isolating packet losses and preventing transient congestion from resulting in PDM reconfigurations. Moreover, the overlay formation algorithm presented in this paper is oblivious to the physical network topology, and this may introduce considerable wide-area network traffic. It would be challenging to design an overlay formation algorithm aware of both the similarity of participating peers and the physical network topology.

IV. SIMULATION SETUP

We implemented the general simulation setup including the community model, the threat model, the transaction model, and a list of simulation parameters.

Threat Model

The threat comes from the untrustworthy peers when they act malicious. A peer fails to provide the requested service or information when acting malicious during a transaction. It further files a fake complaint against the other peer to hide its own malicious behavior. A peer also generates random trust data in response to queries for the data it is responsible for storage when acting malicious for the data storage function. The overall malicious behavior percentage in the community is captured by M= K* mrate.

Simulation Design

We set the total number of peers to 128(N=128). For the first experiment, we vary the malicious behavior factor in the community (M) by varying the percentage of untrustworthy peers with a fixed malicious rate of 1/4(mrate=1/4). The transaction skew factor is set to 0(Sk=0). For the second experiment, we vary the transaction skew factor. The percentage of untrustworthy peers is set to 1/2 (K=1/2) and malicious rate of untrustworthy peers is set to 1/4(mrate=1/4).

Figure 3 represents the trust evaluation accuracy of the two models with respect to the malicious behavior factor in the community. We can make a number of interesting observations. First, Peer Trust and the complaint-only approach perform almost equally well when the malicious behavior factor is low. This is because the complaint-only approach relies on there being a large number of trustworthy peers who offer honest statements to override the effect of the false statement provided by the untrustworthy peers and thus achieves a high accuracy. Second, as the malicious behavior factor increases, Peer Trust stays effective while the performance of the complaint-only approach deteriorates. This can be explained as follows. On the contrary, Peer Trust uses the credibility factor to offset the risk of fake complaints and thus is less sensitive to the misbehaviors of untrustworthy peers.

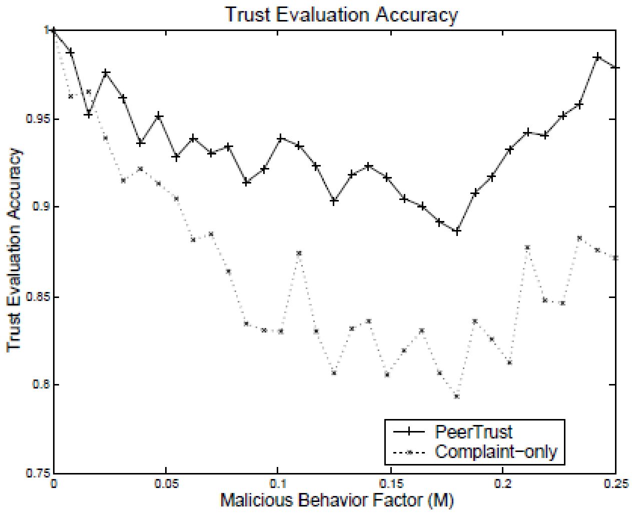

Figure 3. Trust Evaluation Accuracy with Malicious Behavior

V. CONCLUSION

Unfortunately, P2P overlay networks are most formed freely without consideration of either balance of peer load or depth of the spanning tree. Furthermore, the popularity of error prone wireless links is increasing rapidly recently such that not only delay time, but also packet loss rate, must be taken into consideration. Whenever the size of the network grows enormously, number of long paths and overloaded peers, accompanying with long transmission delay and high packet loss rate, increases as well. We have also shown that error-correcting code and packet retransmission can help improve network stability by isolating packet losses and preventing transient congestion from resulting in PDM reconfigurations. Moreover, the overlay formation algorithm presented in this paper is oblivious to the physical network topology, and this may introduce considerable wide-area network traffic.Besides the research directions mentioned in the above paragraphs, this dissertation can also be expanded into addressing other core competencies for P2P applications such as collaboration enforcement. The level of peer collaboration has a direct consequence on the scalability of a P2P application; hence, effective collaboration enforcement is one important factor deciding the success or failure of a P2P application. We are also interested in combining trust management with intrusion detection to address concerns of sudden and malicious attacks.

REFERENCES

[1] L. Mekouar, Y. Iraqi, and R. Boutaba, *Handbook of Peer-to-Peer Networking*, chapter Reputation Management in Peer-to-Peer Systems: Taxonomy and Anatomy, Springer, 2009. 1

[2] P. Garbacki, “Applying the Super-Peer Concept to Existing Peer-to-Peer Networks,” Tech. Rep. PDS-2003-010, Delft University of Technology, Netherlands, 2003. 1

[3] L. Mekouar, Y. Iraqi, and R. Boutaba, “Peer-to-Peer Most Wanted: Malicious Peers,” *Computer Networks Journal, Special Issue on Management in Peer-to-Peer Systems: Trust, Reputation and Security*, vol. 50, no. 4, pp. 545–562, 2006. 2, 3

[4] L. Mekouar, Y. Iraqi, and R. Boutaba, “A Contribution-Based Service Differentiation Scheme for Peer-to-Peer Systems,” *International Journal on Peer-to-Peer Networking and Applications*, vol. 2, no. 2, pp. 146–163, 2009. 3

[5] L. Mekouar, Y. Iraqi, and R. Boutaba, “Impact of Peers’ Similarity on Recommendations in P2P Systems,” in *IEEE International Conference on Computer and Information Technology*, 2010.

[6] K. Aberer and Z. Despotovic. Managing trust in a peer-to-peer information system. In 2001 ACM CIKM International Conference on Information and Knowledge Management, 2001.

[7] E. Adar and B. A. Hubeman. Free riding on gnutella. First Monday, 5(10), 2000.

[8] Y. Atif. Building trust in e-commerce. IEEE Internet Computing, 6(1), 2002.

[9] S. Ba and P. A. Pavlou. Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior. MIS Quarterly, 26(3), 2002.

[10] M. Chen and J. P. Singh. Computing and using reputations for internet ratings. In 3rd ACM Conference on Electronic Commerce, 2001.

[11] F. Cornelli, E. Damiani, S. D. C. di Vimercati, S. Paraboschi, and P. Samarati. Choosing reputable servents in a P2P network. In Eleventh International World Wide Web Conference, 2002.

[12] C. Dellarocas. Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior. In 2nd ACM Conference on Electronic Commerce, 2000.

AUTHOR"S PROFILE:

1. C.Rajitha Persuing her M-tech in GITAm University, Hyderabad Her Research area includes Data Mining and Networking

2. Ch. Venkat Rami Reddy had received his Master of technology (computer science and engineering) from NIT,Calicut. Currently working at GITAM University, Hyderabad, A.P, as an Assistant Professor in department of CSE.