INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

Securing Information In P2P Reputation Management Using Distributed Identities And Decentralized Recommendation Chains

G. Usha Rani
Department of CSE, Sri Sivani College of Engineering, Chilakapalem, A.P., India
M. V. A. Naidu
Associate Professor, Department of CSE, Sri Sivani College of Engineering, Chilakapalem, A.P., India

Abstract:
The motivation behind this paper is to protect the P2P network without using any central component. In this paper we present a cryptographic protocol for ensuring secure and timely availability of the reputation data of a peer extremely at low cost and develop a queuing model to evaluate the time required at each peer to serve its replication requests. The open, sharing and anonymous nature of peer to peer (p2p) network has offered opportunities and threats for the development of distributed computing technology. One way to minimize the threats is to establish the reputation based global trust model. Reputation based p2p systems have the property to detect malicious peers using the reputation of the peers providing the resources. A two-party cryptographic protocol not only protects the reputation information from its owner, but also provides secure exchange of reputation information between the two peers participating in a transaction.

Key words: *Peer to Peer, Cryptography, Distributed, Reputation*

1.Introduction

PEER-TO-PEER (P2P) networks are self-configuring networks with no central control. P2P network increases system robustness by enabling the receiver to obtain data from multiple sources without relying on centralized servers. Peer-to-peer (P2P) computing or networking is a distributed application architecture that partitions tasks or workloads among peers. Information security applies to all aspects of safeguarding (or) protecting information or data. It is necessary to protect the information systems against unauthorized access or modification such as deletion or addition of some part into the information in transit. It is also essential to protect the information system against the denial of service to authorized users or the specification of service to unauthorized users, including those evaluations necessary to detect report and counter such threats.

2.The Main Articles Of This Paper Are

A self-certification-based identity system safeguarded by cryptographically blind identity mechanisms.

- A lightweight and simple reputation model.
- An attack resistant cryptography protocol for generation of veritable global reputation information of a peer.

3.Literature Survey

This section briefly reviews some of the existing P2P reputation systems, focusing particularly on the storage and integrity issues. We start by giving an overview of the reputation systems.

P2P file sharing systems can be centralized, completely decentralized or partially decentralized systems. Centralized P2P file sharing systems use a centralized directory for enquiring files, while downloading a file is achieved directly between peers. In completely decentralized P2P systems, all peers have equal contributions and responsibilities. Moderately decentralized P2P systems occupy the middle ground between centralized and completely decentralized systems.

4.Reputation Models

Resnick et al.defines the reputation system as “a system that assembles, administers, and aggregates feedback about consumers ancient behaviour.”Pseudo spoofing is the use of the numerous pseudonyms in a System by the same real-life entity. The pitfall is that any entity can discard a handle or a sobriquet with which a bad reputation is incorporated and join the system as a new user, under a new sobriquet. This can possibly nullify the usefulness of a reputation system, which allocates reputations to handle.

PeerTrust allocates the reputation information to a certain node on the network for storage, by applying hash functions. Any peer looking for the reputation of another peer uses the search mechanism of the fundamental network to search for the information.

The authors of PeerTrust argue that trust models based completely on feedback from other peers in the community are ineffective and inaccurate. The authors recommend the "degree of satisfaction" of the peer from antecedent transactions and the number of transactions a peer performs in the system should be justified prior to calculating the reputation of the recommended peer.

Abdul-Rahman and Hailes have proposed another trust model with corresponding criterion. They argue that Bayesian probability may not be the best criterion for representing degree of trust, because probability is constitutionally transitive while trust is not. In addition, the reporters provide methods for integrating recommendations and use the context of exhortations and weights to evaluate the reputations from exhortations.

4.1.Reputation Infrastructure

P2PRep developed by the security group of University` di Milano is a reputation-based system implemented on top of Gnutella. In P2PRep, a requester finds a list of potential providers, polls the current neighbours of the preliminary providers and takes votes from them on the goodness of the provider. P2PRep is a highly communication concentrated system because peers do not store state (reputation info) of other peers. P2PRep makes an inherent assumption that the neighbours of a node will have the eminence information of the node.

Zhou et al. Propose a bloom filter approach for fast reputation aggregation. They use gossip algorithms to circulate reputation information in a network. The Gossip-based protocol is delineating to consume dynamic peer joining and departure, as well as to avoid possible peer collaborations.

4.2.Client-Server (Centralized) Reputation Systems

In the reputation systems depend on the client-server model, the server provides pseudonyms (identities) to users and admit them into the system. Once register into the system, a requester (client) selects a service provider (server) (from other users) for a given service, depend on the reputation of the service provider. The requester then acquires a service from the provider. Once the transaction is finished, the requester gives advice to the server depends upon its gratification level from the transaction.

Xu et al. Have proposed a multilevel reputation scheme which is also vulnerable on a central reputation computation engine. The authors attack the hard problem of the burden estimate in a p2p system since peers with good reputation get encumbered by prerequisites. Their strategy allocates trust values to contents and reputation values to peers and authorizes peers at a certain reputation value to the only approaches content at same or less trust value thereby diminishing the load balancing complication in P2P networks.

5.System Architecture

A peer-to-peer (P2P) network is a type of decentralized and distributed network architecture in which individual nodes in the network (called "peers") act as both suppliers and consumers of resources, in contrast to the centralized client–server model where client nodes request access to resources provided by central servers.

In a peer-to-peer network, tasks (such as searching for files or streaming audio/video) are shared amongst multiple interconnected peers who each make a portion of their resources (such as processing power, disk storage or network bandwidth) directly available to other network participants, without the need for centralized coordination by servers.

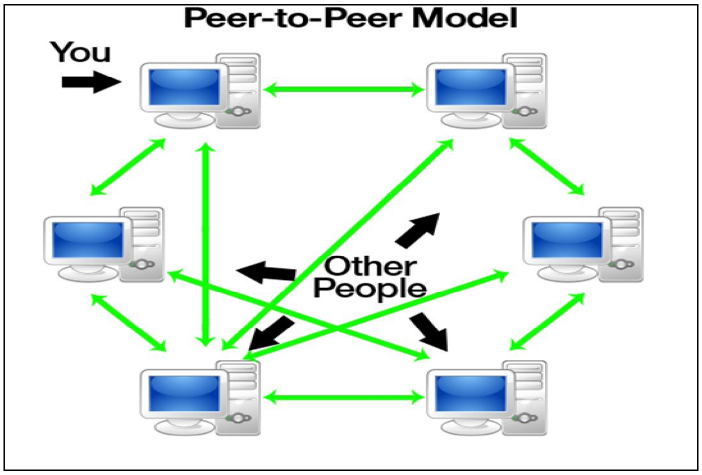


Figure 1

5.1.Existing System

The peers in the P2P network have to be discouraged from leeching on the network. It has been shown that a system where peers work only for selfish interests while breaking the rules spoils to death. Policing these networks is extremely difficult due to the decentralized and ad hoc nature of these networks. Besides, P2P networks, similar to the Internet, are physically expand over geographic boundaries and hence are subject to variable laws.

The traditional mechanisms for generating trust and protecting client-server networks cannot be used for pure1 P2P networks. This is because the trusted central sovereignty used in the traditional client-server networks is absent in P2P networks. Introduction of a central trusted sovereignty like a Certificate Authority (CA) can reduce the difficulty of securing P2P networks. The major drawback of the centralized approach is, if the central authority turns harmful, the network will become unprotected. In the absence of any central authority, warehouse, or global information, there is no silver bullet for protecting P2P networks.

5.2.Proposed System

In this paper, we explore Reputation Systems for P2P networks a more ambitious approach to protect the P2P network without using any central component, and thereby harnessing the full advantages of the P2P network. The eminences of the peers are used to determine whether a peer is a malicious peer or a good peer. Once detected, the malicious peers are repudiated from the network as the good peers do not perform any transactions with the malicious peers. Ejection of malicious peers from the network significantly reduces the volume of malicious activities. All peers in the P2P network are recognized by identity certificates (aka identity). The eminence of a given peer is attached to its identity. The identity certificates are produced using self-certification, and all peers maintain their own (and hence trusted) certificate authority which issues the identity certificate(s) to the peer. Each peer owns the eminence information pertaining to all its past transactions2 with other peers in the network, and reserves it locally. A two-party cryptographic protocol not only protects the reputation information from its owner, but also enables secure exchange of reputation information between the two peers participating in a transaction.

6.Implementation

In this paper, we consider seven modules.

- Login Module
- Active Node in Dynamic root
- Group Controller
- Trusted Group Members
- Data Transfer
- Find Group Key
- Block Untrusted Users

Login Module

6.1.Authentication Checking

This module examines whether the user is authenticated or not if the user is authenticated then they have the permission to process further transactions otherwise they cannot access any transaction in this system.

6.2.Registration Process

If the new user to this system first they must registered in the register module after they have continue to process in the system. Through the registration the user must enter the valid information for create new user name and password if only valid user. Once user registered after they have permitted user of this system.

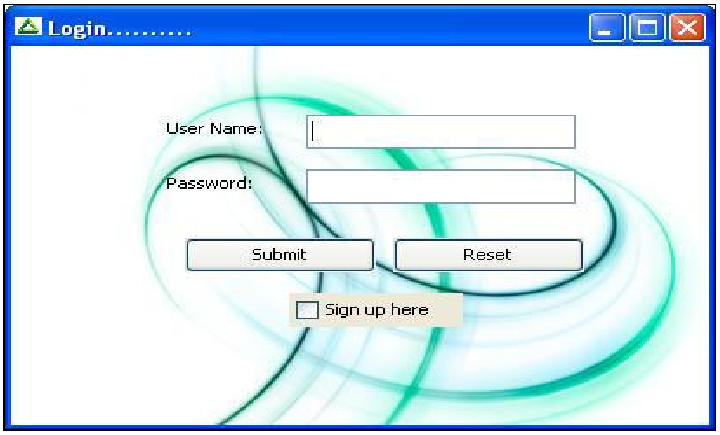


Figure 2

6.2.1.Active Node In Dynamic Route

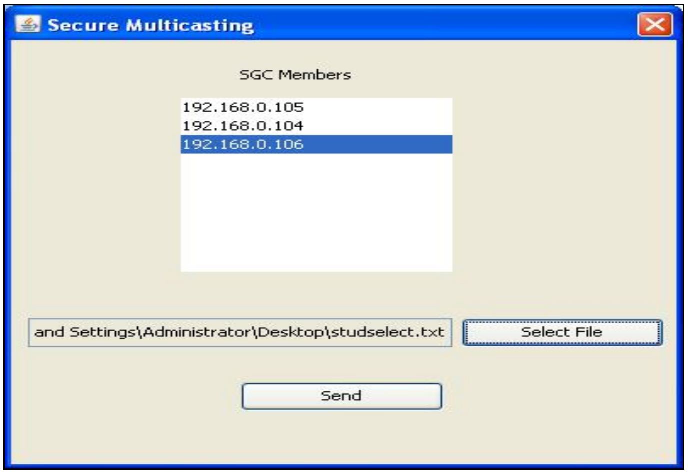
In our communication group have number of client nodes are interconnected in the server. Each group has the distinct group key for communication in the group. When a new member enters or leaves the communication group, only it's indicating for local subgroup. The each group has distinct group key for communication in between who are in the communication group in that time.

6.2.2.Group Controller

Two types of secrecy are provided by this module they are forward and backward secrecy .the forward secrecy is used to prevent a leaving user or expelled group member to continue accessing the group communication .the backward secrecy is used to prevent a new member from decoding the messages exchanged before it joined the group.

6.2.3.Trust Group Members

Our protocol directly addresses the problem of reducing the overload of the group controller. We distribute the multicast communication group into regional subgroups. Each subgroup is singly managed by a subgroup controller (SGC) like a separate multicast group with its own subgroup key. Thus, when a member enters or leaves the communication group, it enters or leaves only its local subgroup. As a result, individual the local subgroup communication key needs to be refreshed and the scalability problem is greatly mitigated.



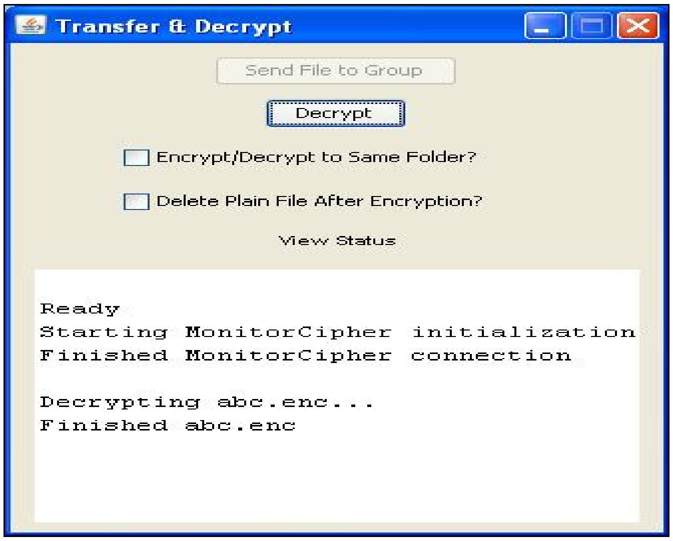
192.168.0.105
192.168.0.104
192.168.0.106

and Settings\Administrator\Desktop\studselect.txt

Figure 3

6.2.4.Data Transfer

In our multicast communication group mainly focus on enabling the data transfer among the server and multiple clients in the network communication..


Transfer & Decrypt
Send File to Group
Decrypt
□ Encrypt/Decrypt to Same Folder?
□ Delete Plain File After Encryption?
View Status

```
Ready
Starting MonitorCipher initialization
Finished MonitorCipher connection

Decrypting abc.enc...
Finished abc.enc
```

Figure 4

6.2.5.Find Group Key

When a new member enters in the communication group then we create a new sub group key for only for its local group as well as existing member leaves from the communication group after that they don’t want to access the local sub group so it need to be refreshed.

6.2.6.Block Untrusted User

Trusted users are formed a group. If a new member request to enter in group, the IP Address will be approved. IP address will be approve with the help of subnet masking, acting as the Class A, Class B, Class C segment of the IP address. If the IP is not suited with the trusted group then it will not be allowed to enter into the trusted group.

7.Conclusion

Peer-to-Peer networks have previously assumed a fail-stop model for nodes; any node accessible in the network was assumed to correctly follow the protocol. However, if nodes are malicious and conspire with each other, it is possible for a small number of nodes to compromise the overlay and the applications built upon it. This paper has presented the design and analysis of techniques for secure node joining, routing table service, and message forwarding in structured P2P networks. These techniques provide secure routing, which can be combined with existing techniques to construct applications that are robust in the presence of malicious participants. Future work Scalability is important for any system; various combinations of this procedure may be used for achieving better result. The accuracy of the detecting may be improved by preprocess the data before analysis. So in this way there is possibility to the future enhancements.

8.References

1. H. Garrett, “Tragedy of Commons,” Science, vol. 162, pp. 1243-1248, 1968.
2. I. Stoica, R. Morris, D. Liben-Nowell, D. Karger, M.F. Kaashoek, F.Dabek, and H. Balakrishnan, “Chord: A Scalable Peer-to-Peer Lookup Service for Internet Applications,” Proc. ACM SIGCOMM, pp. 149-160, Aug. 2002.
3. S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Schenker,“A Scalable Content-Addressable Network,” SIGCOMM ComputerComm.. Rev., vol. 31, no. 4, pp. 161-172, 2001.
4. A. Rowstron and P. Druschel, “Pastry: Scalable, Decentralized Object Location, and Routing for Large-Scale Peer-to-Peer Systems,” Proc. IFIP/ACM Int’l Conf. Distributed Systems Platforms (Middleware), pp. 329-350, Nov. 2001.
5. G. Networks, “Groove Networks,” http://www.groove.net/products/workspace/securitypdf.gtml, 2009.
6. R.L. Rivest and B. Lampson, “SDSI: A Simple Distributed Security Infrastructure,” Proc. Crypto ’96, pp. 104-109, Aug. 1996.
7. N. Li and J.C. Mitchell, “RT: A Role-Based Trust-Management Framework,” Proc. Third DARPA Information Survivability Conf. and Exposition (DISCEX III), Apr. 2003.
8. D. Ferraiolo and R. Kuhn, “Role-Based Access Controls,” Proc. 15th Nat’l Computer Security Conf., May 1992.
9. D. Chaum, “Blind Signatures for Untraceable Payments,” Proc.Advances in Cryptology (Crypto ’82), 1983.
10. L. Zhou, F. Schneider, and R. Renesse, “COCA: A Secure Distributed Online Certification Authority,” ACM Trans. Computer Systems, vol. 20, no. 4, pp. 329-368, Nov. 2002.
11. M. Chen and J.P. Singh, “Computing and Using Reputations for Internet ratings,” Proc. Third ACM Conf. Electronic Commerce, pp. 154-162, 2001.
12. P. Resnick, R. Zeckhauser, and E. Friedman, “Reputation Systems,” Comm. ACM, vol. 43, pp. 45-48, Dec. 2000.
13. E. Friedman and P. Resnick, “The Social Cost of Cheap Pseudonyms,” J. Economics and Management Strategy, vol. 10, no. 2, pp. 173-199, 2001.
14. 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.
15. A. Abdul-Rahman and S. Hailes, “Supporting Trust in Virtual Communities,” Proc. Hawaii Int’l Conf. System Sciences, Jan. 2000.
16. K. Aberer and Z. Despotovic, “Managing Trust in a Peer-2-Peer Information System,” Proc. 10th Int’l Conf. Information and Knowledge Management (CIKM ’01), pp. 310-317, Nov. 2001.
17. A.I. Schein, A. Popescul, L.H. Ungar, and D.M. Pennock, “Methods and Metrics for Cold-Start Recommendations,” Proc. 25th Ann. Int’l ACM SIGIR Conf. Research and Development in Information Retrieval, pp. 253-260, 2002.
18. C. Dellarocas, “Immunizing Online Reputation Reporting Systems against Unfair Ratings and Discriminatory Behavior,” Proc. ACM Conf. Electronic Commerce, pp. 150-157, Oct. 2000.
19. C. Dellarocas, Building Trust On-Line: The Design of Reliable Reputation Mechanism for Online Trading Communities. MIT Sloan School of Management, 2001.
20. E. Damiani, S.D.C. di Vimercati, S. Paraboschi, and P. Samarati, “Managing and Sharing Servents’ Reputations in p2p Systems,”IEEE Trans. Knowledge and Data Eng., vol. 15, no. 4, pp. 840-854, July 2003.
21. 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.

22. L. Liu, S. Zhang, K.D. Ryu, and P. Dasgupta, “R-Chain: A Self- Maintained Reputation anagement System in p2p Networks,” Proc. 17th Int’l Conf. Parallel and Distributed Computing Systems (PDCS), Nov. 2004.
23. 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, Aug. 2008.
24. 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