Secure Group Communication by Establishing a Novel Trust Relationship Model and Detecting Malicious nodes in Peer to Peer Systems

M. Ruby¹, Dr. K. Venkatarao²

¹#1. M.Tech Scholar, Department of Computer Science Engineering, Vignan’s Institute of Information Technology, Duvvada, Visakhapatnam, India.
²#2. Professor, Department of Computer Science and Engineering, Vignan’s Institute of Information Technology, Duvvada, Visakhapatnam, India.

Abstract –
Trust administration in P2P framework is utilized to distinguish vindictive practices and to advance legitimate and agreeable communications. The fundamental objective of the prior P2P frameworks is the capacity of conglomerating assets, which expect certain trustworthiness level of companions. In any case, as P2P frameworks become immensely in size, there will be an impressive number of vindictive companions who convey security assaults and dangers to the entire system. In a disseminated foundation without concentrated server for power, giving security instrument is more confused than in server-driven arrangements, as the presence of different locales builds the defenselessness and security endeavors must be reproduced at various destinations. In this way security issues are one of the significant difficulties that should be deliberately dissected and tended to, particularly for completely decentralized unstructured P2P frameworks. A ton of examines are being directed to enhance the trust administration in shared framework. A few notoriety based trust administration frameworks are investigated here. In this paper, we present building trust connections among associates can alleviate assaults of malevolent companions. This paper presents dispersed calculations that empower a companion to reason about reliability of different associates in view of past cooperation’s and suggestions. Companions make their own particular trust system in their nearness by utilizing nearby data accessible and don't attempt to learn worldwide trust data.

KEYWORDS: Trust management; Peer-to-Peer systems; Reputation system; Sampling approaches; Search process; NTRM; Query processing

I. INTRODUCTION

Peer frameworks fulfill assignments by depending on cooperation. P2P frameworks are presented to security dangers, because of absence of focal power and element in nature. If there should be an occurrence of secure environment, building up of trust relationship can lessen the danger and solid in future associations. The major difficulties for shared (P2P) frameworks are to deal with the dangers included in communication and coordinated effort with cloister obscure and possibly harmful specialists. If there should arise an occurrence of harmful environment, building up trust is a most troublesome errand. Additionally, trust is a social marvel i.e. firm confidence in the unwavering quality and hard to quantify with numeric qualities. Benchmarks are expected to symbolize trust. Positioning of associates is vital with the goal that reliability can be shown in view of measurements characterized. The estimation of trust relies upon associations and criticisms of companions. Cooperation with a companion give particular data yet inputs may contain illusive data. Distributed is a decentralized system building design in which every one of the companions are
A novel trust model is recommended that purpose to diminish harmful action in a P2P framework by setting up trust relations among companions in their contiguity. Nearby perspective of trust is created by its own in light of the past cooperation. In this way, great companions structure element trust bunches in their contiguity and can segregate harmful associates. In novel trust, toward the start of the procedure the associates are thought to be outsiders. Strictly when giving an administration, a companion turns into a colleague of another associate e.g., record transferring. The associate trusts outsiders in the event that it has no colleague. Every associate has an arrangement of colleagues, a subset of which is recognized as its neighbors. Utilizing an administration of an associate is a cooperation, which is assessed taking into account need, and recentness of the connection, and happiness of the requester. An associate’s perception around a companion, suggestion, is computed taking into account recommender’s honesty. It contains the recommenders own experience about the associate, information gathered from the recommenders colleagues, and the recommender’s certainty level in the recommendation. In the event that the certainty level is low, the proposal has a low esteem in assessment. Novel characterizes three trust measurements. Notoriety metric speaks to the faith in the framework and permits gatherings to fabricate trust, or the extent to which one gathering has trust in another inside of the setting of a given reason or choice and is figured in light of proposals. The administration trust metric is utilized for choice of administration suppliers. The suggestion trust metric is required while asking for proposals.

II. RELATED WORK
Trust model creation taking into account taking after trust standards, for example, a) Trust is content-subordinate. b) Negative and positive conviction is bolstered. c) Trust depends on past experience. d) Information trade through proposal. e) Different suppositions of the considerable number of specialists are considered. f) Recommendations may expand or diminish the trust level [2]. Notoriety is the feeling of the general population towards a man or association or assets. In p2p, notoriety speaks to the conclusions hubs and assumption around an agent’s conduct in view of information or perceptions of its past conduct. In this, the clients rate the unwavering quality of gatherings they manage, and impart this information to their associates. Notoriety trust recognizes the vindictive reactions from benevolent ones by utilizing notoriety of companions gave by them. Peer’s past exchange are put away in trust vectors, which are of consistent length, twofold vector of 1 bit i.e. (8, 16, 32). A 1 bit speaks to a legitimate exchange; 0 speaks to an untrustworthy one.

Notoriety based trust administration properties:
1. No focal coordination. No focal database.
2. No associate has a worldwide perspective of the framework.
3. Local conduct rises up out of neighborhood collaborations.
4. Peers are self-ruling.
5. Peers and associations are questionable.

Types of ratings are performed:
1. Trust rating = (trust vector) / (2m) . (2m used for conversion)
2. Distrust rating = (complement of trust vector) / 2m [3]. A lightweight mechanism that allows the data originator to build up trust in the replica holder by means of protocols that do not require past trust or key establishment. The protocol does not prevent cheating and is based on a checksum or hash that is calculated over key-defined ranges of shared data. This check is performed in an iterative fashion with alternating roles, or compensated by the calculation of responses to challenges to prevent DoS attacks [4]. A peer provides trustworthy service and trustworthy feedback. Service is evaluated based on the parameters (file bandwidth, transaction time). Feedback may provide either good or bad values. Reputation system help peers decide whom to trust before undertaking a transaction. Each peer is designed with two sets of reputation ratings; an aggregated service rating ranging from -1.0 to 1.0 with 0 as neutral rating; an aggregated feedback rating ranging from 0 to -1.0 with 1.0 as good rater. Initially, s-rating is set to 0 and feedback to 1.0 for all the peers. A reputation system maintains for each peer a list of peers that has rated it and its rating. Defined as: s-rating(u) = α * s-rating(u)+ β * (ru * f-rating(i)) f-rating(u) = 1 / nu * _nu i=1 fu * f-rating(i) where ru indicates a service rating of -1 or 1; fu is the feedback rating which can be 0 or 1 depending on malicious feedback or helpful feedback; nu represents the total number of transactions that have made use of u’s feedback; and α and β are normalized weight factors, between 0 and 1, used to exponentially decay reputation ratings. A peer may exhibit honest and dishonest ratings. Once a peer has established a good reputation in the network, it can abuse it, and an honest peer may start behaving in a dishonest way too. Thus peer reputation must be of more recent rating interaction rather than old ratings [5].
III. PEER TO PEER SYSTEM
A peer-to-peer network is a type of decentralized and distributed network architecture in which individual nodes in the network 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 this network, tasks are shared amongst multiple interconnected peers who make a portion of their resources directly available to other network participants, without the need for centralized coordination by servers. Below figure provides a conceptual representation of the P2P overlay topology. In this, every machine plays the role of client and server at the same time. Although a P2P network has a number of advantages over the traditional client–server model in terms of efficiency and fault tolerance, additional security threats can be introduced. Users and IT administrators need to be aware of the risks from propagation of malicious code, the legality of downloaded content, and vulnerabilities within peer-to-peer software. Security and preventative measures should be implemented to protect from any potential leakage of sensitive information and possible security breaches.

A. Computation of NTRM
We make the following assumptions. Peers are equal in computational power and responsibility. There are no privileged, centralized, or trusted peers to manage trust relationships. Peers occasionally leave and join the network. A peer provides services and uses services of others. Consider three different types of service like default, congestion and free bandwidth. Using these services we are sending packet to destination using peer to peer system. Computation Of Service consider three type of service in this implemented work to compare which one service is good one to forward the packet. After using these services we will get which one is better. So finally we choose free bandwidth because it takes less time to forward the packet when compare to other two methods. Service value is computed by Service taken by transaction Service Ratio = Specific service value. Service value is constant when service is default and service value is reduced when service is congestion and service value is increased when service is free bandwidth so better one is free bandwidth.

B. Computation of Trust
Each peer stores its trust information based on past interaction. User need to check the trust information before next interaction and Peers contains the trust information about other peers. Trust value will be reducing when packet modifies by attacker in peer to peer system. Trust value is constant when there are no changes in forwarded packet. Trust value is calculated by 1

\[ \text{Trust Ratio} = x \times \text{specific trust value} \]

stored by value Past interaction

C. Computation of Peer Trust Ratio
The main important task is to compute trust ratio of peers and compute trust ratio using service and trust values. A peer selects the next adjacent peer which is having highest trust ratio. Trust ratio of peer is calculated by

\[ \text{Service Ratio} + \text{Trust Ratio Peer} \]

Trust Ratio = Peer Total Transaction

Algorithm Steps:
1: Assign the values Service=5, Trust=10
2: Compute the Trust Ratio of each peers based on past interaction using service and trust values.
3: If there is no transaction then trust ratio is same as trust value.
4: If there is a transaction then need to compute trust ratio of peers using service and trust values.
5: Display the trust ratio of peers in each peer groups.
6: Select the maximum trust ratio of the peer to transmit the packet.
7: Send the message from the sender
8: Exit.

D. Eigen trust
This is distributed algorithm to decrease the number of downloads of inauthentic files in a peer-to-peer file sharing network that assigns each peer a unique global trust value, based on the peer’s history of uploads. Eigen Trust model is designed for the reputation management of P2P system. The global reputation of each peer i is marked by the local trust values assigned to peer i by other peers, and it is weighted by the global reputation of the assigned peers. For normalizing local trust value Cij, the definition is as follow: Si j is meant for each peer enable to store the number satisfactory transactions it has had with peer j, and it is also meant for the number of unsatisfactory transactions it has had with peer.

IV. PROPOSED SYSTEM
In this paper, the following assumptions are considered for the proposed system:

• Peers have equal computational power and responsibility.
• There are no privileged, centralized, or trusted peers to manage trust relationships.
• Peers occasionally leave and join the network.
• A peer provides services and uses services of others.
• For simplicity of discussion, one type of interaction is considered in the service context, i.e., file download.

**Preliminary Notations**

Pi denotes the ith peer. When pi uses a service of another peer, it is an interaction for pi. Interactions are unidirectional. For example, if pi downloads a file from pj, it is an interaction for pi and no information is stored on pj. If pi had at least one interaction with pj, pj is an acquaintance of pi. Otherwise, pj is a stranger to pi. Ai denotes pi’s set of acquaintances. A peer stores a separate history of interactions for each acquaintance. SHij denotes pi’s service history with pj where shij denotes the current size of the history. shmax denotes the upper bound for service history size. Since new interactions are appended to the history, SHij is a time ordered list.

![Figure 1. Operations between the Peers](image1)

**Network Architecture**

Downloading a file is an interaction. A peer sharing files is called an uploader. A peer downloading a file is called a downloader. The set of peers who downloaded a file from a peer are called downloaders of the peer. An ongoing download/upload operation is called a session. A good peer uploads authentic files and gives fair recommendations. A malicious peer (attacker) performs both service and recommendation-based attacks. Four different attack behaviors are studied for malicious peers: naive, discriminatory, hypocritical, and oscillatory behaviors. A non-malicious network consists of only good peers. A malicious network contains both good and malicious peers.

![Figure 2. Proposed NTRM Architecture Diagram](image2)

NTRM 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. Assume that pi wants to get a particular service. Pj is a stranger to pi and a probable service provider. To learn pjs’ reputation, pi requests recommendations from its acquaintances. Assume that pk sends back a recommendation to pi. After collecting all recommendations, pi calculates rij. Then, pi evaluates pks’ recommendation, stores results in RHik, and updates rtik. Assuming pj is trustworthy enough, pi gets the service from pj. Then, pi evaluates this interaction and stores the results in SHij, and updates stij. One peer is marked as trusted by NTRM and if it is turned off from network, there is a possibility to another malicious peer takes its position and act as trusted peer. This can be avoided by the Auto update mechanism.

**V. 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. The parameters like own experience, information from its acquaintances, and level of confidence in the recommendation provided us a better assessment of trustworthiness. Individual, collaborative, and pseudonym changing attackers are studied in the experiments. Damage of collaboration and pseudo spoofing is dependent to attack behavior. Although recommendations are important in hypocritical and oscillatory attackers, pseudo spoofers, and collaborators, they are less useful in naive and discriminatory attackers. NTRM mitigated both service and recommendation-based attacks in most experiments. However, in extremely malicious environments such as a 50 percent malicious network, collaborators can continue to disseminate large amount of misleading recommendations.
Another issue about NTRM is maintaining trust all over the network. If a peer changes its point of attachment to the network, it might lose a part of its trust network. This issue might be studied as a future work to extend the trust model. Using trust information does not solve all security problems in P2P systems but can enhance security and effectiveness of systems. If interactions are modeled correctly, NTRM can be adapted to various P2P applications, e.g., CPU sharing, storage networks, and P2P gaming. Defining application specific context of trust and related metrics can help to assess trustworthiness in various tasks.

VI. FUTURE ENHANCEMENTS
Peer-to-peer (P2P) systems, peers often must interact with unknown or unfamiliar peers without the benefit of trusted third parties or authorities to mediate the interactions. A peer will need reputation mechanisms to incorporate the knowledge of others to decide whether to trust another party in P2P systems. This paper discusses the design of reputation mechanisms and proposes a novel distributed reputation mechanism to detect malicious or unreliable peers in P2P systems. It illustrates the process for rating gathering and aggregation and presents some experimental results to evaluate the proposed approach. Moreover, it considers how to effectively aggregate noisy (dishonest or inaccurate) ratings from independent or collusive peers using weighted majority techniques. Furthermore, it analyzes some possible attacks on reputation mechanisms and shows how to defend against such attacks.

REFERENCES

BIOGRAPHY
M. Ruby has received her Btech degree from Vizag Institute of Technology. She is currently pursuing her Mtech degree from Vignan’s Institute of Information Technology, Visakhapatnam. Her areas of Interest are Computer Networking, Network Security.

Dr. Koduganti Ventakarao is working as Professor Vignan’s Institute of Information Technology, Visakhapatnam. He has experience for over 20 years in Teaching fields. He has published 30 papers in his area of expertise. His areas of interest are Security and Cryptography, Parallel Computing and Grid Computing.