A Contemporary Framework for P2P Connected Systems through Trust Model for Self Organizing Nodes

Bhanusri[1], Raghavendra Rao[2], Janapati Venkata Krishna[3]

[1] pursuing M.Tech (CSE), [2]Assistant Professor (CSE Department), [3]Associate Professor & HOD (CSE Department)
[1,2,3]Holy Mary Institute of Technology and Science, Keesara, Affiliated to JNTU- Hyderabad, A.P, India

***Abstract*— The open nature of the peer-to-peer systems exposes them to malicious actions. Here in this paper we introdusing distributed algorithms that can enable peer to get the trustworthiness of other peers based on interactions of those peers in the past with other peers. The peers in the network are able of creating a trust network on their own proximity by the help of the local information it already have with it and without trying to learn any global trust information. The contexts of the trust, recommendation and service contexts are defined for measuring the trustworthiness in providing services to the other peers and giving recommendations about the other peers. Interactions done with other peers and recommendation about other peers are evaluated based upon the recentness of the information, importance and the satisfaction of the peer parameters. As the satisfaction of the peer is also considered as the most vital one because the recommendation will be always based upon the satisfaction of the peer that is a peer will recommend any other peer only if it is satisfied by the interaction with that peer. In addition to this the recommender's trust worthiness about a recommendation given about a peer will be considered important while evaluating the recommendations. While moving with the simulation experiments on file sharing application it showed that this proposed trust model can reduce attacks on nearly 16 different types of behaviour models. In these experiments we see that good peers were able to form trust relationships in their own proximity and are able of isolating the untrusted peers.**

Keywords**—** Trust Model, Peer-to-peer Systems, trust management

1. INTRODUCTION

The peer-to-peer systems will rely on collaboration among the peers to accomplish the tasks. The Ease for performing malicious activity has been a threat for the Peer-to-Peer Systems. If we create long term relationships among the peers then we can provide a better secure environment by reducing the uncertainty and rusk for the future Peer-to-Peer interactions. But establishing trust among the peers in unknown entity is difficult in the presence of such a malicious environment. Furthermore trust is considered as a social concept and is hard to measure with numeric values. Some metrics are required to represent the trust in computational model. Classification of the peers into trustworthy peers or untrustworthy peers is not sufficient in most of the cases. These metrics should maintain a precision so that the nodes can be ranked according to their trustworthiness. The trust among the peers can be measured using the Interactions and feedbacks of the peers. Though the interactions among the peers provide certain information about the peer but the feedbacks might contain deceptive information. Because of this the assessment of trustworthiness is a challenge.

A central server in the presence of an authority is preferred to store and manage the trust information. This central server will store the trust information securely and will define trust metrics. But this central server will not be present in most of the P2P systems, so the peers in this system will organize themselves for storing and managing the trust information about each other. The management of this model and its information is dependent on the structure of P2P network. In this Distributed Hash Table (DHT) approaches each peer will store the feedbacks of other peer and becomes a trust holder. The DHT will allow you to access the global trust information which is stored by the trust holders efficiently. In these unstructured networks every peer will store trust information about the peers in its neighbourhood or about the peers with which it has interacted in the past. The trust query of the peer is either flooded into the network or may be sent to neighbourhood of the query initiator.

We here in this paper propose a trust model that is able of reducing malicious activity in a P2P system by establishing trust relations among the peers in their neighbourhood. Any prior information or trusted peer will be used to leverage the trust establishment. Peers may not always try to get the trust information from all the other peers. Sometimes the peer develops a local view for itself about the peers that are interacted with it in the past. In this way the good peers will form a dynamic trust group in their nearness and by using these are able to isolate the malicious node. In this model all the peers are assumed to be strangers in the beginning. A peer becomes known to other only after providing a service. At the beginning when the peer does not have any acquaintance it will choose to trust a stranger. Using the service of a peer is called as the interaction and it is evaluated based on the weight, recentness and satisfaction of the requester. An acquaintance is the one who is always preferred over the strangers even though both of them are equally trust worthy. Any peer's feedback on the other peer which is called as the recommendation will be evaluated depending upon the trustworthiness of the recommender since it is to be considered as recommenders own experience.

2. Computational Model

For our Trust Model we make the following assumptions,

All the peers in the network have equal computational power and responsibility. There are no centralized, privileged, or trusted peers to manage trust relationships. The peers in the network will join and leave it occasionally. Every peer will provide services to others and uses the services of the other peers.

2.1 Preliminary Notations

P_i denotes the ith peer. Whenerver P_i usese services of other peer, it says Pi interatction, the interacrtion is in unidirection. For example, if Pi uses services of P_j, it denotes interaction of pi, and in the pj there is no information was stored.

If P_i containes one interaction with P_j, P_j is called as acquaintance of pi. Other wise we called Pj is a stranger to P_i. Pi's set of acquaintance denotes by A_i. For each acquaintance the peer stores a separate history of interaction. Pi's service history expressed by SH_{ij} with P_j, here sh_{ij} express the present size of history. The upper bound service history size expressed by sh_{max} . with this newly coming interactions added with history.

Parameters of an intractoin. After completing an iterction, Pi assigns a satisfaction value for the interaction and calculate the quality of service.The pi's interaction and satisfaction to Kth interaction with pj nis expressed by $0 \leq s^k_{ij} \leq 1$.if the given interaction was not complete $s^k_{ij=}0$. By using weight value interactions importance was measured. The weight of kth interaction of pi with pj expressed by $0 \leq w^k_{ij} \leq 1$.

For calculating skij and wkij are are depending to the application, in the fale providing application, the authentication of a file,the delay average, download speed, of packets transmission rate and offline/online period of the service provider might have the parameter $s^k_{ij.}$ The size of the file and popularity of the file to be calculate with w^k_{ij}.

TABLE 1
Notations of the trust metrics

Notation	Description
skij	Pi's satisfaction about kth interaction with pj
wkij	Weight of pi's kth interaction with pj
fkij	Fading effect of pi's kth interaction with pj
rij	Pi's reputation value about pj

stij	Pi’s service trust value about pj
rtik	Pi’s recommendation trust about Pk
shij	Size of Pi’s service history with Pj

Whenever new interaction was perform the old interation importance will be decreased. This problem is identified by the fading effect parameter and try to maintaine consistace in future interaction. The peer can’t misbehave by depending on new history even though the old interaction lost its importance.The fading reaction of kth interaction of pi with pj expressed by 0≤fkij≤1. calculated as follows.

$$f_{ij}^{k} = \frac{k}{sh_{ij}}, 1 \leq k \leq shij$$

After completion of adding an interaction to SH$_{ij}$, Pi re compute f_{ij}^{k} values. The fading reaction could be described as a time function whenever its value is neede it will recalculated. By the time causing , interactions lose values with this all the peers lose their reputation even though no bad interaction thing happens.

Let $SH_{ij}\{r_{ij}^{1}, r_{ij}^{2}, ..., r_{ij}^{shij}\}, where\ r_{ij}^{k} - (s_{ij}^{k}, w_{ij}^{k})$ is a tuple defining information about the kth interaction. if shij=shmax Tkij is deleted wheever adding the new interaction.After completing the excepiration period the interaction will be deleted from the history. Those must be described according to sh$_{max}$ proceeding rate of interactions.

Trust metrics. The Pi’s standing value about pj is decribed by 0≤rij≤1. Like that 0≤stij,rtij≤1 denotes pi’s recommendation trust value and service about pj.We describe rij = stij = rtij = 0 when Pj is unknown to Pi. This is a security beside pseudonym changing of malevolent peers. Subsequently,those type of peers lost the value and cann’t get benefit by appearing with new one.

2.2 Service Trust Metric

At the time analijing the acquaintance trust in the service, a peer first evaluvate the capability and reliability trust values using the information which are available in the its service history. The competence trust denotes how better an acquaintance satisfied he requirement of past interactions. Here we calculate the competence , interaction must be ratio to their weight and quickness. Then cdij calculated by Pi as shown bellow

$$cb_{ij} = \frac{1}{\beta cb} \sum_{k=1}^{shij} (s_{ij}^{k} . w_{ij}^{k} . f_{ij}^{k})$$

βcb = $\sum_{k=1}^{shij}(w_{ij}^{k} . f_{ij}^{k})$ is normalization coefficient. If in case pj all the communications effortlessly (S$^{k}_{ij}$ = 1 for all k), th βcb (coefficient) guarantee that cbij = 1. With 0≤S$^{k}_{ij}$, S$^{k}_{ij,}$ S$^{k}_{ij}$≤1, with the above definition, cbij always choose a value between 0 and 1.

Even though a peer is capable but it may denotes unreliable behavoiur. The maintaining of consistency is aas importance as capability. The confidence of predictability for future communication is called as integritcommunication is called as integrity belief. The integrity trust of Pi about Pj is represented by ib$_{ij}$ in the context of service. Abnormality from the normal behaviour is a quantity of the integrity belief. Therfore, ib$_{ij}$ is computed as approximization for the standard deviation of communication parameters

$$ib_{ij} = \sqrt{\frac{1}{shij} \sum_{k=1}^{shij} (s_{ij}^{k} . w_{ij}^{\mu} . f_{ij}^{\mu} \quad cb_{ij})^{2}}$$

The meaning of a small value of ibij is most expectable behavior for p$_{j}$ in the future communications. The meaning of w$^{\mu}_{ij}$ and f$^{\mu}_{ij}$ is the values w$^{k}_{ij}$ and f$^{k}_{ij}$ available in the SHij. Later, the weight and fading parameters are independent on satisfaction parametrs, we have interest in average satisfaction parameter. By using w$^{\mu}_{ij}$ and f$^{\mu}_{ij}$ values the above parameters are eliminated from the calculation for all communication. We could estimate f$^{\mu}_{ij}$ as bellow

$$f_{ij}^{\mu} = \frac{1}{sh_{ij}} \sum_{k=1}^{sh_{ij}} f_{ij}^{k} = \frac{sh_{ij} + 1}{2sh_{ij}} \approx \frac{1}{2}$$

The Pi has some future assumptions based on interactions with Pj and pi wishes ot maintaine a satisfaction based on this expectation. If the satisfaction parameter needs to follow a general distribution, the cbij and ibij is treated as the satisfaction parameters standard deviation (σ) and expected mean (μ), respectively. Conferring to the normal distribution’s cumulative distribution, the chance is ϕ(0) = 0.5 if interaction satisfaction is less than cb$_{ij}$. If in case pi sets to st$_{ij}$ = cb$_{ij}$ half of the interaction satisfaction is less than cb$_{ij}$.The lower estimation will makes pi is more confident with pj. From lower future interaction means less satisfaction value caompare than stij value. Stij is might calculated by Pi as bellow

$$St_{ij} = cb_{ij}-ib_{ij}/2.$$

In this current case the future interaction satisfaction rate is less than stij with ϕ(-0.5) = 0.3185 prospect. Adding of ibij to the calculation forces of Pj is perform more consistency from erratic growth ibij value. The selection of ϕ(-0.5) will comes from our research results. In the realtime environment, the satisfaction parameter might be follow the different type of distribution. According its past interaction each peer will use statistical analysis for more resolve detailed distribution change.

So every peer will describe a specific distribution for every acquaintance and change its reliable calculation according to its acquaintances.

From the pj not consider repution The 5ht eqation is not completd. In the initial phase trust relationship model reputation is most important. When there is few or no ineraction with acquaintance , a peer needs to depends on the reputation metric. The competence and integrity trust will get more importance When more interactions happened. So pi calculate st_{ij} as bellow

$$st_{ij} = \frac{sh_{ij}}{sh_{max}}\left(cb_{ij} - \frac{ib_{ij}}{2}\right) + \left(1 - \frac{sh_{ij}}{sh_{max}}\right) r_{ij}.$$

The above will make balances effects of interactions and do thw reputation value on stij value. At the time of Pj is new ot Pi, shij=0, and $st_{ij} = r_{ij}$. If interactions going to increase with pj, shij gets more important and r_{ij} gets less important.Whenever $sh_{ij} = sh_{max}$.

2.3 Reputation Metric (r_{ij})

This reputation metric is quantify new arrival honesty depends on recommendations. If pi desire to compute the value of rij. It will send the reputation queries to collect the references from their acquaintance.

Below algorithm shows how the pi selects the truthness of acquaintances and requists to their recommendations, those can be cooleted with reputation query and |S| express the size of set S. In the algorithm first pi sets high threshold to recommendation trust values and sending requesting for recommendations to highly trusted acquaintances. To reduce unnecessary network traffic it will decrase the threshold and repeats for same work.

Algorithm 1. GETRECOMMENDATIONS(pj)

```
$\mu_{rt} \leftarrow 1\frac{1}{|Ai|}\sum_{pk\in A} rt_{ik}$
$\sigma_{r\,t} \leftarrow \frac{1}{|Ai|}\sqrt{\sum_{pk\in Ai} (rt_{ik} - \mu_{rt})^2}$
$th_{high} \leftarrow \mu_{rt}+\sigma_{rt}$
$th_{low} \leftarrow \mu_{rt}+\sigma_{rt}$
rset $\leftarrow$ ǿ
while $\mu_{rt} - \sigma_{rt} \leq th_{low}$ and | rest | $< \eta_{max}$ do
    for all Pk $\epsilon$ $A_i$ do
        if $th_{low} \leq rt_{ik} \leq th_{high}$ then
            rec $\leftarrow$ RequestRecommendation $(P_k,P_j)$
            rset $\leftarrow$ rset $\cup$ {rec}
        end if
    end for
    $th_{high} \leftarrow th_{low}$
    $th_{low} \leftarrow th_{low} - \sigma_{rt}/2$
end while
return rset
```

Let's take T_i = {p1,p2,….p3} are the group of peers selected in the Algorithm 1and t_i denotes number of peers in the particular group. If the pkϵA_i it had minimum of one interaction with the Pj.

3.4 Recommendation Trust Metric (rtik)

After completing the calculation of rij value, Pi will updates the recommendations truth value of recomenders that was based on the correctness of their recommendations. This segment is going to explain about how Pi updates rtik value based on pk's recommendation.

Like to interactions, three more parameters are calculated about the recommendations. $0 \leq rs^{z}_{ik}, rw^{z}_{ik}, rf^{z}_{ik} \leq 1$ represents the satisfaction, fading effect and weight of Pi's zth recommendation fro Pk,

3.5 Selecting Service Providers

When Pi, searching for specific service, it will get all service providers list, based on file sharing mechanism it will down load a file from one or multiple upoader. Checking the integrity is problem with multiple uploaders. Because which is uploaded by whom. To do online integrity checking with multiple uploaders some of complex methods are utilizing like secure hashes, Merkal hashes and cryptography . By using competence belief, size of service history, trust metric and integrity belif values the selection of service provider will be done. When the Pi wants to download a file it will checks the uploader highest trust service value, it always shoosing the peer which has hieghest priority weight size.The selection process of best service provider is overhead since some peers on idle. A selection algorithm will load rebalance to utilize the all the resources of peers. If the peer complets maximum number of uploaded it will rejects the requests,thus requester will get requests from other peer.

3 CONCLUSION

In our mechanism we are providing trust model peer to peer to connection, a peer may have malicious peers around itself, we need to provide services only for trustd peesrs. Context of trust and recommendation context define for measuring capabilities of peers.

We studied association,individual and pseudonym attackers chainging to check the trustiness of interactions. Another problem is SORT will maintaine trust all over the network. If peer changes it it attachment for the network. It may lose the trust of network. These problems might be deliberate as a future work to extend the trust model.

By using the reliable information it doesn't solvw all the security related issues in P2P systems, but it could be improve security and effectiveness of the system.

REFERENCES

[1] K. Aberer and Z. Despotovic, "Managing Trust in a Peer-2-Peer Information System," Proc. 10th Int'l Conf. Information and Knowledge Management (CIKM), 2001.

[2] F. Cornelli, E. Damiani, S.D.C. di Vimercati, S. Paraboschi, and P. Samarati, "Choosing Reputable Servents in a P2P Network," Proc. 11th World Wide Web Conf. (WWW), 2002.

[3] S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The (Eigentrust) Algorithm for Reputation Management in P2P Networks," Proc. 12th World Wide Web Conf. (WWW), 2003.

[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] A.A. Selcuk, E. Uzun, and M.R. Pariente, "A Reputation-Based Trust Management System for P2P Networks," Proc. IEEE/ACM Fourth Int'l Symp. Cluster Computing and the Grid (CCGRID), 2004.

[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] J. Kleinberg, "The Small-World Phenomenon: An Algorithmic Perspective," Proc. 32nd ACM Symp. Theory of Computing, 2000.

[8] S. Saroiu, P. Gummadi, and S. Gribble, "A Measurement Study of Peer-to-Peer File Sharing Systems," Proc. Multimedia Computing and Networking, 2002.

AUTHORS PROFILE

Ms. Bhanusri, pursuing M.Tech (CSE) from Holy Mary Institute of Technology and Science, Keesara, Ranga Reddy Dist., Affiliated to JNTU-HYDERABAD

Raghavendra Rao, Assistant Professor (CSE Department), Holy Mary Institute Of Technology and Science, Keesara, Ranga Reddy Dist., Affiliated to JNTU-HYDERABAD.

Janapati Venkata Krishna, Associate Professor & H O D (CSE Department), Holy Mary Institute Of Technology and Science, Keesara, Ranga Reddy Dist., Affiliated to JNTU-HYDERABAD.