A Novel Architecture For Peer-To-Peer System to Provide Security

[1]T.B.Priyadarshini, [2]A.Phani Sridhar, [3]G.Kalyanchakravarthi
[1]M.Tech(Computer Science)
[2,3]Asst.Professor

Abstract
This paper propose A NOVEL ARCHITECTURE FOR PEER-TO-PEER SYSTEM TO PROVIDE SECURITY that aims to decrease malicious activity in a P2P system by establishing trust relations among peers in their proximity. In THIS ARCHITECTURE, peers are assumed to be strangers to each other at the beginning. A peer becomes an acquaintance of another peer after providing a service, e.g., uploading a file. If a peer has no acquaintance, it chooses to trust strangers.
THIS ARCHITECTURE defines three trust metrics. Reputation metric is calculated based on recommendations. It is important when deciding about strangers and new acquaintances. Reputation loses its importance as experience with an acquaintance increases. Service trust and recommendation trust are primary metrics to measure trustworthiness in the service and recommendation contexts, respectively.
The service trust metric is used when selecting service providers. The recommendation trust metric is important when requesting recommendations. When calculating the reputation metric, recommendations are evaluated based on the recommendation trust metric

Keywords
Peer to Peer, Security,etc…

I. Introduction

A. Objective of the Project

PEER-TO-PEER (P2P) systems rely on collaboration of peers to accomplish tasks. Ease of performing malicious activity is a threat for security of P2P systems. Creating long-term trust relationships among peers can provide a more secure environment by reducing risk and uncertainty in future P2P interactions. However, establishing trust in an unknown entity is difficult in such a malicious environment. Furthermore, trust is a social concept and hard to measure with numerical values. Metrics are needed to represent trust in computational models.
Classifying peers as either trustworthy or untrustworthy is not sufficient in most cases. Metrics should have precision so peers can be ranked according to trustworthiness. Interactions and feedbacks of peers provide information to measure trust among peers. Interactions with a peer provide certain information about the peer but feedbacks might contain deceptive information. This makes assessment of trustworthiness a challenge. In the presence of an authority, a central server is a preferred way to store and manage trust information, e.g., eBay.
The central server securely stores trust information and defines trust metrics. Since there is no central server in most P2P systems, peers organize themselves to store and manage trust information about each other . Management of trust information is dependent to the structure of P2P network. In distributed hash table (DHT)-based approaches, 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 information of other 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. Since peers generally tend to interact with a small set of peers, forming trust relations in proximity of peers helps to mitigate attacks in a P2P system.

1. Supporting Trust in Virtual Communities:

This work is to provide a trust model for virtual communities that

- Assists users in identifying trustworthy entities and
- Gives artificial autonomous agents the ability to reason about trust. Our trust model must be based on real world characteristics of trust. The model will also need to be simple to understand so that it is intuitive and usable. Additionally, the metrics used must be unambiguous to the user. It will also need to be simple enough to implement in the codes of artificial agents, which may be subject to strict resource constraints.

In our approach to discovering the 'real-world' characteristics of trust, turned to the social sciences. Much work have been carried out on the subject of trust in the field of sociology, philosophy, socio-psychology and economics. Thus it provides a rich environment for us to draw notes from. Work on a trust model that is based on reputation, or word of mouth, as this is an important trust supporting social mechanism.

2. Analysing Topologies of Transitive Trust

This paper describes diverse dimensions of trust that are needed for analysing trust topologies, and provides a notation with which to express trust relationships in terms of these dimensions. The result is a simple way of specifying topologies of trust from which derived trust relationships can be automatically and securely computed.

A. Trust Diversity

Humans use trust to facilitate interaction and accept risk in situations where complete information is unavailable. However, trust is a complex concept that is difficult to stringently define. A wide variety of definitions of trust have been put forward , many of which are dependent on the context in which interaction occurs, or on the observer's subjective point of view. Deutsch's definition of trust is commonly used as a starting point for understanding: While Deutsch breaks trust down further into several different circumstances in which a trusting choice might be made, he concentrates on the fact that trust "is strongly liked to confidence in, and overall optimism about, desirable events taking place."

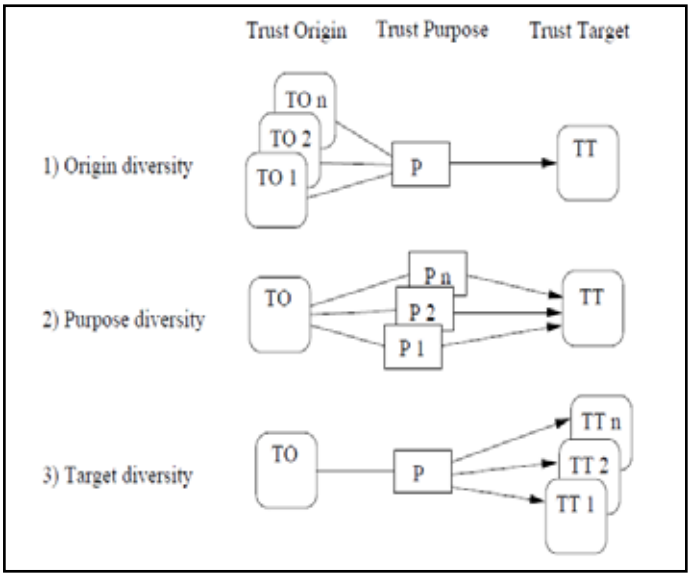


Fig. 1: "Basic Trust Diversity"

B. Trust Transitivity

Trust transitivity means, for example, that if Alice trusts Bob who trusts Clark then Alice will also trust Clark. This assumes that Bob actually tells Alice that he trusts Clark, and this will typically happen in a recommendation. In this simple example the trust origins and trust targets are easily identifiable, but it does not say anything specific about the trust purposes. Let us assume that Alice needs to have her car serviced, so she asks Bob for his advice about where to find a good car mechanic in town. Bob is thus trusted by Alice to know about a good car mechanic and to tell his honest opinion about that, whereas Clark is trusted by Bob to be a good car mechanic.

By assuming Alice's trust in Bob and Bob's trust in Claire to be positive but not absolute, Alice's derived trust in David is intuitively weaker that Claire's trust in David. It could be argued that negative trust in a transitive chain can have the paradoxical effect of strengthening the derived trust.

3. Detecting Deception in Reputation Management

The author developed a model of reputation management based on the Dempster - Shafer theory of evidence. To do so effectively presupposes certain representation and reasoning capabilities on the part of each agent. Each agent has a set of acquaintances, a subset of which are identified as its neighbors. The neighbors are the agents that the given agent would contact and the agents that it would refer others to.

4. Propagation of Trust and Distrust Approaches to trust Propagation

A natural approach to estimate the quality of a piece of information is to aggregate the opinions of many users. But this approach suffers from the same concerns around disinformation as the web at large: it is easy for a user or coalition of users to adopt many personas and together express a large number of biased opinions. Instead, we wish to ground our conclusions in trust relationships that have been built and maintained over time, much as individuals do in the real world. A user is much more likely to believe statements from a trusted acquaintance than from a stranger.

Modules

- Network Formation
- Service Metric
- Reputation Metric
- Recommendation Metric
- Select Service Providers

Modules Description

Network Formation

In this module the peer to peer network is formed for communication and file sharing. Each peer have unique id. Each peer in the network will give the own details such as Peer ID and IP address, through which the transmission is done and similarly give the known peers details ie., neighbor peer information such as Peer ID, IP address and port number which are neighbors to given node. After the Network Formation a Peer can upload or download a file from a neighbor peers.

Service Metric

In this module a peer can compute the service metric. For evaluating an acquaintance's trustworthiness in the service context, a peer first calculates competence and integrity belief values using the information in its service history.

Reputation Metric

In this module the peer find the reputation metric. It measures a stranger's trustworthiness based on recommendations. Assume that p_j is a stranger to p_i and p_k is an acquaintance of p_i. If p_i wants to calculate r_{ij} value, it starts a reputation query to collect recommendations from its acquaintances.

Algorithm 1 shows (in fig. 7) how pi selects trustworthy acquaintances and requests their recommendations. Let η_{max} denote the maximum number of recommendations that can be collected in a reputation query and |S| denote the size of a set S. In the algorithm, pi sets a high threshold for recommendation trust values and requests recommendations from highly trusted acquaintances first.

Then, it decreases the threshold and repeats the same operations. To prevent excessive network traffic, the algorithm stops when η_{max} recommendations are collected or the threshold drops under $(\mu_{rt} - \sigma_{rt})$ value.

Recommendation Metric

A recommendation is evaluated according to recommendation trust value of the recommender. In particular, pi evaluates pk's recommendation based on rtik value. After calculating rij value, pi updates recommendation trust values of recommenders based on accuracy of their recommendations.

Select Service Providers

Service provider selection is done based on service trust metric, service history size, competence belief, and integrity belief values. When pi wants to download a file, it selects an uploader with the highest service trust value. If service trust values are equal, the peer with a larger service history size (hs) is selected to prioritize the one with more direct experience.

If these values are equal, the one with a larger cb – ib/2 value is chosen. If cb – ib/2 values are equal, the one with larger competence belief value is selected. If these values are equal, upload bandwidths are compared. If the tie cannot be broken, one of the equal peers is randomly selected.

Experimental Result

A file sharing simulation program is implemented in Java to observe results of using THIS ARCHITECTURE in a P2P environment. Some questions studied in the experiments are as follows:
HowTHIS ARCHITECTURE handles attacks, how much attacks can be mitigated, how much recommendations are (not) helpful in correctly identifying malicious peers, and what type of attackers are the most harmful.
Downloading a file is an interaction. A peer sharing files is called an uploaded. A peer downloading a file is called a downloader. The set of peers who downloaded a file from a peer are called downloader's of the peer. An ongoing download/ upload operation is called a session.
Attackers can perform service-based and recommendation based attacks. Uploading a virus infected or an inauthentic file is a service-based attack. Giving a misleading recommendation intentionally is a recommendation-based attack.

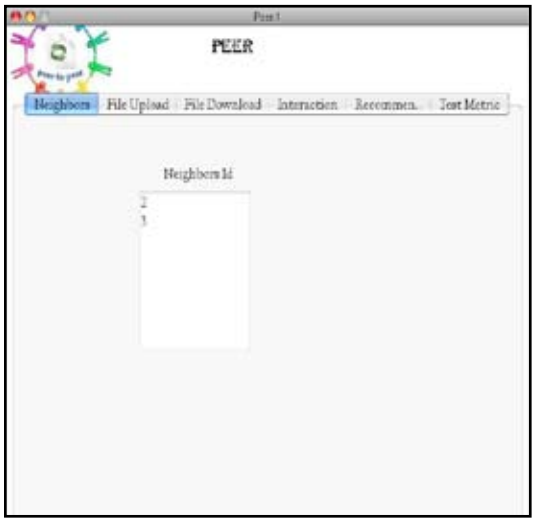
Conclusion

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.

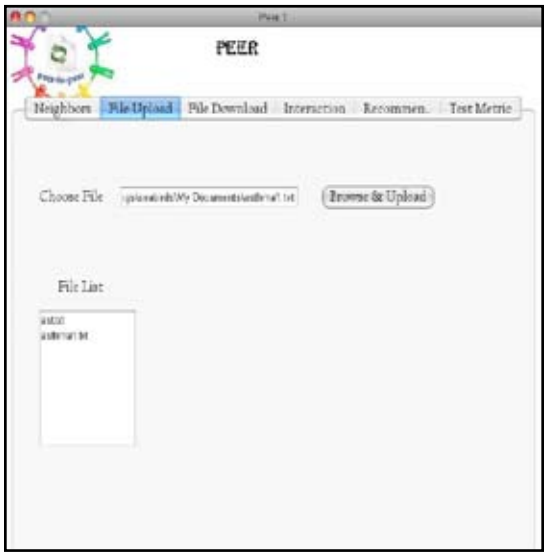
References

[1] A. Abdul-Rahman, S. Hailes,"Supporting Trust in Virtual Communities", Proc. 33rd Hawaii Int'l Conf. System Sciences (HICSS), 2000.
[2] A. Jøsang, E. Gray, M. Kinateder,"Analysing Topologies of Transitive Trust", Proc. First Int'l Workshop Formal Aspects in Security and Trust (FAST), 2003.
[3] K. Hoffman, D. Zage, C. Nita-Rotaru,"A Survey of Attack and Defense Techniques for Reputation Systems", ACM Computing Surveys, Vol. 42, No. 1, pp. 1:1-1:31, 2009.
[4] R. Zhou, K. Hwang,"Power trust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing", IEEE Trans. Parallel and Distributed Systems, Vol. 18, No. 4, pp. 460-473, Apr. 2007.
[5] K. Aberer, Z. Despotovic,"Managing Trust in a Peer-2-Peer Information System".
[6] A.A. Selcuk, E. Uzun, M.R. Pariente,"A Reputation-Based Trust Management System for P2P Networks".

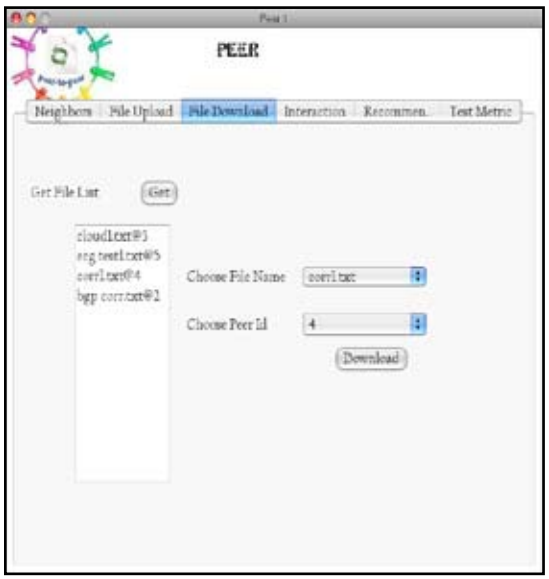
Screen Shots:



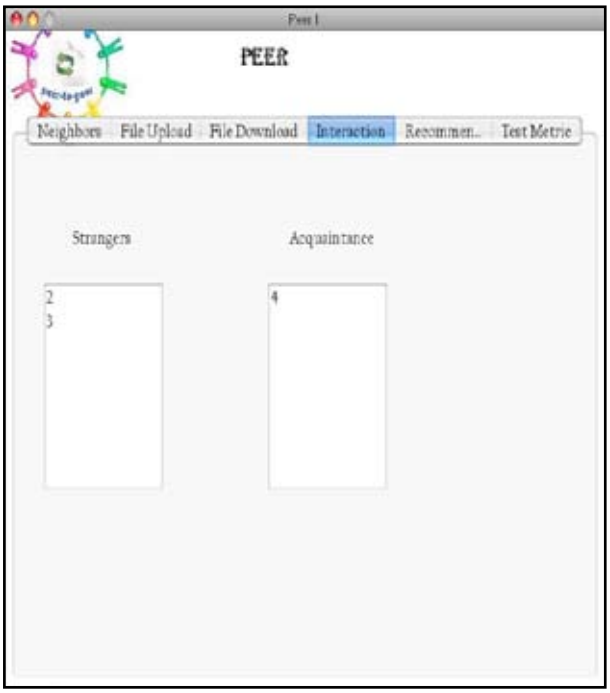
"This screen shows Neighbors window in which it displays neighbors ID".



"This screen shows fileupload window in which we have to choose a file and it displays file list".



"This screen shows file download window, in which we can choose a file and choose a peer id and it displays all the file we are select before".



"This screen shows interaction window in which it displays strangers and acqaitance values".