International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 2 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT1952156

Global Trust : Trust Based Peer-to-Peer Networks using Chat Application

Ramya Chowdary Patchala*, Srujana Nayudu, Sony Pillutla, Madhubabu Janjanam
Department of Computer Science & Engineering, JNTU Kakinada, Guntur, Andhra Pradesh, India

ABSTRACT

In the P2P Networks, the guarantee-based trust model, GeTrust is developed by the establishment of trust relationship in human society and aiming at solving the problems of high computational complexity and in accurate evaluations existed in the recommendation-based trust models. In the establishment of the guarantee relationship between the service peer and its guarantee peer(s) on the basis of their mutual evaluations, and then the establishment of a service relationship between the request peer and the service peer based on their mutual evaluations and the guarantee relationship owned by the service peer. The P2P networks mainly focuses on the characteristics like decentralization, autonomy and anonymity. The trust between the peers is established by the concept of reputation and guarantee. A service peer needs to choose its guarantee peer(s) for the service it is going to provide, and they are both required to pledge reputation mortgages for the service. The request peer makes evaluations on all the candidates of service peer by referring their service reputations and their guarantee peers' reputations, and selects the one with highest evaluation to be its service provider. The availability and prevention of malicious behavior, incentive mechanism and anonymous reputation management strategy is proposed. This is an effective and efficient way of improving security and reducing network overhead. Here we also use concept of mortgage of reputation in order to reduce the slander among the peers and provide them best services.The objective is the development of the chat application in the P2P networks in the basis of a trust model when establishing the trust relationships between the peers by the using the concept of Guarantee-based trust model(GeTrust).

Keywords : P2P Networks, GeTrust, Trust Model, Service peer, Guarantee peer, Request peer, Reputation, Reputation Mortgage.

I. INTRODUCTION

Along with the advancing Internet technology and the continuous growth of network applications, P2P networks, characterized by decentralization, autonomy and anonymity, have been applied to many areas such as file sharing and instant messaging. Existing P2P networks which have been widely used include BitTorrent, Gnutella, eDonkey, and so on. Nevertheless, the malicious behavior like cheating and forging negatively impacts the networks' availability and users' experience. Thus, a trusty and safe evaluation model is needed to supervise and constrain the peers' behavior in P2P networks. Several kinds of trust models have been proposed, in which the recommendation-based trust models are the most commonly used ones, which calculate the target peer's reputation by using the globally collected recommendations. Recommendation-based approach could have a good grasp of the target peer's behavioral attributes. Existing recommendation based trust models suffer from the shortcomings of slow convergence and high complexity of trust computations, as well as huge overhead of network

CSEIT1952156 | Received : 11 March 2019 | Accepted : 27 March 2019 | March-April -2019 [5 (2) : 771-776]

traffic. They also overlook the difference between the peer's recommendation credibility and the peer's global trust, or lack the effective punishment to resist collusion attacks, leading to an inaccurate evaluation on the peer. In human society, a service provider who wants to be trusted by the counterparty could apply for guarantee. Since the service provider and its guarantee(s) both run the risk of damaging their reputations, they need to cooperate smoothly to provide authentic services. Inspired by the establishment of trust relationships in human society, a guarantee-based trust model, this application is proposed.

II. METHODS AND MATERIAL

This section describes the details of our proposed scheme. The process of text recognition is divided into three major parts: (A) Evaluation of Guarantee peer (B) Reputation Mortgage (C) Establishment of Guarantee relationship (D) Incentive Mechanism.

*(*A) Evaluation of Guarantee Peer :

Each service peer must have its own guarantee peer(s) if it wants to provide a service. Applying for a good guarantee peer is critical for a service peer since it could improve the service peer's reputation and thus make the service peer benefit a lot. Each peer keeps two guarantee peer lists, the current guarantee list (CGL) and the backup guarantee list (BGL). CGL stores the information of the peer's current guarantee peers, while BGL holds its backup guarantee peers' information. For the convenience of searching for guarantee peers and also considering the fact that this application is designed for Chord-based P2P networks, we use a converting function to map each guarantee node's IP address into an integer which is in [1, *L*]. Then, we add the mapped integer, e.g. r ($1 \le r \le L$) , to a prefix *GID* for getting a hash value by using the Secure Hash Algorithm, i.e. *InodeID*=Hash(*GID*+*r*). *GID* is a numerical prefix which is used to help peers locate the index peers of guarantee peers, and each peer is told the *GID* when it is joining the network. We take *InodeID* as the *nodeID* of the node which stores the index information of the guarantee nodes. In this way, each guarantee node could have its index information stored on a certain node in the network. Also, each service peer could look for the guarantee peers by consulting the index nodes determined by Hash(*GID*+*r*) ($1 \le r \le L$). Besides, we allow a guarantee peer to send self-nomination to peers in its Finger Table declaring that it could guarantee for their services voluntarily without the evaluation on the service peers. We call such guarantee peer the self-recommender. Upon receiving a self-nomination, the peer could add the self-recommender into its BGL. If the service peer wants to employ self-recommender as its guarantee peer, it only needs to send a guarantee application to the self-recommender and the self-recommender's archive peer to notify them of the direct establishment of the guarantee relationship without any evaluations. This mechanism is helpful for those peers, especially the just joined-in peers, whose reputations are lower to increase their guarantee reputations. However, self-recommenders also run the risk of damaging their reputations due to the blindness of selecting their guaranteed peers.

Before providing a service, the service peer, say *b*, first needs to find its guarantee peers in its BGL. Each guarantee peer that peer *b* has found needs to be evaluated by peer *b*'s archive peer to make sure that the guarantee peer is qualified to guarantee even all its reputation mortgages being pledged for other services are deducted. To this end, we use the concept of remaining guarantee reputation to represent the available guarantee reputation for a new guarantee relationship, which is calculated by (3).

$$\mathbf{R}_{\mathrm{g}}=\mathbf{R}_{\mathrm{g}}{}^{\mathrm{pre}} - \sum_{i=1}^{m} \quad RM^{\mathrm{i}}{}_{\mathrm{g}} \qquad \mathbf{(3)}$$

where R_g^{pre} is the guarantee peer's present guarantee reputation. RM_g^i is the guarantee peer's reputation mortgage being pledged for its ith service. Both R_g^{pre} and RM_g^i are obtained from guarantee peer g's archive peer. m is the number of services being guaranteed by the guarantee peer. Only when the remaining guarantee reputation R_g is not less than zero, could the guarantee peer g be considered to be qualified to guarantee.

(B) Reputation Mortgage :

Guarantee peer(s) have to pledge their reputations, i.e. the reputation mortgages, for the service provided and guaranteed by them. Their reputation mortgages are calculated by (8) and (9), respectively.

$$\mathbf{RM_b = e^{-1/(\lambda * \nu)} * R_b} \qquad (2)$$

$$\mathbf{RMg_i \; = (Rg_i / \textstyle\sum_{j=1}^{v} \; Rg_i) * RM_b} \qquad (3)$$

where v is the number of guarantee peers that the service peer has and is the transaction volume. $\mathbf{Rg_i}$ is the remaining guarantee reputation of the service peer's i_{th} guarantee peer. The reputation mortgages are recorded

from the time at which the guarantee relationship is established and would be deducted from relevant peers' reputations (service peer's service reputation and guarantee peer's guarantee reputation) when the service peer or the guarantee peer breaks off the guarantee relationship (such as giving up voluntarily or dropping out accidentally) or the service peer provides a malicious service.

(C) Process of establishing a guarantee relationship:

Based on the evaluations on guarantee peer and service peer, this section details the process of establishing a guarantee relationship, through which we clarify how many and what kinds of messages would be exchanged. In the process of establishing a guarantee relationship, three kinds of messages, i.e. *Notify*, *Query* and *Reply*, are used. Note that all the messages used to communicate with archive peers are routed with the anonymous approach.

Step 1. Assume peer *b* wants to provide a service, it first needs to look for its guarantee peer(s) in its BGL or by using the index peers if it fails to find enough guarantee peers in its BGL. Here, we suppose peer *g* is one of the selected candidates. Then, peer *b* notifies its archive peer D_b by sending $Notify(b,D_b)=CGN|HID_b|ID_g$.

Step 2. After receiving the notification from peer *b*, D_b requests peer *g*'s guarantee reputation and reputation mortgages being pledged for other services from *g*'s archive peer D_g by sending $Query(D_b,D_g)=HID_g|RM$, and then waits for D_g's reply message of $Reply(D_g,D_b)=HID_g|GR|\{RM_1,RM_2,...,RM_i\}$.

Step 3. Upon receiving the reply message, D_b verifies whether peer *g* is qualified to guarantee according to Formula (3). If so, D_b sends out a guarantee application with the form of $Notify(D_b,\{g,D_g\})=GA|HID_b$ to peer *g* and its archive peer D_g.

Step 4. After receiving the guarantee application, D_g sends the request of

$Query(D_g \;,D_b)=HID_b|SET$ to peer D_b for peer *b*'s service reputation as well as *b*'s historical feedback peer set, and then waits for the reply of $Reply(D_b,D_g)=HID_b|SR|\{ID_1,ID_2,...,ID_n\}$ from D_b.

Step 5. If peer D_g has confirmed that peer *b* is qualified to get guaranteed, then it would send $Notify(D_g,\{D_{b,g,b}\})=GRE|HID_b|HID_g$ to notify peers D_b ,*b* and *g* that the guarantee relationship has been established

(D) Incentive mechanism :

To strongly encourage peers to provide authentic services and guarantees, as well as to stimulate the service peer and its guarantee peer(s) to smoothly cooperate in providing the services, apart from using reputation mortgages, we propose an incentive mechanism as well. When a peer provides more services and guarantees authentically and successfully to achieve a high reputation could it get better services and guarantees. This gives us a hint to design the incentive mechanism. In this application, we reward the service peer and its guarantee peer(s) for their smooth cooperation after their guarantee relationship ends. The rewards are calculated and also they are added to the reputations (the service peer's service reputation and its guarantee peers' guarantee reputations) by the peers' archive peers, respectively.

$$\mathbf{Reward(b)=f_{succ} * RM_b}$$
$$\mathbf{Reward(g_i)=f_{succ} * RM_g}$$

where Reward(b) and Reward(g_i) are the rewards for the service peer b and its ith guarantee peer, respectively.

f_{succ}= F_{succ} / F_{all} is the successful transaction rate of the service peer (guarantee peer) during the last time window T. F_{all} is the total number of feedbacks on the service and F succ is the number of satisfied feedbacks. This application applies this incentive mechanism to encourage the service peer (the guarantee peer) to choose the guarantee peer (the service peer) with high reputation to cooperate with, and thus improve the successful transaction rate.

III. RESULTS AND DISCUSSION

Our simulations examine the performance of this application focusing on the model's effectiveness, computational complexity and ability to resist malicious attacks.

According to the works we define two kinds of node set in the simulations: normal and malicious.

1) Normal peers

Normal peers include two types:

a) Nice-peer (NP).

This type of peer is authentic in providing services, guarantees and feedbacks.

b) Unconscious-peer (UP).

This type of peer provides authentic guarantees and feedbacks, whereas unconsciously provides malicious services with a certain probability, which we set to 0.2 in the simulations.

2) Malicious peers

Malicious peers have three types:

a) Complete-malicious peer (CMP).

CMP provides malicious services, guarantees and feedbacks.

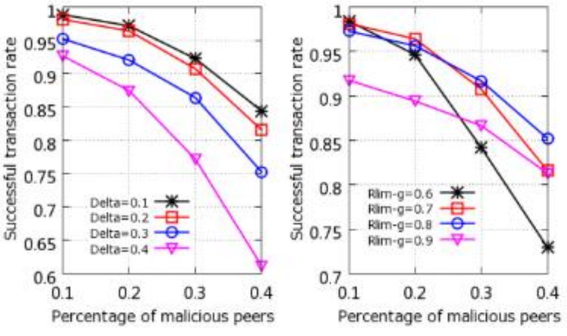
b) Strategic-malicious peer (SMP).

This type of peer behaves strategically based on the amount of its service reputation. When its service reputation is lower, the peer behaves normally (i.e. providing authentic services, guarantees and feedbacks) with a higher probability to accumulate its reputation, and when its service reputation is higher, the peer behaves maliciously with a higher probability to attack the network. In the simulations, we assume that when the service reputation of a SMP exceeds, it would behave normally with the probability of 0.2, otherwise it would behave normally with the probability of 0.6.

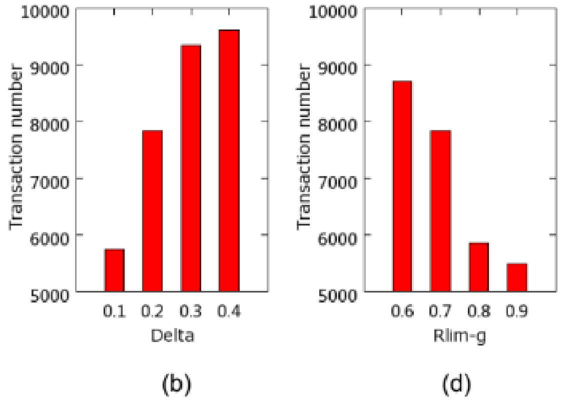
c) Malicious-feedback peer (MFP).

MFP provides authentic services and guarantees, but slanders or builds up specific service peers by providing inauthentic feedbacks.

There are two parameters used in the model,and R_{LIM-g}. Since *Δ* is used to reduce the possibility that two peers with different reputation levels make transactions, the value of should be in (0, 0.5). While R_{LIM-g} is used to ensure that a peer which wants to be the guarantee peer must have higher service reputation.



(a) (c)



Here (a), (c) Evolutions of successful transaction rates with different percentage of malicious peers. (b) Transaction numbers with different Delta (d) Transaction numbers with different R.

Effectiveness of Feedback Verification

In the simulation, we examine the effectiveness of our feedback verification mechanism. The simulation settings are the same as depicted earlier. FMF is short for filtered malicious feedbacks, and SFR is short for successful filtered rate of malicious feedbacks. In the initial phase of the simulation, the reputation difference between normal peers and malicious peers is not distinct, which makes the model unable to prevent malicious peers from receiving services. Thus, there exist a lot of malicious feedbacks. However, after 10th cycle, we see that no matter how many the malicious feedbacks are, our strategy always has its SFR higher than 90%, indicating the effectiveness of our feedback verification mechanism.

IV. CONCLUSION

In this paper, inspired by the establishment of trust relationship in human society and aiming at solving the problems of high computational complexity and inaccurate evaluations existed in the recommendation - based trust models, we presented a guarantee-based trust model in P2P networks. We first described the establishment of a guarantee relationship between the service peer and its guarantee peer(s) on the basis of their mutual evaluations, and then we detailed the establishment of a service relationship between the request peer and the service peer based on both their mutual evaluations and the guarantee relationship owned by the service peer. To strongly encourage peers to provide and guarantee authentic services, we proposed the reputation mortgage and incentive mechanisms. Also, we described the anonymous reputation management mechanism, under which the possibility that a peer falsifies its reputations in collusion with other peers is largely reduced. The simulation results showed that chat application is effective and efficient in terms of lowering the computational complexity, improving the successful transaction rate and curbing the malicious attacks. In the future work, we will focus our efforts on classifying the services and guarantees into categories, and based on which to further improve the model's availability in real-world P2P networks.

V. REFERENCES

[1]. BitTorrent. http://www.BitTorrent.com. 2003.

[2]. Gnutella. http://www.gnutella.com. 2000.

[3]. Edonkey2000.http://www.emule-project.net. 2000.

[4]. S.D. Kamvar, M.T. Schlosser, and H. Garcia-Molina, "The EigenTrust Algorithm for Reputation Management in P2P Networks,"Proc. 12th ACM Int'l World Wide Web Conf. (WWW '03), pp. 640-651, 2003.

[5]. M. Loubna, Y. Iraqi, and R. Boutaba, "Reputation-based trust management in peer-to-peer systems: taxonomy and anatomy," Handbook of Peer-to-Peer Networking, Springer US, pp. 689-732, 2010.

[6]. M. He, Z. Gong, L. Chen, H. Wang, F. Dai and Z. Liu, "Securing network coding against pollution attacks in P2P converged ubiquitous networks," Peer-to-Peer Networking and Applications, pp. 1-9, 2013.

[7]. L. Xiong and L. Liu, “Peertrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities,” IEEE Trans. Knowledge and Data Engineering, vol. 16, no. 7, pp. 843-857, July 2004.

Cite this article as :

Ramya Chowdary Patchala, Srujana Nayudu, Sony Pillutla, "Global Trust : Trust Based Peer-to-Peer Networks using Chat Application", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 2, pp. 771-776, March-April 2019. Available at doi : https://doi.org/10.32628/CSEIT1952156
Journal URL : http://ijsrcseit.com/CSEIT1952156