Avoiding Malicious Activities in Peer to Peer System using Self Organizing Trust Method

G. Samuvelraj
PG Scholar
Department of Computer Science and Engineering
Sri Shakthi Institute of Engineering and Technology
Coimbatore.

N. Nalini
Assistant Professor
Department of Computer Science and Engineering
Sri Shakthi Institute of Engineering and Technology
Coimbatore.

***Abstract* - Networks are subject to attacks from malicious sources. Sending the data securely over the network is one of the most tedious processes. A peer-to-peer (P2P) network is a type of decentralized and distributed network architecture in which individual nodes in the network act as both servers and clients of resources. Peer to peer systems are incredibly flexible and can be used for wide range of functions. And also a Peer to peer (P2P) system prone to malicious attacks. To provide the security over a peer to peer system the self-organizing trust model has been proposed. Here the trustworthiness of the peers has been calculated based on past interactions and recommendations. The interactions and recommendations are evaluated based on importance, recentness, and satisfaction parameters. By this the good peers were able to form trust relationship in their proximity and avoids the malicious peers.**

Keywords— SORT, Network Security, Metrics, Peer to Peer

I. INTRODUCTION

Nowadays, security is considered as one of the most critical parameter for the acceptance of any networking technology. Basically a network uses the client-server model to perform any task. A peer-to-peer is a type of network in which the nodes act as both the client and server. This model of network arrangement is differs from client-server model where communication made to and from any node. A peer-to-peer network depends on the collaboration of nodes to perform the tasks. A peer-to-peer network can be classified into two types as structured and unstructured.

In a structured network the overlay is organized into a specific topology, and the protocol ensures a node can efficiently search network to perform any task. Most structured network uses the Distributed hash table to access the network. In distributed hash table (DHT) based approaches each peer stores the feedback in the table. By this, the peer becomes a trusted one. The information stored in DHT is global and that can be accessed efficiently. The trust information has been calculated by sending trust queries. Trust queries are flooded to the network to collect the trust information. Usually, calculated trust information is not global and does not show opinions of all nodes.

In an unstructured network the overlay is not organized by any design, but rather are formed by nodes that randomly connections to each other. When a peer wants to find a particular data in an unstructured network, the query must be flooded through the network. Flooding causes very high signal traffic, uses more memory, and does not ensure the queries will be resolved. And, there is no guarantee that the query will find a correct peer.

Opportunity to performing malicious activity is a danger for security in peer-to-peer system. Creating trust relationships among peers can provide more secure by reducing the risk. However, creating trust relationship among unknown peer is difficult. An interactions and feedbacks of the peers gives information to measure trust between peers.

A Self-Organizing Trust model proposed to decrease malicious activities in peer-to-peer system by creating trust relationship between peers. In this, the peers do not collect information from all the peers. Instead of that each peers create its own view of trust about the peers interacted in the past. By this the malicious peers are avoided from the network.

In this approach, in the beginning the peers are assumed as a stranger. If a service has been provided by the stranger then the stranger becomes a trusted one to the corresponding peer. By evaluating the trustworthiness the service can be get from stranger. The trustworthiness has been calculated based on the past interactions.

The interactions are evaluated based on the weight, recentness and satisfaction. The recommendation is used to calculate the feedback of a stranger by a trusted one. The recommendation value may affect the trustworthiness of a stranger. These interactions and recommendations are stored in a separate history.

The self-organizing trust model has three metrics to evaluate the trust worthiness. Service trust metric is used to select the trusted third party. It gives the trustworthiness of the various third parties. Reputation and recommendation trust metrics are used to calculate the trustworthiness of the new service provider i.e., a stranger. The reputation value calculated based on past interactions and recommendation trust value calculated based on recommendations.

II. RELATED WORKS

The reputation system is widely used for building trust in all the methods till now. The trust is evaluated to get secured access in an unstructured network. A central server is the preferred way to get access in a network, and it stores opinion and interactions about all the nodes in centralized table. This technique is not feasible in an unstructured network, because the nodes are acting as a client as well as a server in an unstructured network. The distributed hash table (DHT) provides efficient access to trust information but, the DHT is possible only in structured network.

In Aberer and Despotovic's approach [1] all the peers give their negative opinion by using the P-Grid technique. By this a peer said to be trusted until there is no negative opinion. Peer to peer network has more attacking opportunity by malicious peers. Hoffman, Zage and Nita-Rotaru approach [4] attacks in a peer to peer network are overcome by appropriate defense techniques.

In Marsh approach [5] Own experiences are considered to build trust relations, and that does not consider the other's information. In Kamvar, Schlosser, and Garcia-Molina approach [6] An Eigen trust algorithm is used to evaluate the trust value. In CAN approach [2] Secured data access is achieved through trustworthiness and matching of the policies of sender and receiver.

In the eigen trust approach [7] a number of malicious files has been decreased by calculating the global trust value. In the reputation based trust management method [10] the robust reputation mechanism has been used, where the distributed polling algorithm to manage the reputation values to avoid malicious peer. In gossip protocol mechanism [12] a reputation value is calculated for all the nodes to find the attackers. In a self organizing trust model approach [3] each peer stores its own view about interacted peers, by that a trustworthiness is calculated to get a good peer in their proximity.

III. PARAMETERS

'x' denotes the particular peer in a network. When x gets a service from a peer y then y becomes a trusted one to x and stores interaction details. A peer said to be trusted to another peer if it had at least one interaction. Consider that z is a stranger to x. A peer said to be stranger if there is no past interaction between them. Interaction details are stored in service history of appropriate peer. To get the past interactions the service history has been checked.

To calculate the trust value three important parameters are considered. Let w is the weight, s is the satisfaction value and r is the recentness. And these values are defined in 0<=1.

Consider the file sharing application. Were the weight and satisfaction are defined by speed of access, delay, rate of transmission, size, popularity etc., Recentness is achieved by providing more priority to the new interactions over old interactions. The service history must be updated. It should give important to new interactions.

IV. METRICS

Service trust metric

The service trust metric has been used to evaluate the trustworthiness of trusted third party. To evaluate the trustworthiness of trusted third party, a peer calculates the competence belief and integrity belief values using the information in the service history.

The competence belief defines how well a trusted third party satisfied the needs of the peers in past interactions. If a trusted third party completes all interactions perfectly then the competence belief value set to be 1. Otherwise, the value lies in 0<=1 according to the completion of interaction.

Consistency is also important as well as competence. That has been obtained by evaluating integrity belief. Integrity belief value is an approximation. That has been evaluated from interactions. If the trusted third party maintains its level of expectation from requester then the value set to be 1. Otherwise, the value lies between o<=1 according to the satisfaction.

These two values competence beliefs and integrity belief are calculated by using the weight, recentness and satisfaction values. This process has been done for all the trusted third parties and the values are stored in service history. From the service history a third party with the highest trust value is taken as a trusted third party to get recommendations.

Reputation trust metric

The reputation trust metric calculates the trustworthiness of a stranger based on past interactions. To calculate the reputation value, a reputation query will send to peers. The reputation query collects the recommendations from its trusted third party and the maximum number of recommendations collected through reputation query. There is high threshold value has been set to recommendation trust value. It starts to collect recommendations from its highly trusted third party. Likewise, it collects recommendations from all the trusted third party. If the maximum recommendations are received, then the process will be stopped.

After collecting the recommendations the reputation value has been calculated. Additionally competence and integrity belief values also calculated when a peer needs more trustworthiness about a peer. These values are taken from service history. While this, an own experience is considered. When the threshold value of service history is equal to the maximum size of service history, then the trusted third party has high level experience about a stranger.

Recommendation trust metric

Recommendation trust metric is also used in evaluating the trustworthiness of a stranger. The recommendation trust value evaluated to calculate the trustworthiness of a stranger by recommendation from trusted third party. After calculating the recommendation trust metric, a recommendation value of recommender is updated. Three parameters namely weight, satisfaction, and recentness of trusted third party are used to calculate the recommendation trust value. The recommendations are stored in a recommendation history.

To calculate the satisfaction value the requester compares the reputation value, competence belief value, the integrity belief value provided by trusted third party with values in the history. If these values are equal, then the satisfaction value set to be 1. The weight calculated by service history size. If the history is large, then the maximum value is set to the weight. To provide more trustworthiness competence belief and integrity belief are considered. These values are taken from service history of appropriate peer.

After getting all the values a requester calculates the reputation value. Then, the requester evaluates the trusted third party's recommendations trust value and stores the results in service history. If the stranger is trustworthy enough, a requester gets service from the stranger. Getting service is done as follow. First, the recommendation request has been sent to trusted third party. The trusted third party receives a request and sends a recommendation about a stranger. Then, the service request will send to a stranger to get the service. Interactions, opinion and service trust values are stored in a history.

Selecting service provider

After calculating the trustworthiness, the peer selects the service provider to get the needed service. When requesting a particular service there may be several service providers. To select one of the service providers some values are considered.

First, the peer which had the highest service trust value has been selected as the service provider. If the peers had equal service trust values, then the peer which had a larger history size is selected to be a service provider. If history size is also equal, the peer which had a higher competence belief value is selected to be a service provider. If this value also equal, then the bandwidths of the peers are compared. If the bandwidth also equal, then any one of the peers has been selected randomly as a service provider from the list of service providers.

V. ATTACKERS BEHAVIOURS

A good peer provides authentic files and gives needed recommendations. An attacker performs one of the processes given in following.

1. **Naive**: This type of attackers always provides infected files like viruses. Moreover, they give low recommendations about other peers.

2. **Discriminatory**: This type of attackers always provides infected file to a particular group of peers, and provide low recommendation about those peers. Except those peers it behaves as well.

3. **Hypocritical**: This attacker attacks based on time. That is, it gives infected files for a particular time. After that particular time, it becomes as a good peer.

4. **Oscillatory:** This attacker makes high trust value by providing authentic files for a long time. Then for a short time it acts as a naive attacker. After that short time, it behaves as a good peer.

There is another type of attack called pseudospoofers. This type of attackers changes their identity to escape. This process may cause more attacks. The pseudospoofers involves in both service and recommendation based attacks. Anyhow all these attacks are avoided by the self organizing trust method because the self organizing trust method gets recommendations from trusted third party only.

VI. CONCLUSION

The security over peer to peer networks is defined, in which a peer form its trust group by evaluating the trustworthiness. By this a peer can avoid the inauthentic peers from their proximity. The service, reputation and recommendation metrics are used to calculate the trustworthiness of a peer. These metrics are calculated based on past interactions and recommendations. To calculate those values weight, satisfaction and recentness are considered. Recommendations are collected from its trusted third party. By this way the trustworthiness is calculated in better manner.

Various attacks are avoided through this approach because it uses the recommendations and service details from service history to calculate the trustworthiness. This approach can avoid most of the attacks. This security may not provide the solution for all the security problems. But, It is feasible for many applications like file sharing in peer to peer network.

VII. 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] A.B. Can, "Trust and Anonymity in Peer-to-Peer Systems, "PhD thesis, Dept. of Computer Science, Purdue University, 2007.

[3] A.B. Can, Bharat Bhargava "SORT: A Self-Organizing Trust Model for peer-to-peer systems" IEEE transaction on dependable and secure computing, vol-10, January/February 2013.

[4] 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.

[5] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A Survey of Attack and Defense Techniques for Reputation Systems," ACM Computing Surveys, vol. 42, no. 1, pp. 1:1-1:31, 2009.

[6] S. Marsh, "Formalising Trust as a Computational Concept", PhD thesis, Dept. of Math.and Computer Science, University of Stirling, 1994.

[7] 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.

[8] Lin wang "Attacks against peer to peer network and countermeasures" TKK T-110.5290 seminar on network security 2006/2012.

[9] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman,"Reputation Systems," Comm. ACM, vol. 43, no. 12, pp. 45-48,2000.

[10] 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.

[11] L.Xiong, L.Liu "peertrust: Supporting reputation based trust for peer to peer ecommerce communities" IEEE trans. Knowledge and data eng., vol. 16,vol .7,july 2004.

[12] R. Zhou, K. Hwang, and M. Cai, "Gossiptrust for Fast Reputation Aggregation in peer-to-peer networks," IEEE trans.Knowledge and Data Engg., vol. 20, no.9, pp. 1282-1295, sept. 2008.

[13] Y. Zhong, "Formalization of Dynamic Trust and Uncertain Evidence for User Authorization", PhD thesis, Dept. of Computer Science, Purdue University, 2004.