Implementation of P2P Reputation Management Using Distributed Identities and Decentralized Recommendation Chains

P.Satheesh
Associate professor
Dept of Computer Science and Engineering
MVGR college of Engineering
Vizianagaram, India
patchikolla@yahoo.com

P.Naresh
Dept of Computer Science and Engineering
MVGR college of Engineering
Vizianagaram, India
nareshpucha@gmail.com

Abstract

In this paper, we investigate Reputation Systems for P2P networks more ambitious approach to protect the P2P network without using any central component, and thereby harnessing the full benefits of the P2P network. 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. 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 certificate authority which issues the identity certificates to the peer. Each peer owns the reputation information pertaining to all its past transactions with other peers in the network, and stores it locally. A two-party cryptographic protocol not only protects the reputation information from its owner, but also facilitates secure exchange of reputation information between the two peers participating in a transaction.

Index Terms: peer, digital certificate, Encryption, Cryptography.

1. Introduction:

Peer-to-peer (P2P) computing or networking is a distributed application architecture that partitions tasks or workloads among peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes. Peers 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 central coordination by servers or stable hosts. Peers are both suppliers and consumers of resources, in contrast to the traditional client–server model where only servers supply, and clients consume.

Fig 1: Peer to Peer System

This thus gives P2P systems two main key characteristics:

Scalability: There is no algorithmic or technical limitation of the size of the system, e.g. the complexity of the system should be somewhat constant regardless of number of nodes in the system.

Reliability: The malfunction on any given node will not affect the whole system (or maybe even any other nodes).

Peer-to-peer network are classified into two types

- Structured Systems
- Unstructured Systems
Structured P2P 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 P2P network is the distributed hash table, 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.

An unstructured P2P 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 P2P 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 P2P networks are unstructured.

Reputation Models

Resnick et al. define the reputation system as “a system that collects, distributes, and aggregates feedback about consumers past behavior.” The authors outline the problems in eliciting, distributing, and aggregating feedback. Resnick et al. explain the problem of pseud spoofing in [2]. Pseudo spoofing is the use of multiple pseudonyms in a system by the same real-life entity. The disadvantage is that any entity can discard a handle or a pseudonym with which a bad reputation is associated and join the system as a new user, under a new pseudonym. This can possibly nullify the usefulness of a reputation system, which assigns reputations to handles. The authors also advocate that the newcomers should pay their dues in order to mitigate the effect of pseudo spoofing. In other words, the newcomers should not only use the services of the system but should also contribute to the system as per the system guidelines. PeerTrust [3] allocates the reputation information to a certain node on the network for storage, by using hash functions. Any peer looking for the reputation of another peer uses the search mechanism of the underlying network to search for the information. The authors of PeerTrust argue that trust models based solely on feedback from other peers in the community are ineffective and inaccurate. The authors recommend the “degree of satisfaction” of the peer from previous transactions and the number of transactions a peer performs in the system should be accounted for before calculating the reputation of the recommended peer. Abdul-Rahman and Hailes [4] have proposed another trust model and the corresponding metrics. They argue that Bayesian probability may not be the best metric for representing degree of trust, because probability is inherently transitive while trust is not. In addition, the authors provide methods for combining
recommendations and use the context of recommendations and recommender weights to evaluate the reputations from recommendations. Aberer and Despotovic [5] have proposed completely distributed solution for trust management over the P-Grid peer-to-peer network. They store reputation data in the form of a binary search tree, over the network. Any agent looking for the recommendation data of another agent searches the P2P network and computes the reputation from the recommendations received. Chen and Singh [6] and Scheinetal. [7] also provide trust models, similar to those mentioned above. Dellarocas [8] has enumerated the design challenges in the online reporting systems. Dellarocas surveys online reputation, reporting mechanisms, and the corresponding issues. In addition, the author provides a good overview of recommendation repositories, professional rating sites, collaborative filtering systems [9], and regression approaches. Dellarocas also enumerates the attacks on reputation systems and techniques for foiling those attacks.

2. Approaching methods

In our proposed system we have seven modules they are

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

Login Module:

In this module it is responsible for user authentication and registration of new users.

Active Node in Dynamic root

In our communication group have number of client nodes are interconnected in the server. when a new number joins or leaves the communication group only it’s reflecting for local group each group have separate group key for communication in between who are in the communication group in that time.

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.

Trusted Group Members

We divide the multicast group into regional subgroups .each subgroup is independently managed by a subgroup controller like a separate multicast group with its own sub group key .our protocol is responsible for reducing the overload of the group controller.
Data Transfer
In our multicast communication group mainly concentrate on enabling the data transfer among the server and multiple clients in the network communication.

Find Group Key
When a new member joins 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.

Block Untrusted User
Trusted users are formed a group. If a new member request to join in group, the IP Address will be validated. IP address will be validate with the help of subnet masking, such as the Class A, Class B, Class C Part of the IP address. If the IP is not matched with the trusted group then it will not be allowed to enter into the trusted group.

3. CONCLUSION
This paper presents self-certification, an identity management mechanism, reputation model, and a cryptographic protocol that facilitates generation of global reputation data in a P2P 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 self-certification-based identity generation mechanism reduces the threat of liar farms by binding the network identity of a peer to his real-life identity while still providing him anonymity. The Identity mechanism is based on the fundamental that the ranks of the peers are more relevant than the absolute value of their reputation. The cost of this security is the difference in the ranks of the providers because of the use of the proposed mechanism. 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 P2P networks. Currently, the reputation of the provider is considered and the reputation of the requester is ignored.
4. FUTURE ENHANCEMENT

This system can be extended to encapsulate the reputations of both the provider and the requester. In addition, instead of generic number values, the reputation values can be modified in accordance with the context of the reputation.

5. REFERENCES


AUTHOR PROFILE

The Author “P. Satheesh” is an associate professor in CSE in MVGR College of Engineering and pursuing PhD in Acharya Nagarjuna University. His research interest are bioinformatics.

The Author “P. Naresh” done his B.Tech in CSIT in JNTUK doing his post graduation in MVGR College of Engineering. His Area of interest are Networking and Software Engineering.