OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

Detection of Malicious Nodes based on Reputation system In Peer to Peer

[1]Nishant Kumar Jha , [2]Asst.Prof.D.D.Gatade

[1]Department of Computer Engineering, Sinhgad College of Engineering, Pune , India.
[2]Department of Computer Engineering, Sinhgad College of Engineering, Pune India.

ABSTRACT:- As of late, Peer-to-Peer (P2P) record sharing frameworks for the Internet have picked up quickly expanding fame. In the meantime, more than 70% of the activity in the foundation of the Internet is created by such P2P network. In a distributed (P2P) network, since every associate needs to take an interest in transferring information to different companions, pernicious companions might transfer counterfeit information in order to harm the playback and corrupt the execution of ordinary companions in the network. This is known as contamination assault in P2P systems, and it can bring about unforgiving effect to the execution of P2P gushing network. This paper represents proposed system which will calculate the reputation of the peers based on the quality of service it provides to other peers. The system will also address the issue of recalculating of reputation for a relocated peer.

Keywords:- Peer to Peer; Reputation Algorithm; Malicious nodes; Pollution attack; Reputation system ; recommendation algorithm

I. INTRODUCTION

Open nature of peer-to-peer systems exposes them to malicious activity Building trust relationships among peers can mitigate attacks of malicious peers. Peer-to-peer networks (P2Ps) enable the sharing of globally-scattered computer resources, allowing them to be collectively used in a cooperative manner for different applications such as file sharing , instant messaging , audio conferencing , and distributed computing . P2P applications scale to a large community of users and take full advantage of heterogeneous resources widely scattered all over the world. Node cooperation is critical in achieving reliable performance of P2Ps. However, cooperation is challenging in P2Ps, where many diverse and autonomous parties without preexisting trust relationships work together. In Peer to Peer , due to lack of central management, they are severely threatened by a variety of malicious users in todays Internet. 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. Due to presence of malicious activity in network, there is huge degrade in QOS i.e quality of service of different peers. As in this type of network, the basic scenario is uploading and downloading of data and suppose some peers in that network act as a malicious nodes i.e not behaving like a trustworthy nodes, then there is highly degradation in performance and QOS, because of which goal of legitimate nodes is not accomplished Peer-to-peer networks (P2Ps) use reputation systems to provide incentives for nodes to offer high quality of service (QoS) and thwart the intentions of dishonest or malicious nodes. As of late, Peer-to-Peer (P2P) document sharing frameworks for the Internet have picked up quickly expanding fame. In the interim, more than 70% of the movement in the foundation of the Internet is created by such P2P network. The significant favourable circumstances of P2P components contrasted with customary customer/server instruments lie in the expanded versatility for supporting a great many clients and additionally accomplishing more trustworthiness through decentralization. Then again, the P2P idea is confined on record sharing, as well as be sent for decentralized coordination and correspondence in an assortment of other disseminated applications. P2P system is helpless against different assaults because of the presence of noxious hubs which don't agree to the system convention to accomplish their own particular purposes. In a shared (P2P) spilling framework, since every companion needs to take an interest in transferring information to different companions, malignant associates might transfer fake information to harm the playback and corrupt the watching background of typical associates in the framework. This is known as contamination assault in P2P systems, and it can bring about extreme effect to the execution of P2P spilling frameworks. The accomplishments of a few business P2Pstreaming items, have exhibited that P2P spilling is a promising answer for effectively circulating live video streams at a huge scale. Be that as it may, the above issue of malignant companions are spurring the scientists to discover the system or some structure to overcome from this issue as it is picked up quickly expanding prevalence as of late.

The paper is organized as follows: Section 1 Introduction to the project topic. Section 2 literature review related to the project topic and motivation behind the project. Section 3 Programming strategies and Algorithm used for the proposed system. 4. discussion and results and Section 5 conclude the discussion.

II. RELATED WORK

X.Jin and S.-H. G. Chan [8] define that many network services consist of a large set of independent nodes, and these nodes are required to follow some rules to cooperate so as to achieve a given network functionality. To realize such network service, every node must communicate or provide local services with a subset of other nodes which are called neighbors, e.g., upload packets to neighbors, download packets from neighbors and forward packets for neighbors and so on. To guarantee the correct functionality of the network service such that every node can get service with desired performance, nodes must follow the predefined protocols when they participate in the communication with their neighbors. Ahmet Burak Can and Bharat Bhargava [1] proposed that a peer may be a good service provider but a bad recommender or vice versa. Thus, SORT 1 considers providing services and giving recommendations as different tasks and defines two contexts of trust: service and recommendation contexts. Information about past interaction and recommendations are stored in separate histories to assess competence and integrity of acquaintances in these contexts. SORT defines three trust metrics. Reputation metric is calculated based on recommendations. It is important when deciding about strangers and new acquaintances. 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. Q. Wang, L. Vu, K. Nahrstedt, and H. Khurana[5] propose a statistical scheme i.e MIS based on checksum and HMAC. The goal of this scheme is to track the origin of corrupted blocks. The correctness of the MIS scheme of identifying malicious nodes depends on the condition that no one can lie when reporting a suspicious node. HaiyingShen[3] defines many P2P streaming systems focus on improving streaming quality and assume that all nodes in the system cooperate as desired. However, this may not be true in the open environment of the Internet. Some nodes in the system may be selfish and unwilling to upload data to others. Some may have abnormal actions such as frequent rebooting, which adversely affect their neighbors. More terribly, some nodes may cheat their neighbors, launch attacks, or distribute viruses to disrupt the service. Ming-Chang Huang[4] proposed that Malicious peers may misbehave in several ways:

(i)They can modify the payload of a block.
(ii)They can lie when sending checks to the monitor node.
(iii)They can avoid sending checks to their monitor;
(iv)They can churn by alternating between connection and disconnection

The system consists of NP malicious peers: these peers join the swarm and follow the application level protocol for overlay organization and data exchange but they can intentionally modify the payload of blocks that are forwarded to their neighbors. The effect of this unpleasant action is to make invalid chunk reconstruction of the receiving peers thus preventing them from reproducing the original content. The architecture also comprises a set of NM trusted monitor nodes. The tracker assigns each peer to only one monitor node based on the chosen overlay-wide unique identifier: Assume that the peer identifier is an integer ip the tracker assigns it to the monitor whose identifier is equal to ip mod NM. It follows that a peer can only report its checks to the same monitor node for the whole duration of the video stream.As soon as a peer reconstructs a chunk it is assumed that it is able to detect if the chunk is polluted or not. If the chunk is polluted it is not shared with the peer neighbors and a positive check is sent to the monitor assigned by the tracker. On the other hand, a negative check is sent to the monitor upon reconstructing a valid chunk. A check contains the list of peer identifiers that uploaded blocks of that chunk and a binary flag to indicate a positive or negative outcome. Yongkun Li, John C.S. Lui[10] designed a fully distributed detection algorithm which can be executed by every good node to identify its malicious neighbors. The proposed model defined above is a simple attack model for small class networks, but what if there is a large class of networks, then the above architecture is not able to identify malicious nodes. So, to overcome from that problem the general and fully distributed detection framework is applied to identify malicious nodes so as to defend against malicious attack and this framework can be executed by every legitimate node so as to identify its malicious neighbors. AhmetBurak Can and Bharat Bhargava[1] proposed a SORT model based on reputation metric & recommendation metric. In that they define the different model and introduced different algorithm. One of the main algorithm was get recommendation algorithm.

III. PROPOSED SYSTEM

The idea of the reputation system is to compute and distribute the reputation scores for an set of articles (e.g. administration suppliers, administrations, products or elements) inside of a group or domains, in light of an accumulation of suppositions that different substances hold about the articles. The opinions are regularly gone as ratings to a reputation focus which utilizes a particular reputation calculation to progressively process the reputation scores taking into account the got evaluations. Substances in a group use reputation scores for choice making, e.g. regardless of whether to buy a particular service or good. An article with a high reputation score will typically pull in more business than an item with a low reputation score. It is subsequently in light of a legitimate concern for items to have a high reputation score.

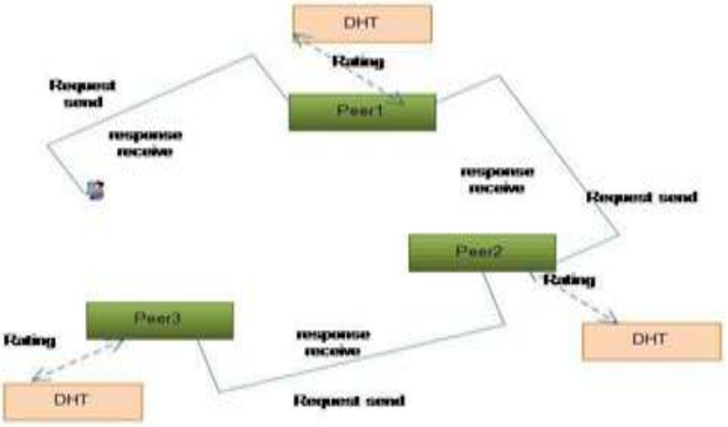

Fig 1. Architectural Diagram

Proposed System Flow & Algorithms:

There are different algorithms, which will be used throughout the process. It will overcome the previous Limitations.

Algorithm Name: Calculate Reputation Value (Node n)

```
If Not
1.      Naive Attack
2.      Discriminatory
3.      Delay
4.      Denial of Service
Return repudiation value = +0.1
Else    Return repudiation value = -0.1
```

Algorithm Name: Reputation Calculation for Peer-to-Peer System (N, G)

```
//N is number of nodes or peers in a network. G is number of Groups in the peer-to-peer network//
1.      Start
2.      For all nodes
3.       SET Threshold value of repudiation = 0.5
4.      Max Repudiation value = 1.0
5.      Min Repudiation value = 0.0
6.      A node checks for the data in its group Database
6.1.    If data is present in the group Database
6.1.1    If repudiation value responding node >= 0.5
A.      Request for the required data is send to the node having the data
B.       Request is served by responding node.
C.      Request node calculate repudiation value for the service
 Respond Node Repudiation = Calculate Repudiation Value (responding node)
D.       For request node the
New repudiation value of responding node
= repudiation + Respond Node Repudiation
```

```
a.      If  New repudiation value > Max Repudiation value
SET Respond Node Repudiation = Max Repudiation value
b.      Else If New repudiation value < Min Repudiation value
SET Respond Node Repudiation = Min Repudiation value
6.1.2   If repudiation value responding node < 0.5
It is treated as malicious node. And is not allowed to work

6.2     If data is not present in the Database of nodes of the group
6.2.1   The requesting node broadcasts the request to all the nodes of its group.
6.2.2   All the nodes broadcast the request to other groups they are connected with.
A. If data not found, no data found message is delivered to requesting node.
B.If data is found in some other group node then
a.      Repeat steps 6.1.1 to 6.1.2
C.If repudiation value of other node of other group >= 0.5
D
a.      Serve the request to requesting node of same group
Repeat steps 6.1.1 to 6.1.2
7.      End
```

Algorithm Name: Change of Peer for Peer-to-Peer System (N, G)

```
//N is number of nodes or peers in a network. G is number of Groups in the peer-to-peer network//
1.      Start
2.      Change peer in same group of same network
2.1     Node request to other node for change of neighbour
2.2     Requesting node sends its Repudiation value to other node.
2.2.1 If Repudiation value > 0.5
Requesting node cannot change neighbour
2.2.2   If Repudiation value > 0.5
a.Other node refers requesting node Repudiation value to the equitant.
b.If average of Repudiation value of Requesting node < 0.5
Requesting node cannot change neighbour
c.If average of Repudiation value of Requesting node >= 0.5
Requesting node becomes neighbour of other node.
3.Change peer in other group of same network
3.1Node request to other node for change of neighbour
3.2Requesting node sends its Repudiation value to other node.
3.2.1If Repudiation value > 0.5
Requesting node cannot change neighbour
3.2.2If Repudiation value > 0.5
a.Other node refers requesting node value with the nodes it is connected with, in requesting node group.
b.If average of Repudiation value of Requesting node < 0.5
Requesting node cannot change the group
c.If average of Repudiation value of Requesting node >= 0.5
C1.Connection with all nodes is lost for requesting node .
C.2 It becomes neighbour of other node of other group.
4.Stop
```

Description of Proposed System:

Proposed system of this paper basically focus on some issues i.e what if the service provider detach its attachment from exiting network and attach to new peer i.e it shifts its point of attachment to the new peer and form the network.Suppose in past the shifted peer had provided excellent services to all peers ,So, is it necessary to recalculate the reputation score or value of new shifted peer ? So the changes which this project will address are that it is not necessary to recalculate the reputation of new shifted peer. As in previous model, ratings where calculated by client side and stored it on its DHT, but after the point of attachment of server will change its rating may required in future. So instead of recalculating from starting, it is better to send back the server's ratings to server side. So it is necessary to stored ratings in both side i.e client as well as server side. fig 1 shows the flow of proposed system.

IV. RESULTS AND DISCUSSION

The proposed system will calculate the reputation of the peers based on the quality of service it provides to other peers. The system will also address the issue of recalculating of reputation for a relocated peer.The experimental results will show the effectiveness of reputation system, which will provide QOS by using proposed algorithm

V. CONCLUSION

Open nature of peer-to-peer systems exposes them to malicious activity. Building trust relationships among peers can mitigate attacks of malicious peers. Peers create their own trust network in their proximity by using local information available. This paper focuses on scheme which will be based on the reputation system and distributed algorithms that enable a peer to reason about trustworthiness of other peers based on past interactions and recommendations. This paper basically focus on the issues which are not taken into consideration while developing previous model. There are two contexts of trust, service, and recommendation contexts, are defined in this report to measure trustworthiness in providing services and giving recommendations. It also focuses some issues which will overcome in future like what happen when peer detach its attachment and join to new network. What about its previous reputation, Is it necessary to calculate its reputation from starting. Exiting reputation system doesn’t send the rating to the server side which may led to some problem when peer leave the network, So basically a new algorithm is developed to overcome form these issues.

REFERENCES

[1]. AhmetBurak Can, Bhargava, B., "SORT: A Self-ORganizing Trust Model for Peer-to-Peer Systems," Dependable and Secure Computing, IEEETransactions on , vol.10, no.1, pp.14,27, Jan.-Feb. 2013

[2]. HaiyingShen.; Liu, G.; Gemmill, J.; Ward, L., "A P2P-based Infrastructure for Adaptive Trustworthy and Efficient Communication in Wide-Area Distributed Systems," Parallel and Distributed Systems, IEEE Transactions on , vol.PP, no.99, pp.1,1,2013

[3]. HaiyingShen; Yuhua Lin; Ze Li, "Refining Reputation to Truly Select High-QoS Servers in Peer-to-Peer Networks," Parallel and Distributed Systems,IEEE Transactions on , vol.24, no.12, pp.2439,2450, Dec. 2013

[4]. Ming-Chang Huang,” Introduction to Two P2P Network Based Reputation Systems”978-0-7695-4696-4/12 © 2012 IEEE DOI 10.1109/ISBAST.2012.12

[5]. Q. Wang, L. Vu, K. Nahrstedt, and H. Khurana, “MIS: Malicious nodes identification scheme in network-coding-based peer-to peer streaming,” in INFOCOM, Proceedings IEEE,march 2010, pp. 1 –5, 2010

[6]. R,Gaeta.; Grangetto, M., "Identification of Malicious Nodes in Peer-to-Peer Streaming: A Belief Propagation-Based Technique," Parallel andDistributed Systems, IEEE Transactions on , vol.24, no.10, pp.1994,2003, Oct.2013

[7]. ShuzhenXu; Li, Mingchu; Chen, Yuanfang; Shu, Lei; Gu, Xin, "A cooperation scheme based on reputation for opportunistic networks," Computing, Management and Telecommunications (ComManTel),2013 International Conference on , vol., no., pp.289,294, 21-24 Jan. 2013

[8]. X. Jin and S.-H. G. Chan, “Detecting malicious nodes in peer-to peer streaming by peer- based monitoring,” ACM Trans. Multimedia Comput.Commun. Appl., vol. 6, pp. 9:1– 9:18, March 2010.

[9]. Y. Li and J. C. Lui, “Stochastic analysis of a randomized detection algorithm for pollution attack in P2P live streaming systems,” PerformanceEvaluation, vol. 67, no. 11, pp. 1273 – 1288, 2010

[10]. Yongkun Li; Lui, J.C.-S., "On detecting malicious behaviors in interactive networks: Algorithms and analysis," Communication Systems and Networks(COMSNETS), 2012 Fourth International Conference on , vol., no., pp.1,10, 3-7Jan. 2012

[11]. Ze Li; HaiyingShen; Sapra, K., "Leveraging Social Networks to Combat Collusion in Reputation Systems for Peer-to-Peer Networks," Parallel &Distributed Processing Symposium (IPDPS), 2011 IEEE International , vol.,no., pp.532,543, 16-20 May 2011