Differential Gossip Algorithm in Peer-to-Peer Networks using Rank Aggregation

Gunda Srilakshmi¹, B.Mallikarjuna Rao²
¹M.Tech Scholar, Department of Computer Science and Engineering, Malineni Lakshmaiah Women’s Engineering College, Guntur, Andhra Pradesh, India.
²Associate Professor, Department of Computer Science and Engineering, Malineni Lakshmaiah Women’s Engineering College, Guntur, Andhra Pradesh, India.

Abstract— Reputation Aggregation in distributed systems is by and large an extremely time and asset expending process. Also, the vast majority of the techniques think about that as a hub will have same reputation with every one of the hubs in the system, which is not valid. This paper proposes a reputation aggregation algorithm that uses a variation of prattle calculation called differential Gossip. In this paper, gauge of reputation is thought to have two sections, one regular part which is same with each hub, and the other one is data gotten from prompt neighbors in view of the neighbors’ immediate communication with the hub. The differential Gossip is quick and requires less measure of assets. This instrument permits calculation of autonomous reputation esteem by a hub, of each other hub in the system, for every hub. The differential babble trust has been researched for a power law arrange shaped utilizing special connection (PA) Model. The reputation processed utilizing differential Gossip trust demonstrates great measure of resistance to the intrigue. We have checked the execution of the calculation on the power law systems of various sizes running from 1000 hubs to 1,000,000 hubs.

Introduction:

Shared frameworks have pulled in noteworthy thought in later past as these systems are more versatile than the client server systems. In any case, free riding has ascended as a noteworthy test for conveyed systems. Penchant of centers to draw resources from the compose and not giving anything thusly is named as Free Riding. As centers have conflicting interests thusly, intolerant direct of center points prompts issue of free riding. This lead of center points can be illuminated by surely understood prisoners' issue. In a record sharing framework, if center points are considered as players, their NE will be the framework where none of them will share the benefits. Trial looks at on Gnutella framework attested this. Trust or reputation organization structures can be used in shared frameworks to beat the issue of free riding furthermore to stay away from a bit of the ambushes. Such reputation organization structures have been in e-business passageways like e-inlet, yet they have the favorable position that they rely on upon client server building. In disseminated record sharing frameworks, as there is no central server or store, trust must be assessed and set away by each center point in an appropriated outline, and all such trust qualities ought to be gathered to produce an effective reputation organization system.

Reputation and Trust frameworks utilize trust and reputation ideas for confronting and overseeing malevolent practices. Despite the fact that there are numerous definitions for trust idea, taking after is an all around characterized clarification of it: "Trust mirrors the conviction or confidence or desires on the trustworthiness, respectability, capacity, accessibility and nature of administration of focus on hub's future movement or behaviour"[1]. At the end of the day, trust alludes to the conclusion of every companion about the conduct of the others as indicated by its past encounters. This supposition more often than not is pronounced with a numerical esteem. Reputation frameworks help associates to pick dependable hotspots for exchanges by collecting distinctive trust values and positioning companions in light of their worldwide notorieties. Notoriety total strategies as a piece of notoriety frameworks have been created for social affair data about past exchanges and practices of the companions.

The main problems in P2P systems are how to gather, spread and control information which is needed for computing reputation at each node. In these networks, a desired reputation system should have minimum overhead in infrastructure, computation, storage and number of messages [2, 3]. Fault tolerance, scalability and accuracy in determining malicious peers are the other features which an acceptable reputation system should have. Gossip algorithm is a suitable method for quick and correct reputation aggregation in P2P systems [4,5].Gossip based data aggregation is inspired by...
gossip dissemination in social relations. In this method, in each step or time period, each node communicates and exchanges information with one or more nodes that are randomly chosen which leads to approximate distribution of information to all nodes [6, 7]. Gossip algorithm is simple and has remarkable features including robustness, fault tolerance and scalability [7]. However, it imposes pretty much overhead in the networks with the large number of peers. GossipTrust [3] is a noteworthy method which uses Gossip algorithm. In this method, peers share their local trust values with their random neighbors so that the values converge to global reputation for every peer. Despite GossipTrust contribution in increasing the scalability, by increasing in the number of peers, not only computation time of the reputation aggregation increases, but also accuracy and convergence of the reputation values confront some obstacles [8]. GossipTrust uses the Kempe et. al’s algorithm [7] for gossiping. The Kempe algorithm has been proven to be correct when network is strongly connected [6]. This is while P2P networks are not strongly connected and it is known that structure of P2P networks shows power-law properties [9, 10]. This inconsistency reduces the accuracy of GossipTrust and increases the convergence time of the reputation data.

In P2P networks, dynamic nature and large number of nodes lead to some issues for completely distributed algorithms. Management, aggregating and computation of the reputation information are some of these issues. GossipTrust has been designed for completely distributed networks. But, in this method, by growing the number of nodes, high overhead causes reduction in the number of transactions and participation of the nodes. One possible solution to get out from completely distributed systems is to consider different levels for nodes based on their capabilities and to use a semi-central reputation system. In semi-central systems, disadvantages of both distributed and central systems decrease and advantages of both systems can be used.

**Related Work**

Reputation systems provide a method for predicting the quality and reliability of transactions in the future. The main problem in reputation management is how to deal with malicious behaviors. The most general way is to use the peers' recommendation about the providers. Peers rate those who have previously communicated with them. Peers, who are requesting a service, establish trust through analyzing different trust values which others have been given to the providers [1]. P2P reputation management systems should be distributed, efficient, scalable, reliable, and secure in computation, storage and spreading the trust values. There are some useful surveys about the category of reputation, trust systems and security threats followed by their comparison [1, 2, 18, 19]. The work in [19] is a survey which introduces a remarkable taxonomy for reputation systems, along with a reference model for reputation systems as well as the comparison of existing reputation researches and the deployed reputation systems. As one of the recent works on reputation systems, Secure and Effective distributed P2P Reputation System proposed by Srikanth and Madhuri in [20] can be mentioned. In this model, Self-certification, an identity management mechanism, and a cryptographic protocol to exchanges trust between the peers are used. This method facilitates generation of secure reputation data in a P2P network, in order to expedite detection of rogues.

The core of the proposed algorithm in this paper is the gossip algorithm. The most important and related gossip based algorithms are following. Kempe et al. [7] proposed some gossip based algorithms for data aggregation. Jelasity et al. [6] also proposed the push-pull gossip algorithm. n not strongly connected networks, the Jelasity algorithm works better than the Kempe algorithm for data aggregation. Gossip algorithms are also used by Bachracht et al. [4] for reputation aggregation. DifferentialGossipTrust [5] is a gossip based algorithm or aggregating reputation specifically in peer networks. Instead of simple push gossip algorithm such as Kempe, it suggests a differential push gossip algorithm. Nodes uses different number of pushing based on the degrees of themselves and their neighbors. The authors in [3] proposed the GossipTrust algorithm which is used as the basic method for reputation aggregation in the proposed model in this paper. We will review this algorithm in detail in the next section.

To increase efficiency of communications, social communication models and virtual social networks are increased recently, P2P networks are not exception to this rule. For solving some problems of P2P systems, social based or Group based solutions are suggested. The proposed GGRA algorithm also uses grouping concept to reach its mentioned goals. Previously some group based models are suggested. One of the proposed models is grouping based on peers' interests [12, 13, 17, 21]. Using this kind of grouping, requests for resources (services) are most related to their own groups. Therefore, searching related groups for finding owners of target resources is usually enough. This way, searching for resources can be done more quickly, so most of the useless searching time and traffic can be saved. Other researches based on groups are done with the aim...
of setting secure policies and increasing security in networks [16, 22, 23]. Since grouped P2P networks are more practical and peers usually trust to their groups, reputation systems have been created based on groups. Further, existence of different P2P groups requires reputation system which is able to obtain reputation of peers based on features of groups. Authors in [16] have proposed a trust and reputation model based on peer group as GroupTrust. In this model, reputation is computed based on the similarities of services’ contexts and the similarity of groups. Also, the trust values of those who have communicated with a peer and are in the same group are considered. GroupRep [22] is another group based reputation system for P2P networks which proposed a filtering cluster algorithm to filter unfair rating provided by malicious nodes. GTrust [17] provides better trust using group membership and trust propagation between unknown persons. The other model proposes a solution for access control [14]. In this model, selection of service provider and also response to requests are based on reputation of peers’ groups. GARM [15] model divides peers which have the same resources in the same groups. In GARM, each Pre-trusted node in each group chooses the provider. Pre-trusted node also makes an anonymous path from provider to requester for sending the service. In this model peers compete for increasing their own reputation. In EigenGroupTrust [23], each group has a leader who is a pre-trusted node. Each peer uses credential and trust delegation to ensure reliability of resources. In this algorithm at first EigenTrust [24] algorithm is executed in each group and then EigenTrust is performed between leaders. Note that EigenGroupTrust has not considered gossip as a method for aggregating in distributed P2P networks. ILGT [25] and GRAT [8] are partly similar models which both use GossipTrust and try to use group formation to improve GossipTrust scalability.

ILGT and GRAT are the most related works to our GGRA algorithm but the concept of group in these two works are different from GGRA and they have some deficiencies. In ILGT, peers can easily manipulate their own list and collusive groups can easily be formed. Also, while for getting accurate reputation based on GossipTrust, reputation of all peers are needed to be calculated simultaneously, in ILGT only reputation of the provider peers are computed in each group. In general, the assumptions of ILGT and GRAT affect accurate execution of GossipTrust and these assumptions are not justifiable.

Proposed Algorithms

GossipTrust Algorithm

In this Section GossipTrust algorithm [3] is described in detail. The algorithm works as follows:

In a P2P network with n nodes, after each transaction between two nodes, the transaction receiver expresses its trust to the sender by a number. Gossip steps as shown in Figure 1 are repeated until all the nodes converge to the reputation value of nodes. Convergence testing is done

Basic Assumptions

In the proposed algorithm, it is assumed that there exist some distinct established groups in the network.

Each peer is member of only one group and each group has a representative member. Peers communicate and exchange services (information or resources) with the other peers in their groups or out of their groups as shown in Figure 3. In this Figure, R1, R2, and Ri are representatives of groups G1, G2, and Gi, respectively.

After receiving a service, each peer expresses the value of its trust to the sender with a number based on the quality of the received service. The goal of GGRA algorithm is to achieve reputation of all peers based on the trust values in a distributed, accurate and scalable manner.

The algorithm works based on the following assumptions:

(1) Groups in P2P network are established before the aggregation starts. Groups may be formed based on different criteria such as friendship, interest to different subjects or any other similarity measure.

(2) For each group there is a representative (albeit the algorithm can be extended to deal with more than one representative). This peer can be selected from the most reputed or pre-trusted peers. Usually designers and those who are initially connected to P2P networks are not willing to be malicious [24, 26].
(3) Before the reputation aggregation start, each peer knows its group, its group representative, and all the members of the existing groups.

In addition to the mentioned assumption of the GGRA algorithm, the following points should be considered too:

(1) **Joining to the network**: In P2P networks, each node for joining to the network needs to know the addresses of peers who are previously connected to the network. In the proposed algorithm, peers can refer to the bootstrapping site for getting information of groups. This information consists of address of the representative peer and other peers of its own group.

(2) **Grouping Methods**: There are different ways for grouping peers. One way is clustering through the peers' similarity like the interests of them. In this kind of grouping, the group in which peer has the most activity in it, can be chosen as its group. The other way is to use an algorithm which increases efficiency such as creating groups with equal members. However, the best way is to divide peers according to their connectivity graph. This graph is different from the graph which is established for joining, connecting to the network and searching for resources. In this method, Pre-trusted nodes or bootstrapping servers use the history of peers that are involved in transactions in order to group according to the connectivity graph. For example, social connectivity network can be used as an infrastructure (Connectivity graph). In these networks, Community detection algorithms [27] can be used to divide peers according to the social friendship graph.

(3) **Network type**: In GGRA, gossiping and grouping are used for computing the reputation. Gossip based algorithms are distributed algorithms and representatives of groups in GGRA work as semi-central agents. Although GGRA algorithm takes advantage of a semi-central management scheme, it can be used in distributed, central and semi-central P2P networks too. In the semi-central networks such as the second generation of P2P networks [11], each server can be considered as representative of each group. In the centralized networks, grouping can be done using the central server, and in distributed networks grouping can be done using the bootstrapping server.

**Algorithm 1 - GGRA Algorithm**

1: Do GossipTrust algorithm in groups to get each members' reputation
   - First phase: Do reputation aggregation in each group
2: Do algorithm 2 to get the reputation of groups
   - Do the Gossip averaging algorithm
3: Do GossipTrust algorithm between groups' representatives to get reputation of each group
   - Second phase: Do reputation aggregation between groups
4: Broadcast reputation of all groups and their members by gossiping in each group
   - Third phase: Broadcast reputation by aggregation in each group

**Convergence Speed**

In this simulation, convergence speed of GossipTrust and GGRA algorithms with different number of nodes have been compared. Number of steps needed for execution of GGRA algorithm (T_{GGRA}) is the sum of intra group, inter group and broadcast steps as shown. T_{intra} is the maximum execution time (number of steps) between all groups in the first phase, T_{inter} is the execution time (number of steps) between representatives in the second phase and T_{broadcast} is the maximum execution time (number of steps) between all groups in the third phase. To compare the execution time between GGRA and GossipTrust algorithm, at first GossipTrust is performed in the formed network without considering groups. In GossipTrust simulation, communication of each peer is only with its friends i.e. each peer sends gossip information only to its friends. The other setting of simulation is described. As the results of evaluation in confirms, there is remarkable decrement in execution time of GGRA in comparison with GossipTrust. Indeed, due to partitioning peers into different groups, number of participating nodes in GGRA Algorithm decreases. It is clear that with reduction in number of nodes, the convergence speed increases too.

**Conclusion**

Malicious behaviours are a standout amongst the most difficult issues in P2P systems. Notoriety framework is known as a worthy answer for the specified issue. As per the specific usefulness of the notoriety framework in this environment, a
wanted calculation ought to have versatility and precision elements to advance this kind of systems.

In this research, a productive calculation, GGRA, for reputation collection in P2P systems is proposed. In GGRA, GossipTrust is executed at the same time in all gatherings and in a firmly associated chart rather than power-law diagram. In this way, diminishment in time, number of messages and storage room are accomplished as focal points.

As per the assessment comes about, the proposed GGRA calculation is helpful in gatherings which a large portion of correspondences are with intra assemble peers. This property is found in social based gatherings which itself assists P2P frameworks with being survival. This is on the grounds that the associates partake more in these frameworks, they attempt to safeguard from their gatherings and deny demonstrating noxious activities. Utilizing social gatherings dispenses with the requirement for knowing notoriety of all associates. In this way, loads of movement and time can be spared. These favorable circumstances make utilizing informal organizations as a framework for P2P systems to be conceivable and more effective. Moreover, utilizing semi-focal delegates as a part of the proposed demonstrative decreases calculations and increment productivity however much as could be expected.

References


