An Unstructured Peer To Peer Networks With Its Trust Management and Its Optimizing Overlay

R.Padmapriya[1], Shanthi.E[2]

[1]*PG Project Student, Dept of ECE, Bannari Amman Institute of Technology, Sathyamangalam, TN.*
[2]*Assistant Professor, Dept of ECE, Bannari Amman Institute of Technology, Sathyamangalam, TN.*

***Abstract*— Protecting the network from malicious attacks is an important yet challenging security issue in mobile ad hoc networks as well as in peer to peer networks. A peer-to-peer (P2P) network is a type of 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 a security over peer to peer system the self-organizing trust model has been proposed. It protects the network by detecting and reacting to the malicious nodes, where local neighboring node collaboratively monitor each other and sustain each other Here the trustworthiness of the peers has been calculated based on past interactions and recommendations. The interactions and recommendations are evaluated based on performance, behavior with neighborhood. By this the good peers were able to form trust relationship in their proximity and avoids the malicious peers.**

Index Terms*—— SORT, Repudiation, Malicious attacks

I. Introduction

Peer-to-peer is “community-oriented" information exchange tools that were popularized when Napster hit the scene and it acts as network storage for web storage model. Napster is used to exchange MP3 music files, it helps users locate information on other user's computers and access it directly and no need of main server on the network.

Information has been widely distributed, rather than it stored on servers. This is not a new concept has been around for some time in collaborative software and Microsoft Windows' peer-to-peer networks. Napster introduces some software that is automatically foe search the index that supports for messaging, mailing service and storage of multimedia purposes.

Drawback of peer to peer network is the security problem for each user has to assign password for connect with the other user and malicious attacks is possible. Peer to peer networks is divided into structured and unstructured peers are free to join in unstructured but in structured it is fixed random network

Anonymous nature of peer-to-peer (P2P) systems exposes them to malicious activity. Building trust relationships among peers can mitigate the attacks of malicious peers. This paper enables a peer to reason about trustworthiness of other peers based on their past interactions, recommendations and reputations. Peers create their own trust network in their proximity by using local information available and do not try to learn global trust information.

II. TRUST SERVICES

Trust services are based on trust, service, and recommendation reputation, Interactions and recommendations are also has been evaluated based on peer to peer performance and its parameters.

Metrics should have precision so peers can be ranked according to trustworthiness. Trust models on P2P systems have extra challenges comparing to e-commerce platforms. Malicious peers have more attack opportunities in P2P trust models due to lack of a central authority.

III. REPUTATIONAND RECOMMENDATION

Reputation is one of the methods for evaluating the trust in peer to peer as well as unstructured network this approach is based on the calculation of recommendations and past interactions with neighbors. Here the sort technique is used for comparing with other techniques

IV. SERVICE TRUST METRIC

It has been used to evaluate the trustworthiness of trusted third party neighbor nodes.

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 as per the satisfaction. The two values competence belief 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 highest trust value is taken as a trusted third party to get recommendations.

A. Reputation trust metric

The reputation trust metric calculates the trustworthiness of a stranger based on past interactions. To calculate the reputation value reputation query has been send to peers. The reputation query collects the recommendations from its trusted third party. And also the maximum number of recommendations collected through reputation query. There is high threshold value has been set for recommendation trust value. It starts to collects recommendations from it 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 maximum size of service history then the trusted third party has high level experience about a stranger.

B. 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 values of recommenders are 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, 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 weight set to be maximum value. The competence and integrity belief also considered to provide more trustworthiness. 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 get service from the stranger. Getting service is done as follow. First the recommendation request has been send to trusted third party. The trusted third party receives a request and sends a recommendation about a stranger. Then the service request has been send to stranger to get the service. Interactions, feedbacks and service trust values are stored in history.

C. Selecting service provider

After calculating the trustworthiness, the peer selects the service provider to get the needed service. While that there may be several service providers. To select one of the service providers some values are considered. First, the peer which had highest service trust value has been selected as service provider. If the peers had equal service trust values, then the peer who had lager history size is selected to be a service provider. If history size is also equal, the peer which had highest 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 peer has been selected randomly as service provider from the list of service provider.

V.ATTACKER BEHAVIOURS

An attacker performs one of the processes given in following.

Ever since Napster that allowed individuals to trade in the music commodity, P2P has been used in many types of applications such as content storage, distributed file sharing etc., Their ability to build an extremely resourceful system by aggregating the resources of a large number of independent nodes enables P2P systems to compete the capabilities of many centralized systems for relatively little cost. P2P systems are believed to remain an important approach and continue to gain popularity and impact in the future due to the anonymity, cost sharing, dynamism and scalability that P2P systems possess.

The main goal of the earlier P2P systems is the capability of aggregating resources, which assumes certain honesty level of peers. However, as P2P systems grow tremendously in size, there will be a considerable number of malicious peers who bring security attacks and threats to the whole network. In a distributed infrastructure without centralized server for authority, providing security mechanism is more complicated than in server-centric solutions, as

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

2. **Discriminatory**: This attacker always provides infected file to particular group of peers and provide low recommendation about those peers. Except those peers it behaves as good.

3. **Hypocritical**: This attacker attack basis on time. That

is, its gives infected files for particular time. After that it becomes a good peer.

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

There is another type of attack called pseudo Spoofers. 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 self organizing trust method because, the self organizing trust method gets recommendations from trusted third party only.

VI. RESULTS AND DISCUSSION

Software used : NS 2.34 (Network Simulator)
Operating system : Fedora

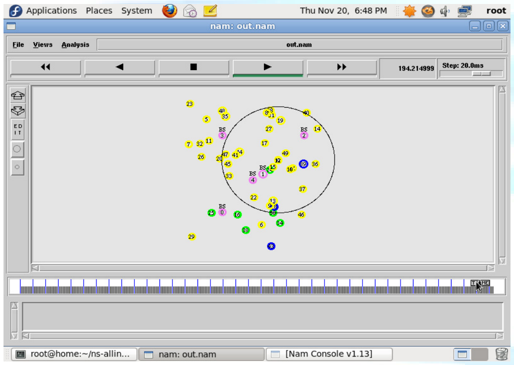


Fig 1: Data is tranfer throught the network

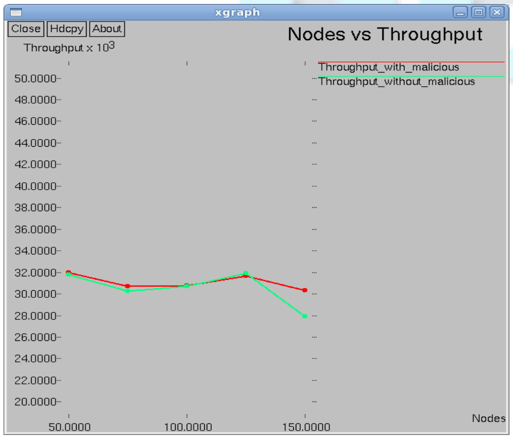


Fig 2: Node vs. Throughput

Fig 3: No of malicious vs Detection_count

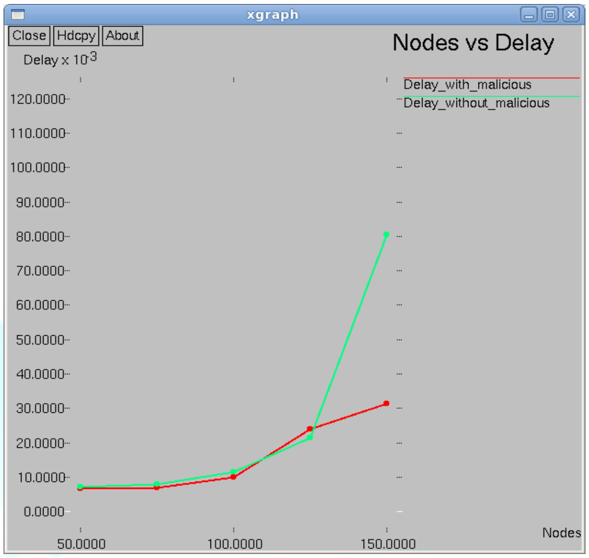
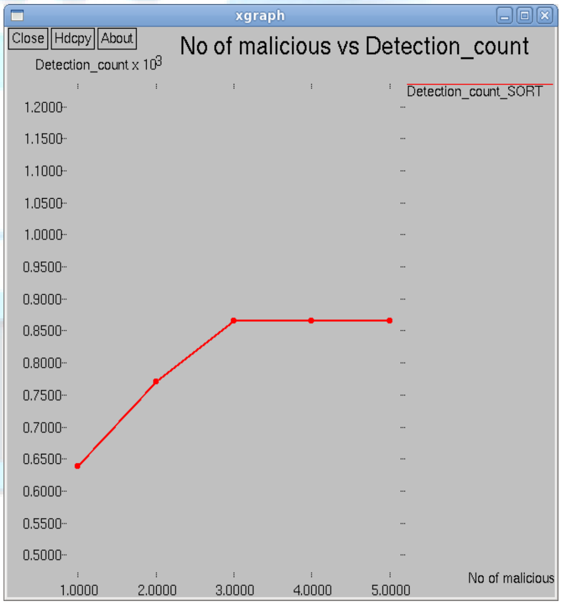


Fig 4: Node vs. Delay



VII. 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. Recommendations provide more confidence about a peer. 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 because the self organizing trust method gets recommendations only from trusted third party. This security may not provide the solution for all the security problems. But, it's feasible for many applications like file sharing in peer to peer network.

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

[8] World Wide Web Conf. (WWW), 2003.
A.A. Selcuk, E. Uzun, and M.R. Pariente, "A Reputation-Based Trust Management SysteforP2PNetworks," Proc. IEEE/ACM Fourth Int'l Symp.Cluster Computing and the Grid (CCGRID), 2004.

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