Secure Communication in Unstructured P2P Networks based on Reputation Management and Self Certification

C.V. Arulkumar
PG Scholar
Dept. of Information Technology,
SNS College of Technology

K. Jeyakumar
PG Scholar
Dept. of Information Technology,
SNS College of Technology

M. Malarmathi
Assistant Professor
Dept. of Information Technology,
SNS College of Technology

T. Shanmugapriya
Assistant Professor
Dept. of Information Technology,
SNS College of Technology

ABSTRACT
In unstructured P2P networks there is a possible of malicious codes and false transactions. It generates the false identities in order to perform false transactions with other identities. The proposed method uses the concept of DHT and reputation management which provides efficient file searching. The self certification (RSA ALGORITHM and MD5) is used for ensuring secure and timely availability of the reputation data of a peer to other peers. The reputations of the peers are used to determine whether a peer is a malicious peer or a good peer. Once the malicious peer is detected the transaction is aborted. The reputation of a given peer is attached to its identity. The identity certificates are generated using self-certification, and all peers maintains their own (and hence trusted) certificate authority which issues the identity certificate(s) and digital signature to the peer.

General Terms
Unstructured P2P Networks.

Keywords
RSA, MD5, Reputation Management.

1. INTRODUCTION
A peer-to-peer commonly abbreviated to P2P. PEER-TO-PEER (P2P) networks are self configuring networks with minimal or no central control. Peer-to-Peer Systems are divided in to two types. They are Structured P2P systems and Unstructured P2P systems.

In structured peer-to-peer networks, connections are done based on some routing algorithms. They typically use distributed hash table-based (DHT) for indexing. Unstructured peer-to-peer networks do not have any algorithm for organization or optimization of network connections. An unstructured P2P network is formed when the overlay links are established arbitrarily. The new peers can be constructed by copying the existing links of other nodes, and then the peer builds its own links over time.

P2P networks are more vulnerable. It may consist of malicious code, viruses, worms, and Trojans than the client-server networks. The traditional mechanisms for generating trust and protecting client-server networks cannot be used for pure P2P networks. The major disadvantage of the centralized approach is, if the central authority turns malicious, the network will become vulnerable and the transactions are false. Each and every peer is associated with Certification Authority (CA).To perform the false transaction the malicious peer might start multiple CA's and it generates multiple groups of identities. In order to counter a malicious peer having multiple CA's, the peers are divided into groups based on different criteria such that a peer cannot become a part of multiple groups. Each peer obtains its group certificate from the appropriate authority and attaches it to its CA. The certificate of a group authority is publicly accessible by any node inside or outside the group. The peer sends its blinded signature (or) credentials to the group authority and the authority verifies the credentials and signs the group certificate. The authority remains stateless, i.e., it does not maintain any information to correlate a certificate with the peer.

To overcome this, self certification and Reputation Management is used. Here the reputation is done by using Distributed Hash Table (DHT).The reputations of the peers are used to determine whether a peer is a malicious peer or a good peer. All peers in the P2P network are identified by identity certificates .The reputation of a given peer is attached to its identity. The identity certificates are generated using self-certification, and all peers maintain their own (and hence trusted) certificate authority which issues the identity certificate(s) to the peer. This information's are stored locally.

2. RELATED WORKS
In [1] the unstructured P2P net- works, peers willingness to share the content they have and forward the queries plays an important role during the content search process. Using these objective criteria past peer behaviors is tracked. Reliable peer reputations could be used in a variety of ways. They can help well-reputed peers and other peers with good reputations and hence help them in making decisions about who to serve content to and who to request content from. During the bootstrapping process for joining the P2P network, peers can potentially use reputations to decide who to directly connect to in the overlay topology. Since each peer stores its own reputation locally, for reputations to be reliable and elective, they have to be updated and stored securely to prevent malicious peers from the reputation system.

In [2] the unstructured peer to peer systems a completely decentralized, self-maintaining, and sufficiently secure peer identification service that facilitates the consistent mapping of globally unique peer identifications onto dynamic IP addresses. Peers generate universally unique identifications locally and store them along with their public key, their current IP address .If a certain quorum of identical answers is returned the mapping is considered trustworthy and the peer is contacted. If contacting the peer fails then the peer is either online or has changed its IP address (this cannot be distinguished). The requester can now either assume that the

peer is online and give up or, in the latter case, submit a new query to determine the new IP address. If contacting the peer succeeds in either case, its public key is used to determine whether the contacted peer really is the one identified by the mapping or whether a different peer reuses the address or a malicious peer tries an impersonation attack.

In [3] Digital signatures are used in message transmission to verify the identity of the sender and ensure that a message has not been modified after signing. RSA algorithm is extensively used in the popular implementations of Public Key Infrastructures. The performance of the two public key cryptosystem (RSA and MD5) and the new algorithm has been implemented and compared. The results obtained show that signing and verification operations are faster in the case of using new algorithm than in the case of RSA and MD5. Also it can forbid any one from reaching the sender's message because with the new algorithm an intruder cannot pose the message sent since the sender's private key is unknown for him. On the receiver part, the message is verified by using sender's public key and his private key to decrypt the message successfully.

An effective reputation management system using peer reputation and file reputation together in DHT-based structured P2P networks. Reputation system works better in preventing untrustworthy files from spreading than existing systems even in cases of allowing malicious peers to change their identities.

In [10] the unstructured peer to peer, network uses Naïve Bayes Algorithm. It is based on Bayesian statistics with strong independence assumptions.

Prob (B given A) = Prob (A and B) / Prob A

In simple terms, a naive Bayes Classifier assumes that the presence (or absence) of a particular feature of a class is unrelated to the presence (or absence) of any other feature.Bayes classifiers can be trained very efficiently in a supervised learning setting.

3. PROPOSED METHODOLOGY

Figure 1 illustrates the proposed technique. There are three major steps in the proposed method. They are,

3.1 Construction of unstructured peer to peer networks
3.2 Construction of Distributed Hash Table
3.3 Implementation of Reputation Management
3.4 Implementation of Self Certification (RSA) and Digital Signature (MD5) for Secure Communication

PEER-TO-PEER (P2P) networks are self-configuring networks with minimal or no central control. P2P networks are more vulnerable to dissemination of malicious or spurious content, malicious code, viruses, worms, and Trojans than the traditional client-server networks, due to their unregulated and unmanaged nature.

In unstructured peer to peer, information about one peer is unknown to the other. (i.e.) to enable communication between the peers, the peers in the network should know some information about the other peer in the network.

The proposed system uses the distributed hash table where each and every peer has the separate hash table. The information stored in the hash table is based on Reputation management (tracking users past activity).It helps to perform the file searching operation efficiently.

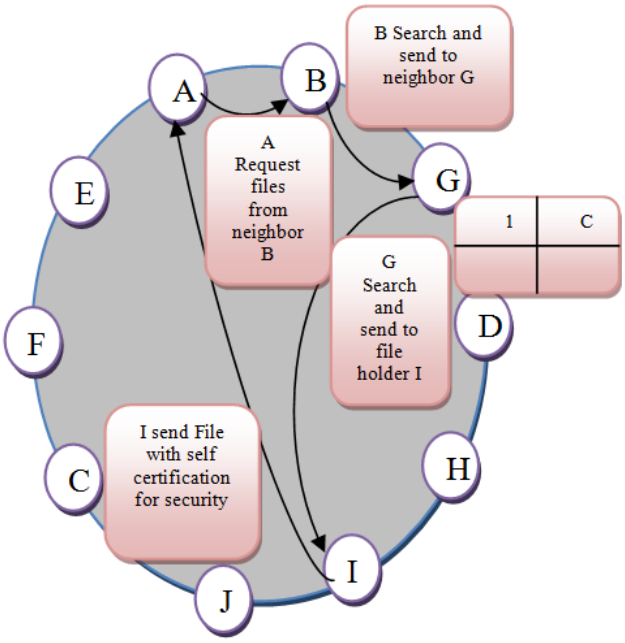

Figure 1: An Overview of communication in peer to peer Unstructured network using self certification and reputation management

The reputations of the peers are used to determine whether a peer is a malicious peer or a good peer. Once detected, the malicious peers are ostracized from the network as the good peers do not perform any transactions with the malicious peers. Expulsion of malicious peers from the network significantly reduces the volume of malicious activities.

Each and every peer has the unique identity, based on this, the peer is identified and the transaction is begined. The certification is attached with identity of the peer. The certification uses the concept of RSA and DSS.where the algorithm generates the private key and public key, these identities are attached with reputation of the given peer. The sender sends the information which is associated with its private key and signature, the receiver encrypts using its public key, these in formations are updated periodically in Distributed Hash Table. DHT allows to search for specific content identified by a hash key and to eventually perform Boolean operations upon the results of searches that used different keys .It provides considerable fast search times in respect to unstructured solutions. Using the index value the files are stored and retrieved. If malicious peer performs false transaction means it can be identified easily and the transaction is aborted.

For example the system consist of N peers (A to E) where the file searching is done randomly .Initially its sends the request with its identity to nearest peer, it checks the file in DHT, if it has the file, the peer sends those information with self certification. These operations are done based on reputation management. The reputation of a given peer is attached to its identity. The identity certificates are generated using self-certification, and all peers maintain their own (and hence trusted) certificate authority which issues the identity certificate(s) to the peer. A self-certification-based identity system protected by cryptographically blind identity mechanisms. A light weight and simple reputation model. An attack resistant cryptographic protocol for generation of authentic global reputation information of a peer's.DSS provide authentication and authorization.

4. IMPLEMENTATION

The proposed method is implemented using Java. The proposed method is compared with file searching operation with existing system and how malicious peers are identified using RSA and MD5.

A system that collects, distributes and aggregates the feed back about consumers past behavior. The server provides pseudonyms (identities) to users and inducts them into the system Based on the sever id the client starts the file searching If the file found it retrieves and stores the file to its hash table.

The peer generates the public key and private key using RSA algorithm. The sender encrypts the information or file using its own private key and receiver's public key. Similarly the receiver decrypts the file using its private key and sender's public key. The content Auditing is done using Naive Bayes algorithmMD5 is mainly used to provide Digital Signature. The large messages are compressed before the encryption.

	Peer IP	File Name	Reputation Management	Content Auditing
1	192.168.0.1	File1.doc	Retrieved by Peer3	Content editing
2	192.168.0.2	File2.txt	Retrieved by Peer1	Content deletion
3	192.168.0.3	File2.java		

Figure 2: Distributed hash table

The comparison graph shows (fig 3) the efficient file searching method in unstructured peer to peer system with Reputation Management and with out Reputation Management and (fig 4) shows that our method significantly reduces the number of malicious peer accessed during communication.

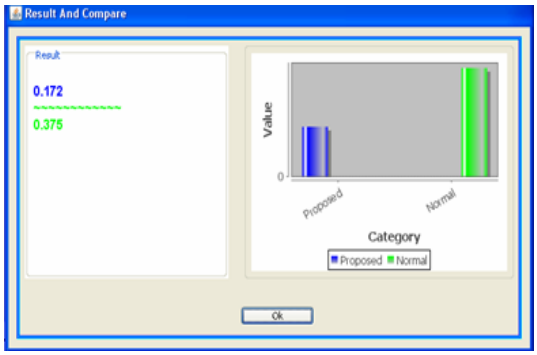

Figure 3: Comparision of proposed method with existing technique(file searching)

Figure 4: Comparision of proposed method with existing method

5. CONCLUSION

The file searching is efficient and easy in unstructured peer to peer networks based on Reputation Management . During the tranfer of files there is possible of distribution of viruses,worms and trojan horses and malicious peers to over come this the self certification (RSA and DSS) is used,it provides authentication and authorization. It easily finds the malicious peers and aborts the transaction.Therefore the proposed method provides the efficient and secure communication between the peers.

6. ACKNOWLEDGEMENTS

The authors would like to thank Director cum secretary, Correspondent and Principal of SNS College of Technology, Coimbatore for their motivation and constant encouragement. The authors would like to thank the faculty Members of Department of Information Technology for the critical review of the manuscript and for their valuable input and fruitful discussions. Also we take privilege in extending gratitude to their family members and friends who rendered their support throughout this research work.

7. REFERENCES

[1] M. Gupta, P. Judge, and M. Ammar, "A Reputation System for Peer-to-Peer Networks," Proc. 13th Int'l Workshop Network and Operating Systems Support for Digital Audio and Video (NOSSDAV),2003.

[2] M. Hauswirth, A. Datta, and K. Aberer, "Handling Identity in Peer-to-Peer Systems," Proc. Sixth Int'l Workshop Mobility in Databases and Distributed Systems,Sept. 2003.

[3] "An efficient signature system using optimized RSA Algorithm" Eng. Rania salah el-sayed *,prof. Moustafa abd el-aziem**, dr . Mohammad ali gomaa

[4] P. Resnick, R. Zeckhauser, and E. Friedman, "Reputation Systems," Comm. ACM, vol. 43, pp. 45-48, Dec. 2000.

[5] L. Xiong and L. Liu, "PeerTrust: Supporting Reputation-Based Trust in Peer-to-Peer Communities," IEEE Trans. Knowledge and Data Eng., vol. 16, no. 7, pp. 843-857, July 2004.

[6] B.C. Ooi, C.Y. Kiau, and K. Tan, "Managing Trust in Peer-to-Peer Systems Using Reputation-Based Techniques," Proc. Fourth Int'l Conf. Web Age Information Management, Aug. 2003.

[7] L. Liu, S. Zhang, K.D. Ryu, and P. Dasgupta, "R-Chain: A Self- Maintained Reputation Management System in p2p Networks," Proc. 17th Int'l Conf. Parallel and Distributed Computing Systems (PDCS), Nov. 2004.

[8] Z. Xu, Y. He, and L. Deng, "A Multilevel Reputation System for Peer-to-Peer Networks," Proc. Sixth Int'l Conf. Grid and Cooperative Computing (GCC '07), pp. 67-74, 2007.

[9] S.D. Kamvar, M.T. Schlosser, and H. Garcia-Molina, "The Eigentrust Algorithm for Reputation Management in P2P Networks," Proc. 12th Int'l World Wide Web Conf., pp. 640-651, 2003.

[10] E. Damiani, D. di Vimercati, S. Paraboschi, P. Samarati, and F. Violante, "A Reputation-Based Approach for Choosing Reliable Resources in Peer-to-Peer Networks," Proc. Conf. Computer and Comm. Security (CCS '02). pp. 2007