International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 10 5986 - 5988

Fuzzy Based Trust Model for Peer to Peer Systems

Gayathri S.P
ME student, University of Mumbai
Department of Computer Engineering
Pillai Institute of Information Technology, New Panvel
Mumbai, Maharashtra
gayathridinu@gmail.com

Madhumita A Chatterjee
Professor, University of Mumbai
Department of Computer Engineering
Pillai Institute of Information Technology, New Panvel
Mumbai, Maharashtra
mchatterjeee@mes.ac.in

***Abstract*—**Unknown nature of peer to peer system opens them to malicious actions. A fuzzy based trust model can create trust relationships among peers. Trust decisions are adaptive to modifications in trust between peers. A peer's trustworthiness in giving services and recommendations are assessed in service and recommendation context. The model utilizes fuzzy logic to integrate eight trust evaluation factors into the reputation evaluation process for improving the efficiency and security of peer to peer system. The reputation and recommendation trust metric is combined for computing a global trust metric which helps in selecting the best service provider. In this manner peers develop a trust network in their vicinity without utilizing earlier information and can tone down attack of malicious peers.

Keywords- *Peer-to-peer systems, reputation, trust management, hierarchical fuzzy system, security*

*****

I. INTRODUCTION

In a peer to peer system, the "peers" are personal computer frameworks which are joined with one another by means of internet. The system is self-organizing in that there is commonly no centralization of assets. Accordingly, link capacity is circulated all through peers in the system, and subsequently control is disseminated. Peer to peer clients have double usefulness that is, they can work as clients when they have to download and they can work as a server when the framework needs to serve the assets to different clients.

Trust implies a peer's confidence in an alternate peer's ability, trustworthiness and unwavering quality taking into account its own particular direct encounters. In peer to peer system, a trust model serves to recognize malicious nodes by discovering the trust estimations of every node. All our social associations rely on trust. For instance, in actual life we have just a restricted number of friends to assess from the perspective of trust, yet such number blasts in social networks. Moreover, in actual life our trust is created slowly in time, on the basis of our social experiences, which is not possible in social networks as a result of the tremendous number of potential associations. So, we need to project the capability of our trust using some gadgets.

A fuzzy based trust model for peer to peer framework permits a peer to build up a trust network in their closeness. A peer can make trust associations with good quality peers around itself by detaching malicious peers. To compute the limits of peers in providing recommendations and giving services, two context of trust are defined: recommendation and service context. In this manner the model characterizes four trust metrics: Service trust, Recommendation trust, Reputation and global trust metric. When selecting service providers, the service trust metric is utilized. The recommendation trust metric is important when inquiring recommendations. At the point when calculating the reputation metric, recommendations are assessed in view of the recommendation trust metric. Reputation and recommendation trust metric is combined to form the global trust metric.

Outline of the paper is as per the following. Section 2 examines the related research. Section 3 displays the proposed framework. Section 4 depicts the summary.

II. RELATED WORKS

This section refers to the significant past literature that utilizes the different trust models. These trust models are working on peer to peer system.

According to Bharat Bhargava and Ahmet Burak Can [1] a "Self-ORganizing Trust model" (SORT) for peer to peer systems can decrease malicious activity by creating trust relations among peers in their closeness.

Qiyi Han, Hong Wen, Ting Ma and Bin Wu [2] proposed a ''Self-Nominating Trust Model Based on Hierarchical Fuzzy Systems for Peer-to-Peer Networks''. Hierarchical fuzzy system integrates 8 factors into the reputation evaluation process.

"Pseudo Trust: Zero-Knowledge Authentication in Anonymous P2Ps" by Li Lu, Jinsong Han, Yunhao Liu, Lei Hu, Jinpeng Huai, Lionel M. Ni, and Jian Ma,[3] is a zero-knowledge authentication scheme, where each peer, creates an unforgeable and verifiable pseudonym utilizing a one-way hash function as an alternative of using its real identity.

Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons, and Abraham D. Flaxman [4] discussed the paper "SybilGuard: Defending against Sybil Attacks via Social Networks". The protocol gurantees that the quantity of attack edges does not depend on the number of Sybil identities.

ShanshanSong, Kai Hwang, and Runfang Zhou, Yu-Kwong Kwok[5], defines "Trusted P2P Transactions with Fuzzy Reputation Aggregation". This is an efficient and effective reputation system in view of fuzzy-logic approach, utilizing fuzzy-logic's capacity to handle vagueness, fuzziness, and deficient information adaptively.

III. PROPOSED SYSTEM

The proposed system considers various elements in the trust assessment process. These elements are incorporated by a hierarchical fuzzy system to total the fuzzy reputation matrix. The proposed system has been partitioned into four modules: Reputation Metric, Service Trust Metric, Recommendation Trust Metric and Global Trust Metric.

Initially all peers are assumed to be strangers. Peers must contribute others in order to build trust relationships. A trusted peer cannot observe all interactions in a peer to peer system and might be a source of misleading information. A peer turns into

an acquaintance of another peer after giving a service to it. Using a service from a peer is called a service interaction. A recommendation represents an acquaintances opinion about a peer. A peer requests recommendations only from its acquaintances. There are no trusted peers to oversee trust relationships. Peers periodically leave and join the network. Figure 1 depicts the architecture of fuzzy based trust model. Once the peer logs in, it can interact with other peers via upload and download process. After interaction, trust metrics are calculated so as to identify the malicious peers.

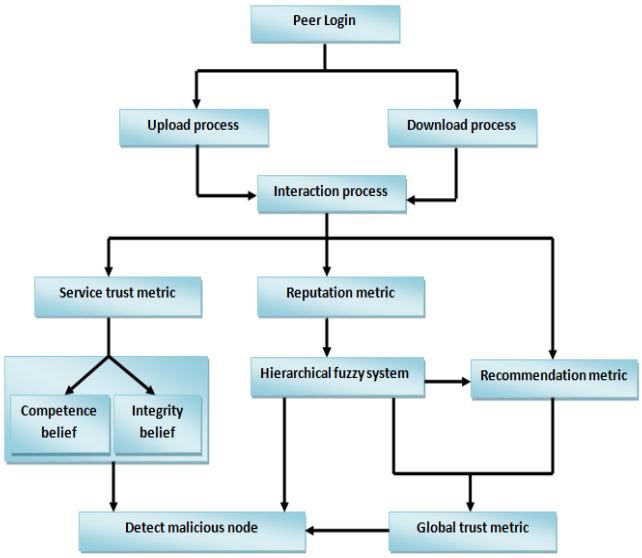

Figure 1. Architecture of fuzzy based trust model.

A. *Interaction Process*

The interaction process takes place by connecting all the peers that wish to upload and download the files. The interaction process consists of two phases: Upload process and Download process.

P_i means the i^{th} peer. At the point when P_i utilizes a service of an alternative peer, it is an interaction for P_i. Interactions are considered as unidirectional. For instance, if P_i downloads a file from P_j, it is an interaction only for P_i since the information about the download is not saved in P_j. P_j is an acquaintance of P_i, if P_i had at least one interaction with P_j. Otherwise, P_j is a stranger to P_i. A_i indicates P_i's set of acquaintances. A peer stores a different history of interactions for every acquaintance. SH_{ij} signifies P_i's service history with P_j where sh_{ij} indicates the current size of the history. sh_{max} signifies the upper bound for service history size. Since new interactions are annexed to the history, SH_{ij} is a time ordered list.

In upload process, a peer shares resources with different peers. When the file is shared, acquaintance list is reorganized in order to know its neighborhood process that has interacted. In download process, peer request other peers to download the resources. After the interaction process, trust values are evaluated.

B. *Reputation Metric*

Reputation is a peer's belief in another peer's capabilities, honesty and reliability. In this fuzzy based trust model eight factors are integrated into the reputation evaluation process. At the beginning phases of an interaction, it is hard to build the reputation because, it is dangerous to contact another peer and download its resources. These trust factors[2] permit a peer to recommend themselves whenever and accordingly advance their resources.

The trust factors are defined as follows:

1) Malicious behavior (MB)

In peer to peer environment, malicious behavior is a vital security factor. One way of preventing malicious peers is to decline their reputation level in the event that they are undesirably elected as service providers. In the mean time, malicious peers ought to be recognized and stamped too.

2) Bandwidth (BW)

Bandwidth decides a peer's capacity for giving data transactions. A bigger bandwidth gives more data transactions.

3) Online time rate (OR)

Due to the dynamic and self-governing nature of peer to peer networks, a peer can join and leave the system whenever. Online time rate is recorded to demonstrate the rate of peer's login time.

4) Download success rate (DR)

Only successful downloads are the precondition for sharing. Peer can record the quantity of success download and the quantity of failed download to get the download success rate.

5) File Size (FS)

It shows the size of the requested resource and the quantity of files included in the resource.

6) Time to live (TL)

This component demonstrates the remaining (online) time before a peer clears out. The requester can estimate the task progress in light of this component.

7) Upload Speed (US)

Similar to the bandwidth, upload speed decides the capacity of sending information.

8) Content relevance (CR)

Spam and irrelevant files are not common. Indeed a true and accessible file can be appended with irritating data for example unfamiliar popup link or spam advertisement.

The above trust factors are integrated by a Hierarchical fuzzy trust system to compute the reputation value of peers. The outline of Hierarchical Fuzzy System is given underneath.

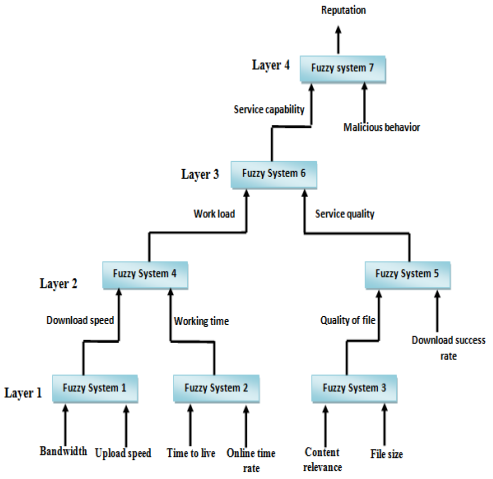

Figure 2. Hierarchical fuzzy trust framework.

There are six intermediate variables in the system. Bandwidth and upload speed is utilized to infer the download speed. Time to live and online time rate is utilized to infer the

working time of the peer. Content relevance and file size contributes the quality of file. Download speed, working time, quality of file and download success rate will be fed as inputs to the 2nd layer fuzzy system. Thus the outcome of 2nd layer fuzzy system that is work load and service quality is utilized by 3rd layer fuzzy system to infer service capability. Fuzzy logic utilizes the service capability and malicious behavior to infer the reputation value of the peer.

C. Service trust metric

After completing an interaction, P_i assesses quality of service utilizing three parameters: Satisfaction, Weight and Fading effect. Satisfaction[1] indicates how well a service provider was at the time of an interaction. An interaction's impact is measured with a weight[1] value. The importance of an interaction fades as new interactions happen which is called as fading effect. Let $s_{ij}^k, w_{ij}^k, f_{ij}^k$ indicate the satisfaction, weight and fading effect of k^{th} interaction of P_i with P_j where, $0 \le s_{ij}^k, w_{ij}^k, f_{ij}^k \le 1$. The fading effect [1] is computed as follows:

$$f_{ij}^k = \frac{k}{sh_{ij}}, 1 \le k \le sh_{ij} \quad (1)$$

A peer computes an acquaintance's competence and integrity belief[1] values utilizing the information from its service history. Competence belief, cb_{ij} speaks to how well an acquaintance fulfilled the needs of past interactions. It is measured as the average behavior in the past interactions.

$$cb_{ij} = \frac{1}{\beta_{cb}} \sum_{k=1}^{sh_{ij}} \left(s_{ij}^k . w_{ij}^k . f_{ij}^k \right) \quad (2)$$

Where the normalization coefficient, $\beta_{cb} = \sum_{k=1}^{sh_{ij}} \left(w_{ij}^k . f_{ij}^k \right)$

Confidence level in the predictability of future interactions is called integrity belief, ib_{ij}. It is computed as an approximation to the standard deviation of interaction parameters.

$$ib_{ij} = \sqrt{\frac{1}{sh_{ij}} \sum_{k=1}^{sh_{ij}} \left(s_{ij}^k . w_{ij}^\mu . f_{ij}^\mu - cb_{ij} \right)^2} \quad (3)$$

P_i may compute service trust metric[1] as follows:

$$st_{ij} = cb_{ij} - {ib_{ij}}/{2} \quad (4)$$

D. Recommendation metric

Recommendation[2] implies an acquaintance's feedback about a peer. When peer C collects the recommendation trust information of peer D, peers who have the direct interaction experiences with peer D will send a feedback to peer C. Then peer C compute a recommendation trust metric of peer D as formulated below.

$$R(C,D) = \sum_{i=1}^{N} sim(C,i) . {LT(i,D)}/{sim(C,i)} \quad (5)$$

where N is the number of peers who send the feedbacks. LT(i,D) is the reputation metric of peer D. sim(C,i) is the similarity measure between peer C and peer i. The similarity measure reflects the cognitive similarity by the way of comparing trust evaluation among peers and is defined as:

$$sim(i,j) = \sum_{l \epsilon M} \left(1 - d\left(LT(i,l), LT(j,l) \right) \right) / |M| \quad (6)$$

Here M is the mutual friends of peer i and peer j.

E. Global trust metric

The global trust metric[2] is integrated as the weighted sum of the reputation and the recommendation trust metrics.

$$T_{global} = \alpha LT + \left((1-\alpha) R \right) \quad (7)$$

where the weighting factor α is a value between 0 and 1. α can also be automatically assigned as

$$\alpha = m/(n+m) \quad (8)$$

Where m is the number of reputation feedbacks and n is the number of recommendation feedbacks.

IV. Conclusion

Fuzzy based trust model will not only resolve the security issues in peer to peer systems but can improve security and efficacy of systems. The model evaluates trust in a comprehensive manner, where peers are promoted to share by distinguishing their sharing desires and transmission abilities. The trust model can speed up reputation accumulation process to promote peer activities while balancing the workload in the network.

Acknowledgment

I am deeply indebted to my guide Dr. Madhumita A Chatterjee for her legitimate direction and valuable recommendations which assisted me to improve my works. I would like to thank my family members who helped me with this venture. I am grateful to my college Pillai Institute of Information Technology, New Panvel for their significant backing.

References

[1] 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, january/february 2013

[2] Qiyi Han, Hong Wen, Ting Ma and Bin Wu,''Self-Nominating Trust Model Based on Hierarchical Fuzzy Systems for Peer-to-Peer Networks'' IEEE/CIC ICCC 2014 Symposium on Privacy and Security in Commutations

[3] Li Lu, Member, IEEE, Jinsong Han, Member, IEEE, Yunhao Liu, Senior Member, IEEE, Lei Hu, JinpengHuai, Member, IEEE, Lionel M. Ni, Fellow, IEEE, Jian Ma, "Pseudo Trust: Zero-Knowledge Authentication in Anonymous P2Ps " IEEE Transactions on Parallel and Distributed Systems.

[4] Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons, Member, IEEE, and Abraham D. Flaxman, "SybilGuard: Defending Against Sybil Attacks via Social Networks" IEEE/ACM Transactions on Networking, Vol. 16, No. 3, June 2008.

[5] ShanshanSong, Kai Hwang, Runfang Zhou, Yu-Kwong Kwok, "Trusted P2P Transactions with Fuzzy Reputation Aggregation" IEEE Internet Computing November - December 2005.

[6] Anupam Das and M. Mahfuzul Islam, "A Novel Feedback Based Fast Adaptive Trust Model for P2P Networks" 35th Annual IEEE Conference on Local Computer Networks.

[7] Runfang Zhou, Member, IEEE, and Kai Hwang, Fellow, IEEE Computer Society, "PowerTrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing" 2007 IEEE Published by the IEEE Computer Society