A Depth Survey on Peer to Peer Systems

G.Selvavinayagam
B.E, M.E, M,Sc (psy),M.B.A, (Phd)
Assistant Professor, Department of Information Technology, SNS college of Technology, Coimbatore.

U.Sahana B.E
Pg scholar, Department of Information Technology,SNS College of Technology, Coimbatore.

ABSTRACT
A trust model for P2P networks is presented, in which a peer can develop a trust network in its proximity. A peer can isolate malicious peers around itself as it develops trust relationships with good peers. Two context of trust, service and recommendation contexts are defined to measure capabilities of peers in providing services and giving recommendations. Interactions and recommendations are considered with satisfaction, weight, and fading effect parameters. A recommendation contains the recommender's own experience, information from its acquaintances, and level of confidence in the recommendation. These parameters provided us a better assessment of trustworthiness. Individual, collaborative, and pseudonym changing attackers are studied in the experiments. Damage of collaboration and pseudo spoofing is dependent to attack behavior. Although recommendations are important in hypocritical and oscillatory attackers, pseudo spoofers, and collaborators, they are less useful in naive and discriminatory attackers.

Keywords
Trust management, Reputation, peer to peer systems, security

1. INTRODUCTION
P2P computing is the sharing of computer resources and services by direct exchange between systems.[1]These resources and services include the exchange of information, processing cycles, cache storage, and disk storage for file.P2P computing takes advantage of existing computing power, computer storage and networking connectivity, allowing users to leverage their collective power to the 'benefit' of all. In peer to peer system Trust metrics defined on service and recommendation trust contexts help a peer to reason more precisely about capabilities of other peers in providing services and giving recommendations. If all peers are behave good, reputation of a peer is proportional to its capabilities such as network bandwidth, average online period and number of shared files. In a malicious network, service and recommendation-based attacks affect the reputation of a peer. Three individual attacker, three collaborator and three pseudo poofer behaviors are studied. SORT mitigates service-based attacks in all scenarios. For individual attackers, hypocritical ones take more time to detect. Identification of collaborators usually takes longer than identification of an individual attacker. Pseudospoofers are more isolated from good peers after every pseudonym change. Since good peers get more acquaintances with time, they do not prefer to interact with strangers and leave pseudospoofers isolated. Two types of collaborators present interesting behavior. Hypocritical collaborators use unfairly high recommendations and attract more good peers at the beginning. They can take advantage of SORT for their attacks. However, good peers eventually identify them and contain their attacks. Discriminatory collaborators have a better reputation than hypocritical collaborators since they do not attack 80% of the peers. However, their service-based attacks are mitigated faster since victims quickly identify them. They gain a highest recommendation trust average and cause the victims to have the lowest average. Thus, they can continue to give misleading recommendations which can be stopped if a trusted third party is used. Defining a context of trust and its related metrics increases a peer's ability to identify and mitigate attacks in the context related tasks. Therefore, various contexts of trust can be defined to enhance security of P2P systems on specific tasks. For example, a peer might use trust metrics to select better peers when routing P2P queries, checking integrity of resources, and protecting privacy of peers.

2. REPUTATION SYSTEM USING SELF CERTIFIED CRYPTOGRAPHIC EXCHANGES
It presents [2] Enabling peers to develop trust and reputation among themselves is important in a peer-to-peer system where resources (either computational, or files) of different quality are offered. It will become increasingly important in systems for peer-to-peer computation, where trust and reputation mechanisms can provide a way for protection of unreliable, buggy, infected or malicious peers. The authenticity of the reputation information is the basis of assuring the normal running of Trust Management System (TMS). After analyzing the security risks existing in the current TMS, this paper proposes a secure and effective reputation based distributed trust management model which uses Self-certification, an identity management mechanism, and a cryptographic protocol that facilitates generation of secure reputation data in a P2P network, in order to expedite detection of rogues. This paper discusses the reputations managed in the network, the corresponding reputation information given to peers and identification of malicious nodes. Once the malicious nodes are identified based on their download's ratios and activities in the network, instead of ostracizing the selfish peer completely, the proposed system provides services at lower bandwidth and its presence can boost up network performance. The proposed model is more secure, robust and effective on attacks from various malicious peers, including peers with malicious behaviors and peers with security threats, and shows more improvements in the security feature of the trust management.

3. THE EIGER TRUST ALGORITHM IN P2P SYSTEM
It presented [3] a method to minimize the impact of malicious peers on the performance of a P2P system. The system computes a global trust value for a peer by calculating the left principal eigenvector of a matrix of normalized local trust values, thus taking into consideration the entire system's history with each single peer. We also show how to carry out the computations in a scalable and distributed manner. In P2P simulations, using these trust values to bias download has shown to reduce the number of inauthentic files on the network under a variety of threat scenarios. Furthermore,

rewarding highly reputable peers with better quality of service incents non-malicious peers to share more files and to self-police their own file repository for inauthentic files.

4. TRUST MANAGEMENT SYSTEM FOR P2P NETWORKS

It presents [4] a potential improvement on the basic protocol may be realized by preserving the hashes of the malicious files downloaded. These hashes can later be used to send a warning to the querying peer when a relevant query is received. This protocol can be enhanced to include this feature with the following modifications: The warning messages received in a query are grouped along with the normal responses according to their file hash value. If selected into the top θ T for trust evaluation, a warning message's trust and distrust ratings are reversed in the trust score calculation, contributing a significant distrust factor to the average. The limitations of our protocol must also be noted. Being a reputation-based protocol, our system in the end relies on the judgment of its users. Therefore, it can be effective only against attacks that are discernible by the user. Nevertheless, many attacks in P2P systems fall into this category, such as the common decoy files attacks.

5. GOSSIP TRUST FOR FAST REPUTATION AGGREGATION

In P2P network, global reputation aggregation [5] is quite expensive when the network grows to reach millions of nodes. To our best knowledge, Gossip Trust offers the very first attempt to extend the gossip protocol for reputation aggregation in P2P networks without any structured overlay support.

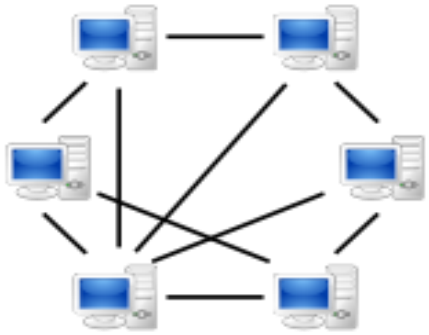

Fig 1: General Structure of Peer to Peer networks

6. GNUTELLA NETWORK

It paper [6] verified the theoretical conclusion by measuring the traffic at multiple, randomly chosen, nodes. As a result, the total Gnutella generated traffic is proportional to the number of connections in the network. Based on our measurements we estimate the total traffic (excluding file transfers) for a large Gnutella network as 1 Gbps: 170,000 connections for 50,000-nodes Gnutella network times 6 Kbps per connection, or about 330 TB/month. To put this traffic volume into perspective we note that it amounts to about 1.7% of total traffic in US Internet backbones in December 2000 . We infer that the volume of generated traffic is an important obstacle for further growth and that efficient use of underlying network infrastructure is crucial for better scaling and wider deployment. One interesting feature of the network is that, over a seven-month period, with the network scaling up almost two orders of magnitude, the average number of connections per node remained constant. Assuming this invariant holds, it is possible to estimate the generated traffic for larger networks and find scalability limits based on available bandwidth.

7. FORMALISING TRUST

It presents [7] the problem that of subconscious trust, is more difficult to address. The problem of information overload is a real one, and agents have to be shielded from it. Again, if they consider in a trusting fashion every aspect of their environment, local or displaced, then they will have very little time, if any, to carry out the tasks which may have been assigned to them. A simple answer is to allow an implicit trust in certain things, much as is done now in DAI with everything. Thus, things like the perceived, or expected, behaviour of the environment would be implicitly trusted — agents would expect that, say, walls don't move, or that certain physical laws will always be obeyed. Because the trust is implicit, these things do not have to be considered ordinarily, and thus the agent need have no explicit knowledge of them. Just as with humans, when such implicit trust is abused, the agent is subject to a shock For example, when we go out, we trust that we will get to where we are going without injury. When this does not happen, and we are in an accident, the resultant shock is considerable — this applies whether we are hurt or not, since our trust in the proper workings of things is found to be misplaced, and it is so implicit as to be almost sacrosanct. This raises important questions for artificial agents. Whilst they should not be 'bogged down' with unnecessary considerations of the environment at large, they should be aware often possible problems and pitfalls in the environment. With an implicit trust, acknowledging the potential problems, but accepting (trusting) their infrequency, we can allow agents to exist in harmony in their environment and each other, accepting unexpected events with sensible behavior.

8. CONCLUSION

P2P system is a promising paradigm for services operating at the edges of the network. Decentralized P2P applications offer big cost/time savings.P2P networks currently scale in small to mid-size networks.many open issues in P2P security, resource and performance Management. e.g.: metrics, reliability, and scalability, multimedia. Their impact on security will depend on the adoption of peer-to-peer networks in standard computing environments. If systems use peer-to-peer networks as email is used today, then they will be significant methods of delivery of malicious code. The use of two-way network communication also exposes the system to potential remote control. More importantly, the usage of a peer-to-peer network creates a hole in a firewall and can lead to the exporting of private and confidential information. Therefore, administrators should begin analyzing their networks for peer-to-peer network usage and configure firewalls and systems accordingly to limit or prevent their usage.

9. REFERENCES

[1] Ahmet Burak Can and Bharat Bhargava ."SORT: A Self ORganizing Trust Model for Peer-to-Peer Systems", IEEE Trans. Dependable And Secure Computing, VOL. 10, NO.1.JANUARY/FEBRUARY 2013.

[2] M. Srikanth and K.B. Madhuri, **"**Secure and Effective P2P Reputation System using Trust Management and Self Certified Cryptographic Exchanges", IJCSI

International Journal of Computer Science Issues, Vol. 10, Issue 2, No 2, March 2013

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

[4] 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.

[5] R. Zhou, K. Hwang, and M. Cai, "Gossip trust for Fast Reputation Aggregation in Peer-to-Peer Networks," IEEE Trans. Knowledge and Data Eng., vol. 20, no. 9, pp. 1282-1295, Sept. 2008.

[6] M. Ripeanu, I. Foster, and A. Iamnitchi, "Mapping the Gnutella Network: Properties of Large-Scale Peer-to-Peer Systems and Implications for System Design," IEEE Internet Computing, vol. 6, no. 1, pp. 50-57, Jan. 2002.

[7] S. Marsh, "Formalising Trust as a Computational Concept," PhD thesis, Dept. of Math. And Computer Science, Univ. of Stirling, 1994.

.