ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

# Secure Reputation Mechanism For Unstructured Peer To Peer System

**N. Vijaya Kumar.[1], Prof. Senthilnathan [2]**

M.E, Department of CSE, P.S.V College of Engineering and Technology, Krishnagiri, Tamilnadu, India[1]

Head of the Department, Department of CSE, P.S.V College of Engineering and Technology, Krishnagiri, Tamilnadu, India[2]

**ABSTRACT :** Distributed hash tables (DHTs) share storage and routing responsibility among all nodes in a peer-to-peer network. These networks have bounded path length unlike unstructured networks. Unfortunately, nodes can deny access to keys or misroute lookups. We address both of these problems through replica placement. In its simplest form, a peer-to-peer network is created when two or more PCs are connected and share resources without going through a separate server computer. In effect, every connected PC is at once a server and a client. Peer to peer networks can be categorized into structured and unstructured peer to peer networks. The proposed system can be used on top of both structured and unstructured peer to peer networks. In structured networks, the peer or system which start to search a file into other peers by establishing paths (i.e. the source system knows where the searching happen are). The unstructured peer to peer networks do not have a well-known architecture. In unstructured networks, there is no relationship between the source with other peers except neighbor peer and its location. Our proposed work is to search a file in a structured and unstructured peer to peer network.

The absence of a central authority in a peer to peer network poses unique challenges for reputation management in the network. These challenges include identity management of the peers, secure reputation data management, Sybil attacks, and above all, availability of reputation data. Reputation management is each and every peer must store the searching and file identified information or details which help to reduce the searching time in both type of peer to peer network. Need security for unstructured network search because the searching peer doesn't know where the file is searched and download. In this project, we added a cryptographic protocol for ensuring secure and timely availability of the reputation data of a peer to other peers at extremely low costs. Content auditing is done on receiver side even signature fails and mentions the ratio or impact of fake content. As result, a peer's reputation motivates it to cooperate and desist from malicious activities. The cryptographic protocol is coupled with self-certification and cryptographic mechanisms for identity management and countering Sybil attack.

## I.INTRODUCTION

### 1.1 PEER TO PEER NETWORK

PEER-TO-PEER networks are self-configuring networks with minimal or no central control. Peer to peer 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. For example, the infamous VBS. Gnutella worm that infected the Gnutella network, stored Trojans in the host machine. The peers in the peer to peer network have to be discouraged from leeching on the network. It has been shown in Tragedy of Commons that a system where peers

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

work only for selfish interests while breaking the rules decays to death. Policing these networks is extremely difficult due to the decentralized and ad hoc nature of these networks. Besides, peer to peer networks, like the Internet, are physically spread across 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 peer to peer networks. This is because the trusted central authority used in the traditional client-server networks is absent in peer to peer networks. Introduction of a central trusted authority like a Certificate Authority (CA) can reduce the difficulty of securing peer to peer networks. The major disadvantage of the centralized approach is, if the central authority turns malicious, the network will become vulnerable. In the absence of any central authority, repository, or global information, there is no silver bullet for securing peer to peer networks. Decentralized peer to peer systems are typically classified into two categories: structured peer to peer systems and unstructured peer to peer systems.

### 1.2 ARCHITECTURE OF PEER TO PEER SYSTEMS

Peer-to-peer systems often implement an abstract overlay network, built at Application Layer, on top of the native or physical network topology. Such overlays are used for indexing and peer discovery and make the peer to peer system independent from the physical network topology. content is typically exchanged directly over the underlying Internet Protocol (IP) network. Anonymous peer-to-peer systems are an exception, and implement extra routing layers to obscure the identity of the source or destination of queries.

#### 1.2.1 Structured Systems

Structured peer to peer networks employ a globally consistent protocol to ensure that any node can efficiently route a search to some peer that has the desired file, even if the file is extremely rare. Such a guarantee necessitates a more structured pattern of overlay links. By far the most common type of structured peer to peer network is the distributed hash table (DHT), in which a variant of consistent hashing is used to assign ownership of each file to a particular peer, in a way analogous to a traditional hash table's assignment of each key to a particular array slot.

#### 1.2.2 Unstructured Systems

An unstructured peer to peer network is formed when the overlay links are established arbitrarily. Such networks can be easily constructed as a new peer that wants to join the network can copy existing links of another node and then form its own links over time. In an unstructured peer to peer network, if a peer wants to find a desired piece of data in the network, the query has to be flooded through the network to find as many peers as possible that share the data. The main disadvantage with such networks is that the queries may not always be resolved. Popular content is likely to be available at several peers and any peer searching for it is likely to find the same thing. But if a peer is looking for rare data shared by only a few other peers, then it is highly unlikely that search will be successful. Since there is no correlation between a peer and the content managed by it, there is no guarantee that flooding will find a peer that has the desired data. Flooding also causes a high amount of signaling traffic in the network and hence such networks typically have very poor search efficiency. Many of the popular peer to peer networks are unstructured. The main requirements are:1. A self-certification-based identity system protected by cryptographically blind identity mechanisms, A light weight and simple reputation model. 2. An attack resistant cryptographic protocol for generation of authentic global reputation information of a peer.

### 1.3 GENERAL PROJECT DETAILS

Reputation systems based on DHT have been used both in client-server and peer to peer networks. The current state of art in reputation systems for peer to peer networks can be classified into three main categories. The first two categories consist of the reputation models and systems developed for the peer to peer networks. These reputation systems

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

exemplify the usefulness of a reputation system and other related reputation metrics, for mitigation of the impact of malicious nodes on peer to peer networks. The third category consists of the reputation systems developed for client-server systems. Open nature of peer-to-peer systems exposes them to malicious activity. Building trust relationships among peers can mitigate attacks of malicious peers. This paper presents distributed algorithms that enable a peer to reason about trustworthiness of other peers based on past interactions and recommendations. Peers create their own trust network in their proximity by using local information available and do not try to learn global trust information. Two contexts of trust, service, and recommendation contexts, are defined to measure trustworthiness in providing services and giving recommendations. Interactions and recommendations are evaluated based on importance, recentness, and peer satisfaction parameters. Additionally, recommender's trustworthiness and confidence about a recommendation are considered while evaluating recommendations. We propose a Self-Organizing Trust model (SORT) that aims to decrease malicious activity in a peer to peer system by establishing trust relations among peers in their proximity. As a consequence, a user of such semantic peer to peer systems is not always satisfied with the answers returned to his queries. After a while, when having received enough answers, he may naturally be inclined to trust/distrust further answers obtained by those sources that have contributed to obtain previous good/bad results. The proposal of an adequate model to assess the level of confidence that a peer may have in a given answer is thus an important issue. In such semantic peer to peer systems, no user imposes to others his own ontology but logical mappings between ontology's make possible the creation of a network of people in which personalized semantic marking up of data cohabits nicely with a collaborative exchange of data. The mappings are exploited during information retrieval or query answering for query reformulation between peers.

### 1.4 A NEW TRUST MODEL FOR TRUSTWORTHINESS-BASEDROUTING PROTOCOLS IN SENSOR NETWORKS

For wireless sensor networks (WSNs), particularly those deployed in adversary environment, a major concern's how to the provide security to the carried data by using various security primitives, while maintain the trust worthiness among the nodes in the networks. A commonly used strategy is to assume that there exists a public key infrastructure (PKI)or other certificate authority (CA) during its deployment in the network. However, an initially trusted node may become compromised due to various attacks launched by malicious nodes. The major problem is how to build up and update the trust among the nodes. In this paper, we propose a new model to estimate the trustworthiness among the nodes. The value of the trust worthiness can be observed by each node independently. Routing protocol and propose anew secure trustworthiness-based anonymous routing (STAR) protocol. The trustworthiness of a node is selected as a routing metric so that the nodes with malicious behavior can be avoided. The simulation results have demonstrated the effectiveness of the

.**Advantages**

- Securely and accurately generating provenance information within a computing system. Understanding and controlling the storage and computational overheads of managing the provenance information.

**Drawbacks**

Privacy and confidentiality and the inherent information leakage associated with its collection are daunting (very difficult).

## II. DISTRIBUTED HASH TABLE (DHT) BASED TECHNIQUE

Management of trust information is dependent to the structure of peer to peer network. In distributed hash table (DHT) based techniques, each peer becomes a trust holder by storing feedbacks about other peers**.** Global trust information stored by trust holders can be accessed through DHT efficiently. In unstructured networks, each peer stores trust information about peers in its neighborhood or peers interacted in the past. A peer sends trust queries to learn trust

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

information of other peers. A trust query is either flooded to the network or sent to neighborhood of the query initiator. Generally, calculated trust information is not global and does not reflect opinions of all peers.

**Drawbacks**

- Client response time will be high because of long searching time.
- Congestion overflows due to flow of many clients' request.
- Low level trust peer security system thus allows several malicious attacks with reference to unstructured networks.

**Self-Organizing Trust Model Technique**

SORT aims to decrease malicious activity in a PEER TO PEER system by establishing trust relations among peers in their proximity. **No a priori information or a trusted peer** is used to leverage trust establishment. **Peers do not try to collect trust information** from all peers. Each peer develops its own local view of **trust about the peers** interacted in the past. In this way, good peers form dynamic trust groups in their proximity and can isolate malicious peers.

We implemented a peer to peer file sharing and searching and conducted experiments to understand impact of SORT in mitigating attacks especially false data injection.

We define cryptographic verification as a robust mechanism that ensures the **true origin of the data produced** by an entity such as a system stored data. Therefore, we aim to detect the two specific behaviors (traffic-checkpoint bypassing and fake data injection) under the assumption that our detection system is not compromised at the run time. We define three operations for data-provenance verification on a host: setup, sign, and verify.

- **Setup.** The data producer sets up its signing key k and data consumer sets up its verification key k0 in a secure fashion that prevents malware from accessing the secret keys.
- **Sign (D; k).** The data producer signs its data D with a secret key k, and outputs D along with its proof sig.
- **Verify (sig; D; k0).** The data consumer uses key k0 to verify the signature sig of received data D to ensure its origin, and rejects the data if the verification fails.

Although simple, the **cryptographic provenance verification** method can be used to ensure and enforce correct system and network properties and appropriate workflow under a trusted computing environment.

The main contributions of this project are:

1. A self-certification-based identity system protected by cryptographically blind identity mechanisms.
2. A light weight and simple reputation model.
3. An attack resistant cryptographic protocol for generation of authentic global reputation information of a peer.

In addition SORT, peers send reputation queries only to peers interacted in the past using DHT, which reduces network traffic comparing to flooding-based approaches.

**Advantages**

- The protocol prevents the forgery of fake data events by malware under reasonable assumptions.
- Low level traffic flow thus improves response time and avoids possibilities of malicious activities.
- Established better trusted platform.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

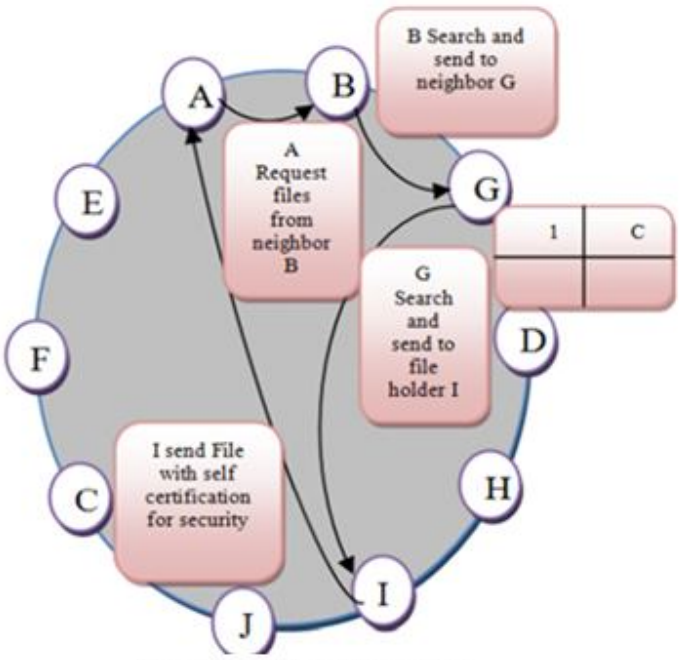
(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

## III. ARCHITECTURE DIAGRAM




3.4 Architecture Diagram

**SYSTEM MODELS**

- Unstructured Peer to Peer network formation
- Reputation or hash table based searching
- Asymmetric cryptography approach
- Digital signature matching system
- Data auditing under training sets

## IV. UNSTRUCTURED PEER TO PEER NETWORK

An unstructured peer to peer network is formed when the overlay links are established arbitrarily. Such networks can be easily constructed as a new peer that wants to join the network can copy existing links of another node and then form its own links over time. In an unstructured peer to peer network, if a peer wants to find a desired piece of data in the network, the query has to be flooded through the network to find as many peers as possible that share the data. Each peer known only their neighbor peer that's represents unstructured Peer to Peer network

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

## V. REPUTATION OR HASH TABLE BASED SEARCHING

In the unstructured peer to peer networks, peers willingness to share the content they have and forward the queries plays an important role during the content search process. Each and every peer in the network must maintain this table which is used to forward the peer request to the apt peer instead of its neighbor peer. 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 peers past activity).It helps to perform the file searching operation efficiently. The self certificate is used for ensuring secure and timely availability of the reputation data of a peer to other peers. 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

**Asymmetric Cryptography Approach**

Peers generate universally unique identifications locally and store them along with their public key, their current IP address. Implementation of Self Certification and Digital Signature for Secure Communication is focused in this module. RSA is used to generate public key and for data encryption and decryption

**Digital Signature Matching System**

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 DS. 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, at receiver side receives the file and generates the signature, it will be matched with the attached signature if true conclude no more presence of malicious peer else proceed next module steps.

**Data Auditing Under Training Sets**

Each receiver maintains trained data sets which are used whether signature verification fails. Each content or word must be compared with trained data set and find the similarity if the similarity is much more then it concludes the content must be malicious to the peer so on the attack basis it just warns the peer else the file will be received successfully and safe

## VI. CONCLUSION

This project presents self-certification, an identity management mechanism, reputation model, and a cryptographic protocol that facilitates generation of global reputation data in a peer to peer network, in order to expedite detection of rogues. A reputation system for peer-to-peer networks can be thwarted by a consortium of malicious nodes. Such a group can maliciously raise the reputation of one or more members of the group. There is no known method to protect a reputation system against liar farms and the absence of a third trusted party makes the problem of liar farms even more difficult. The global reputation data are protected against any malicious modification by the third party peer and are immune to any malicious modifications by their owner. The proposed protocol reduces the number of malicious transactions and consumes less bandwidth per transaction than the other reputation systems proposed in its category. It also handles the problem of highly erratic availability pattern of the peers in peer to peer networks.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

## VII. FUTURE ENHANCEMENT

In the above proposed work they successfully identified whether the fake data's present in the received file or not but fails to classify the fake data ratio because if fake data impact is not affect able which apt to receiver then it must be trusted one so out work is to find the good and bad count of words in the received file. This must be needed one for avoiding loss of legitimate files. We are using **Bayesian probability** technique for text classification.

### BAYESIAN PROBABILITY TECHNIQUE

Each receiver maintains trained data sets which are used whether signature verification fails. Each content or word must be compared with trained data set and find the similarity if the similarity is much more then it concludes the content must be malicious to the peer so on the attack basis it just warns the peer else the file will be received successfully and safe.

- **Preparation of Testing/classifying Set.**
  All received files in the testing set are pre classified and mixed together**.**
- **Preprocessing.**
  All the words in the file are preprocessed as separate words in the trained file.
- **Generating word list.**
  A tokenizes file contents into word lists. A stop word list is used to delete stops words from word lists.
- **Generating word maps.**
  A word map is a list of words that appear both in a given. One word map contains words that appear in the received file.
- **Classifying an file**
  According to the word maps, probabilities of *W* word map to determine if a word is an unwanted word.

### CLASSIFICATION BASED SORT TECHNIQUE

Step 1: Initialize server with respect to ip address and port number and its neighbor peer thus make unstructured network configurations.
Step 2: Generate signature with respect to each peer according to its own certificate key.
Step 3: Client start to file search in the other peers by routing the request to its neighbor peer.
Step 4: Each peer search its hash table if match occur act as replica system and forwards the request to the respective peer instead of its neighbor else search it in local folder and forwards to its neighbor peer.
Step 5: Send the file to the request peer in encrypted format and signature will be generated as per file content size then attached in the packet header.
Step 6: Client systems receive the file and generate the signature according to received content then matches the signature with the signature in the header packet and decrypts the file if file auditing is success else conclude that falsy content is present in the original file content.
Step 7: If identified the fake content presence in the original file then able to find out the ratio of good and bad word count before rejection of original file. By applying classification mechanism this could be possible, then as per ratio result the file will be declared as secure or rejected.

## ACKNOWLEDGEMENT

The success and final outcome of this project required a lot of guidance and assistance from many people and I am extremely fortunate to have got this all along the completion of my project work. Whatever I have done is only due to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

guidance and assistance and I would not forget to thank them. I respect and thank my guide Mr. B. SENTHIL NATHAN M.E., Asst.Proffesor Department of Computer Science and Engineering for providing all support and guidance which made me to complete the project on time. . The blessing, help and guidance given by him time to time shall carry me a long way in the journey of life on which I am about to embark .Lastly, I thank almighty, my parents, husband and children for their constant encouragement without which this assignment would not be possible.

## REFERENCES

[1] K. Abiders 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.A. Selcuk, E. Uzun, and M.R. Pariente, "A Reputation-Based Trust Management System for PEER TO PEER Networks," Proc. IEEE/ACM Fourth Int'l Symp. Cluster Computing and the Grid (CCGRID), 2004.
[3]F. Cornelli, E. Damiani, S.D.C. di Vimercati, S. Paraboschi, and P. Samarati, " Choosing Reputable Servents in a PEER TO PEER Network," Proc. 11th World Wide Web Conf. (WWW), 2002.
[4]J. Kleinberg, "The Small-World Phenomenon: An Algorithmic Perspective," Proc. 32nd ACM Symp. Theory of Computing, 2000
[5]L. Xiong and L. Liu, "Peertrust: Supporting Reputation-Based Trust for Peer-to-Peer Ecommerce Communities," IEEE Trans. Knowledge and Data Eng., vol. 16, no. 7, pp. 843-857, July 2004.
[6]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, Sept. 2008...
[7]S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The (Eigentrust) Algorithm for Reputation Management in PEER TO PEER Networks," Proc. 12th World Wide Web Conf. (WWW), 2003.
[8]S. Saroiu, P. Gummadi, and S. Gribble, "A Measurement Study of Peer-to-Peer File Sharing Systems," Proc. Multimedia Computing and Networking, 2002.
[9] 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.
[11] S. Marsh, "Formalising Trust as a Computational Concept," PhD thesis, Dept. of Math. and Computer Science, Univ. of Stirling, 1994.
[12] A. Abdul-Rahman and S. Hailes, "Supporting Trust in Virtual Communities," Proc. 33rd Hawaii Int'l Conf. System Sciences (HICSS), 2000.
[13] B. Yu and M. Singh, "A Social Mechanism of Reputation Management in Electronic Communities," Proc. Cooperative Information Agents (CIA), 2000.
[14] L. Mui, M. Mohtashemi, and A. Halberstadt, "A Computational Model of Trust and Reputation for E-Businesses," Proc. 35th Hawaii Int'l Conf. System Sciences (HICSS), 2002.
[15] A. Jøsang, E. Gray, and M. Kinateder, "Analysing Topologies of Transitive Trust," Proc. First Int'l Workshop Formal Aspects in Security and Trust (FAST), 2003.