IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 3, Ver. II (May.-June. 2017), PP 34-40
www.iosrjournals.org

Detecting Malicious Peers with Past Behavior and Identifying Absolute Trust Peers in P2P Networks

Navaneetha.M[1], Dr. M.ShivaKumar[2]
[1]*Assistant Professor/Department of CSE/CMRIT/Bangalore/Karnataka/india*
[2] *Professor/ Department of CSE / PNSIT/Nelamangala/Karnataka/india*

Abstract : *Peer-to-peer (P2P) computing or networking is a distributed application architecture that partitions tasks or workloads between peers. The peers evaluate other peers based on their past interactions and then aggregate this information in the whole network. However it may not be the true reflection of past behavior of the peers. Moreover such type of aggregation gives only the relative ranking of peers without any absolute evaluation of their past. This is more significant when all the peers responding to a query, are malicious. In such a situation only the peer came to know that who is better among them without knowing their rank in the whole network. Hence to mitigate the attacks by malicious peers and to motivate the peers to share the resources effectively and securely, in this paper, a new algorithm is proposed which accounts for the past behavior of the peers and will estimate the absolute value of the trust of peers. Consequently, good peers or malicious peers are identified. The proposed algorithm converges at some global consensus much faster by choosing suitable parameters. Because of its absolute nature it will equally load all the peers in network. It will also reduce the inauthentic download in the network which was not possible in existing algorithms.*
Keywords: *Peers, P2P, Malicious, SORT, aggregation.*

I. Introduction

Peer-to-peer (P2P) networking is a distributed application architecture that partitions tasks between peers. Peers are equally privileged, equipotent participants in the application. Distributed Networking is computing network system, said to be "distributed" when the computer programming data worked on more than one computer implemented over a network. Network is a group of two or more computer systems linked together. In network topology, security is considered as one of the critical parameter. Network uses the client-server model to perform any task.P2P is a type of network in which the nodes act as both the client and server where communication can be made from any peer whereas it differs centralized client-server model client nodes request a servers for resources. P2P network depends on the collaboration of nodes to perform the tasks and classified into two types as structured and unstructured [6].

Every peer in p2p network can initiate the communication and has equal responsibility. But due to lack of functionality of central control, some peers can easily sabotage the network by putting inauthentic contents in the network. Such peers are called malicious peers. Furthermore, rational behavior encourages the peers only to draw the resources from network without sharing anything. These types of peer are called free riders [11]. In this paper, metric and an aggregation algorithm is proposed which truly capture the past behavior of the peers. The proposed aggregation algorithm does not require any kind of normalization. It is purely decentralized and does not require any kind of central authority or pre-trusted peers. By [11] the Absolute Trust is based on the concept of weighted averaging and scaling of local trust.

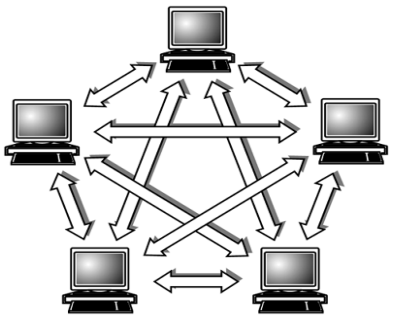


Fig.1 Peer to Peer network

In reputation systems, all the peers evaluate the other peers, based on the past interactions and assign them some trust value, also called local trust value. These local trust values are basic information, which are aggregated in whole network to form the global reputation of the peer. This aggregation process is different for

structured and unstructured p2p network. The interactions are evaluated based on the weight, recentness and satisfaction. The recommendation is used to calculate the feedback of a peer by a trusted peer. These interactions and recommendations are stored in a separate history. By [7] service trust metric is concerned with the evaluation of trustworthiness of the acquaintances on the basis of service they provide. To evaluate this, a peer needs to calculate two parameters: competence belief and integrity belief values. These parameters are evaluated under two criteria's: based on the service and based on the recommendation.

1.1 Organization of This Paper

The remainder of this paper is organized as follows. In Section II, literature review followed by the summary. The related work and comparison table is described in Section III**.** We present our proposed architecture in Section IV and in Section V conclusion of this paper. Section VI includes further enhancements.

II. Literature Review

In [5] Peer to peer network is network composed of heterogeneous and autonomous peer that cooperate with each other in decentralized manner. All peers are both users and providers of resource. SORT (Self Organizing Trust Model) algorithm used to decrease malicious activity by establishing trust in peers. Each peer develops its local view of trust by past interaction of peer. Using this, good peer form Dynamic trust group and isolate malicious peer. Peer do not tries to collect trust information from other peers. SORT does not provide trust all over the network, in case of changes its point of attachment to the network. Reputation management system is used to overcome free riding in peer to peer network. Resource allocated for the system seems to better way because node does not have very good reputation about other peer. But peer may serve at least some amount of resources with finite probability .This avoids disconnection among peers. This algorithm optimal shared capacity and does not support when nodes more than actual demand by [2].

From [3] Reputation aggregation in peer to peer networks is generally time and resource consuming process. A peer will not have same reputation in the network. In reputation aggregation network, a variant gossip algorithm is used. It is also called as differential gossip. The estimation of reputation is done for every peers and information is received from immediate neighbor. The tendency of peer to draw resource from the network but not sharing anything in return is called free riders, the major problem. The free riders are overcome by Gossip algorithm. The differential gossip algorithm is used for spreading information among decentralized network and randomly chooses their communication peer partners. Push, pull and Push Pull are the ways to perform Gossip algorithm. The issue is considering only the feedback of trusted node with higher weight.

In [1] Reputation systems provide a mechanism to reduce risk such as security and operational by building trust relationship and identifying malicious peer. The reputation model is so called flow based model .The system is based on ranking only without absolute values. This makes the system to determine whether peers are actually trustworthy or untrustworthy. The flow based reputation metric gives only absolute value instead of merely a ranking both analytically and numerically based on their past interaction. Computing absolute reputation values makes it possible to quantify trustworthiness of peer. In this paper the methods used are Eigen trust, page rank, SALSA and peer trust. The flow models are based on theory of Markov chain. The feedback provided by the users is aggregated and normalized in order to obtain a Markov chain. Markov steps are applied until stable state is reached. Metric depends on parameters values 1. Pattern matrix (indirect evidence matrix) stores the feedback. 2. Starting reputation vector provides direct information to the network about trustworthiness.

By [4] malicious attacks in reputation based system are minimized. System collects the feedback from peers to improve the fidelity and to estimate honesty. Central server is preferred to store and manage trust. The peer system creates a secure structure of file based on the IP address of transmitter and receiver and so on. The secure transmission is only opened for peer beneficiary peers. Secure transmission is done based on Blow fish algorithm which is not based on past interaction. Blow fish algorithm has two parts (1) key expression, (2) data encryption. In DHT approach, each peer becomes trust holder for storing feedback. Global trust information are stored by trust holders and accessed through DHT. A peer sends trust queries to learn trust information of other peers. Secure file structure is introduced in this system for establishing faith relationship. Good peers form faith group. This method saves the files from intruders and hackers. Trust is a social concept and hard to measure using numerical values.

From reference [6] it provide security in P2P self-organizing trust model is proposed. Trustworthiness of peers is calculated based on past interaction and recommendations. The interactions and recommendations are evaluated based on importance, recentness, and satisfaction parameters. By this the good peers form trust relationship in proximity and avoids malicious peers. The interactions are evaluated based on the weight, recentness and satisfaction. The recommendation is used to calculate the feedback of a stranger by a trusted one. These interactions and recommendations are stored in a separate history. For storing the feedback distributed hash table (DHT) approach is used. Metrics are evaluated using service trust metric, reputation trust metric,

recommendation trust metrics and then peers selects the service provider to get needed service. A good peer provides authentic files and an attacker can perform one of the processes such as Naïve, Discriminatory, Hypo critical and oscillatory. Another type of attacker is called pseudo spoofs. The security provided by this method may not provide solution for all the security problems.

In [8] Peers create own trust network by using local information that are available but does not try to learn global trust information. SORT is a technique is used to establish trust relationship among peers. Trust information is based on service and trust values based on past interactions. This trust information helps to build a secure environment to transmit a packet. In general, trust information computation is not global hence it does not reflect opinions of all peers. In attacker model, the analysis is done on individual attackers by creating network topology. The network topology is tested with four trust calculation methods. They are No trust, No reputation query, SORT and Flood reputation query. Every time peer need to ask server for which peer is to be selected for next interaction so it takes lot of time and bandwidth wastage. If server got failure then all the information about the peers could be lost. The major problems of service providers are openness and search in P2P. Any peers can join network at any time so the malicious peer intrudes. To select the best service provider there is no efficient search mechanism. But only trust metric is evaluated and relationship is constructed among peer. Trust is measured for particular peer by service providers and recommendation is collected from a peer about another peer. Then malicious peer separated from good peer. The parameters used in trust metrics are satisfaction measure, importance and fading effect. The metrics used are service, recommendation and reputations from [7].

In [10] Nature of peer to peer system exposes themselves to malicious activity. Building trust can mitigate malicious peer attack. Distributed algorithm is enabled for trustworthiness of peer based on past interaction and recommendations. 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. Peers can provide a more secure environment by reducing risk and uncertainty in future P2P interactions. 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. Here trustworthiness is a major challenge while feedbacks contain deceptive information.

In [9] Distributed algorithm is used by peers by peers to know about trustworthiness based on past interaction. The trust peer upload reliable files and gives true recommendation. The malicious peer also performs both service and recommendation based attacks. A service based attack is uploading virus infected or inauthentic files. Self-Organizing Trust Model (SORT) detects the service based attack and recommendation based attack. If one peer wants to upload/download file from another peer means peer will send the query to peer interacted in the past to learn the trust information of other peers. This model mitigates sixteen different malicious attacks. Peers create their self-trust network in their nearness by using local information available and do not try to learn worldwide trust information. Metrics should have precision so peers can be ranked according to trustworthiness. Queries are answered by point to point system.

By analyzing pseudo spoofs, the two effects (1) it clear bad history which increases malicious attacks[2].Peer become more isolated from good peers which decreases malicious attack. Here pseudo spoofs behavior is avoided. P2P overlay networks do not arise from the collaboration between established and connected groups of systems and without a more reliable set of resources to share. Finally P2P network, malicious peer attacks needs to be mitigated. The motivation of peers to share the resources should be encouraged. The aggregation process in the reputation system is done based on the past interaction. Aggregation provide ranking for the peers in the network based on the information obtained from past. The ranking system for the peers is similar to random surfer model. The distributed aggregation algorithm is used to evaluate the global trust value of peers by collecting the local trust from different peers. This aggregation can be done either by Gossiping protocol or by taking feedback only from few significant peers. In true sense feedback from only few peers does not make the global trust.

2.1 Summary

From the above literature survey, the malicious peers and the free riders are the issues in the peer to peer systems. This can be overcome by ranking method based on past interaction of the peers. Any peer can initiate the communication as the network is decentralized. The Blow fish algorithm collects feedback from peers but does not depends on past interaction. SORT algorithm is done based on past interactions and DHT is used for storage. Using this algorithm, malicious peers are isolated by forming trust group. The differential Gossip algorithm in which files are uploaded through which inauthentic content is identified and ranking is provided. Finally, the efficient algorithm used to ignore malicious peers and free riders is Absolute trust. In this algorithm peers are evaluated based on their past interaction and ranking is provided. It also calculates the local trust and global trust value is used to reduce the inauthentic downloads in P2P network.

III. Related Work

Reputation system which is used in the e-commerce environment should establish the trust among the buyers. In e-commerce environment there is no presence of central authority hence it has only to record the past experience of buyers. The feedback collected in the presence of central authority network is easy but in distributed network it is difficult task. DHT is used for the efficient location of trust holder peers in structured network. In unstructured network global trust is calculated from local trust. The calculation of global trust needs to wait for feedback obtained from some limited number of peers. Feedback is done based on gossip algorithm using metric. The trust worthiness is calculated from weighted average of local trust and feedback from few peers.

From the above literature review, the methodologies of various peer to peer systems are identified. The comparison of methodologies with the parameters are evaluated and represented in tabular form. The comparison table 1: parameter comparison clearly shows the efficiency of algorithms for parameters such as security, robustness, scalability, authentic contents, trustworthiness of peer and finally system effectiveness. From table, Absolute trust algorithm is more secure, robust and scalable. In this algorithm good peers provide authentic files and right feedback and malicious peers provide inauthentic and wrong feedback. Hence, trustworthiness of P2P network is measured using local and global trust value.

IV. Proposed Architecture

Absolute trust is the proposed algorithm in which metric values are calculated and feedback is obtained. The aggregation algorithm is used here to capture the past behavior of peers. Initially local trust values are calculated using raw data or information and using local values global trust values are estimated among peers. These values are stored and based on their past interactions, ranking is provided to each peer in peer to peer network.

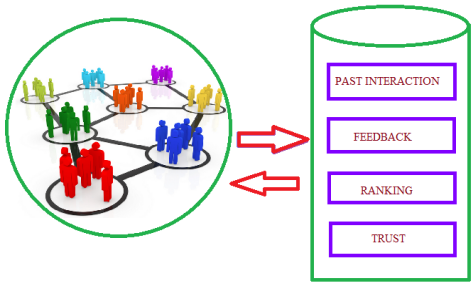


Fig. 2 P2P with Absolute Trust Model

The block diagram for above architecture as follows. In which source and destination peers are identified. The P2P network has servends where each peer in the network can act as both client and server. Initially when a peer request for the resource in the network any peer responds to the query which is initially stored in the Dynamic Hash Table (DHT). DHT is used for efficient location storage to hold trust peers. Each data is temporally stored in the cache and present in the data server. The resources searched by the source peer is obtained as a source file from other peers in the network and shared on the network through the data servers and given to the DHT. The information needed by the source peer is downloaded from data server. All peers in the network can download the resources and each peer is further evaluated to verify whether the peer is good or malicious one. For further evaluation past interactions made by the peers are consider to provide ranking for peers. The feedback is essential part in the network, which is collected from each and every peer to know which peer is better among them. The trust is calculated in two ways by calculating the local trust and global trust value. To calculate global trust value peers has to wait for the sometime to obtain feedback.

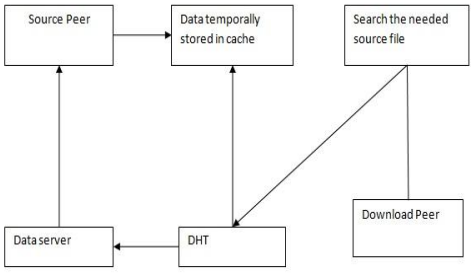


Fig. 3. Block Diagram

4.1. Modules and Module Description

- Past behavior
- Feedback
- Ranking
- Trust

Past Behavior - P2P is a decentralized network in which any peer can initiates the communication. Peer acts as both client and server. Peers in P2P network are resource providers and every interactions made is stored. The interactions such as resource sharing, asking queries is termed as past behavior. The metric and aggregation algorithm is used to evaluate the past behavior. Past behavior is modeled as trust.

Feedback-Feedback is collected among the neighbor peers about a peer. It is based on the past interactions made in P2P. It is to evaluate the peers whether it responds to query or only draw the resources shared. The peers that only draw resources from the network are known as free riders. Feedback is aggregation of information which is evaluated from peers. Each peer evaluate other peers for collecting local trust values to form global trust value. The different peers are evaluated using Distributed aggregation algorithm. This aggregation can be done either by using Gossiping protocol or by taking feedback.

Ranking-Rank is given to all peers that take place in the network. Ranking is provided based on peer's past interactions and feedback. The good or malicious peers are identified by ranking ie., which peer is better among the peers. Aggregation algorithm only gives ranking of peers and doesn't provide any absolute value. It only tells us which peer is better among them in P2P network. Ranking helps to find inauthentic downloads from peers using probabilistic approach.

Trust- Trust values are aggregation of the information about the peers based on the ranking. Absolute trust algorithm is based on concept of weighted averaging and scaling local trust. Absolute trust equally loads all the peers in P2P network. Trust values should be calculated recursively and any changes made in peers then immediately local trust values gets updated. This reduces inauthentic contents.

V. Trust Model

In P2P network, peers only exchange the files as the resources. The trust values is calculated from the individual peers and aggregated in the whole network. Local trust is the basic trust metric, which is the raw data used for calculation of global trust in the network. Local trust can be classified as satisfied and unsatisfied and it is calculated based on the amount of interactions, date of transactions and number of transactions. For free riders information aggregation is alone focused in the network. Evaluation can be done by three ways such as one-to-many, many-to-one, one-to-one. In one-to-many evaluation one peer evaluates all peers and in many-to-one many peers evaluate one peer. In one-to-one evaluation one peer evaluates another peer, this evaluation is meant to be uniform because it is done only by one peer.

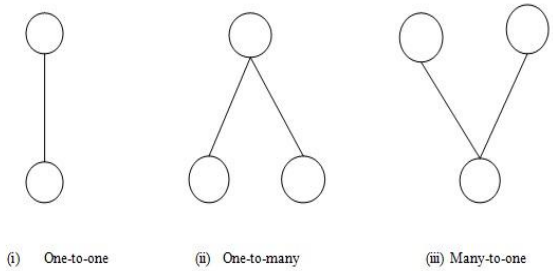
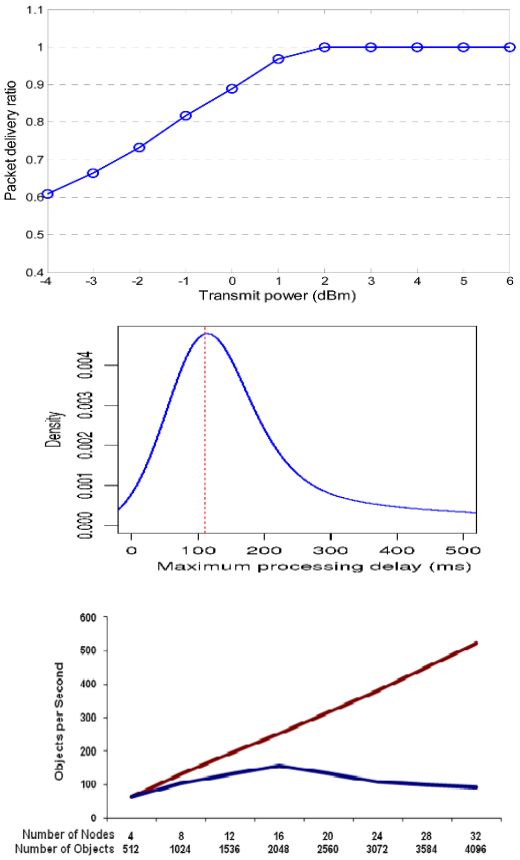


Fig. 4 Trust models

VI. Experimental Analysis and result

4.1 Number of nodes Vs PDR, Delay & Throughput

The following graph analyse the ratio between the number of nodes with PDR, Delay and Throughput. The calculation of Packet Delivery Ratio (PDR) is based on the received and generated packets as recorded in the trace file. In general, PDR is defined as the ratio between the received packets by the destination and the generated packets by the source. Packet Delivery Ratio is calculated using awk script which processes the trace file and produces the result. Throughput is the number of successfully received packets in a unit time and it is represented in bps. Throughput is calculated using awk script which processes the trace file and produces the result. Energy based routing is the important routing functionality required by network. Energy of the node is considered while selecting the router to balance the energy consumption of the network.



VII. Conclusion

In this paper, an algorithm for aggregation of local trust in peer-to peer network is proposed that satisfies all design considerations mentioned in the introduction namely avoiding malicious peer and free riders. In Absolute Trust algorithm, aggregation is done without normalization, hence it provides the feedback of the peer based on their past behavior. The calculation of global trust is done recursively and it converges at some unique value. The updates have to be sent only in case of change of local trust value. So, lesser number of messages is required to update the global trust. This algorithm can be implemented in truly distributed system where no central authority is present. This algorithm shows that it is robust against the various attacks like individual malicious, unpredictable malicious and collective malicious. Distribution of load is even on individual good peer and more uniform compared with relative ranking mechanism.

VIII. Further Enhancement

In this paper, The Metric based aggregation algorithm is proposed for finding malicious peers and free riders. However the algorithm is limited only to malicious attacks, further the same algorithm with additional metrics can be used to find the various attacks like Sybil, DOS and SQL injection attacks. Since, the algorithm holds the metrics like past behavior, feedback and trust values of peers, it can also be used to resolve the intruder attacks in p2p networks.

Table 1: Parameter Comparison

Methodologies/ Parameters	**Security**	**Robustness**	**Scalability**	**Authentic**	**Trust**	**Effective**
Flow based reputation[1]	Nil	High	Nil	Nil	Difficult to determine	Effective
Differential Gossip algorithm [3]	Medium	High	Nil	Nil	Low	Nil
Blow Fish algorithm[4]	High	Medium	Medium	Nil	Increase trustworthy	Effective
SORT [5][6][8][10]	Enhance security	Low	High	Inauthentic	Difficult	Effective
Distributed algorithm [9][10]	Low	High	High	Authentic	Trustworthy	Effective
AbsoluteTrust algorithm [11]	High	High	High	Authentic	Trustworthy	Effective

Reference

[1] Antonino Simone, Boris Skori and Nicola Zannone, "Flow based reputation: more then just ranking", International Journal of Information Technology and Decision Making, November 2011.

[2] Ruchir Gupta, Yatindra Nath Singh," A Reputation Based Framework to Avoid Free-riding in Unstructured Peer-to-Peer network",IEEE Transaction, July 2013.

[3] Ruchir Gupta and Yatindra Nath Singh," Reputation Aggregation in Peer-to-Peer Network Using Differential Gossip Algorithm",IEEE Transaction, January 2014,

[4] Kayalvizhi and Bharathi, "Efficient and distributed network model for P2P systems", International Journal of Computer Science and Mobile Computing, Vol. 3, Issue.2 , February 2014,pg.626-632.

[5] R. Gayathri and V.Vaishnavi,"Secure shell transfer through malicious nodes from peer to peer", International Journal of Advanced Information and Technology,Vol.21, No. 21, January 2014.

[6] G. Samuvelraj and N.Nalini," Avoiding malicious activities in peer to peer systems using SORT method", International Journal of Engineering Research and Technology, Vol.3,Issue.3, March 2014.

[7] S. Nithya and Dr. Kannan Balasubramanian," Trust Metrics Evaluation for Peer-to-Peer Systems", International Journal of Advanced Research in Computer Science & Technology, Vol. 2 Issue Special 1 Jan-March 2014.

[8] M.Mamatha and E. Chitti Babu,"Building trust relationship among peers using SORT", International Journal of Scientific Engineering and Technology Research, Vol.3,Issue.22, October 2014.

[9] I. Narasima Rao, K.Vineela and J.V.S.Arundhati ," A trust model for node to node system using DHT", International Journal of Advanced Technology and Innovative Research,Vol. 7,Issue.5, June 2015, pg: 0612-0621.

[10] Vasu Deva Rao and Laxmikanth,"SORT: Self Organising Trust Model for P2P systems", International Journal and Magazine of Engineering , Technology, Management and Research,Vol. 2,Issue 11,November 2015.

[11] Sateesh Kumar Awasthi and Yatindra Nath Singh," Absolute Trust: Algorithm for Aggregation of Trust in Peer-to- Peer Networks", IEEE Transaction, January 2016.

Author(s) Profile

Navaneetha.M, Assistant Professor, Department of CSE, CMR Institute of Technology, Bangalore. Her area of interest is Computer Networks & network security and had published many papers in national and international journals.

Dr M.Shivakumar, Professor, Department of Computer science and Engineering, PNSIT, Nelamangala. Obtained doctoral degree in Network Security. His area of interest is Image Processing and Network Security, he has published many papers in both National and International Journals and Conferences.