International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

Authentication of the P2P Network using the Aggregated Fidelity Score Method

M.S.Saranya, K.Thangadurai

Abstract: ***The most important issue in the P2P network is authenticating whether a network can be fully trusted before permitting full access and if the non-credible peers in a network gains access to the network it will actually cause lot of security related problems like man in the middle attack and denial of access attack. To overcome these attacks and to safe guard the peer network, a new fidelity based method is presented in this paper. The notion here is to calculate the loyalty score of the network based on the percentage of data delivered successfully and search time taken by the node and then if the score is higher than the permissible threshold value, the network is considered as a credible network and if the score is less, then the data on the network is blocked to ensure the curtail of the aforementioned attacks. The simulation results showcased that the proposed fidelity based approach is superior and performed with a high success rate and with less delay and drop rates.***

Index Terms:Peer to Peer network,aforementioned attacks, Fidelity based method, drop rate.

I. INTRODUCTION

The most important feature offered by the peer to peer network is its ability to serve several replica of the content and transmit it across the network on plethora of nodes. Even though this method has several advantages, the main limitation or the snag is the replica node will gain the authentication policies of the original node and there by integrity of the entire P2P network will be slashed and the replica nodes will usually be misused by publishing the wrong data files and unwanted data files which will be unnecessarily downloaded and utilized by the end users. The peer to peer system works differently unlike the contemporary client server models since each node has its own functionality and acts as a server and the key present in the network is used by all the nodes at the same time. The P2P system can be described as “It is a typical distributed system which has no centralized control and in every node the software are executed to carry out its functions without any lag”.

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author
M. S. Saranya, Department of Computer Science, Government Arts College (Autonomous), Karur (Tamil Nadu), India. E-mail: ms.saranya23@gmail.com.
Dr. K. Thangadurai, Assistant Professor and Head, Department of Computer Science, Government Arts College (Autonomous), Karur, (Tamil Nadu), India. E-mail: ktramprasad04@gmail.com

Since the peer to peer networks are generally constructed at the application layer and utilize the original network to transmit the data and messages is rightly called the overlay network. Primitive systems like Gnutella floods the data in the entire network and all the nodes in the system will deceive the data but since the data that is being transmitted has a delivery time within which it has to be delivered would pose a serious problem. As the time progresses the data which travels across every node will fade slowly and could not ensure that the transmitted data will reach the destination node. Besides this problem, the traffic congestion in the network will cause a severe hindrance and reduce the network credibility [J01].

A.PROBLEMS RELATED TO SECURITY

The peer to peer systems are completely dissimilar to the usual client server systems and this hinders the method of safeguarding the nodes using some predefined policies and administrators. The main part in security namely the authentication and the authorization is quite weak in the peer to peer systems and this will cause lots of security problems like spoofing the nodes and secret message will be intruded by the false nodes which will threaten the privacy of the nodes present in the P2P systems. This intrusion will permit the nodes prone to various attacks like man in the middle attack and denial of service attacks. The P2P systems are prone to some common attacks [M01] like worms, Byzantine faults, Eclipse attack and identity enforcement popularly called Sybil attacks.

II. RELATED WORKS

The author Mortazavi [M01] proposed a reputation based method which works on the co-operation levels of the user in the P2P system and delivered a better reputation to the peers.

The author Ruichuan Chen [R01] proposed an approach which relies on the trust of the peers and allows only the trusted peers to perform the desired actions by verifying the integrity of the content requestor and provide a reliable method to perform the transmission without any attacks.

The author Thomas Repantis [T01] proposed framework which consists of a middleware based on the trust, reputation and ad-hoc networks. The middleware acts as an agent to store the reputation information of each peer in its neighborhood peer and then self-organize the content and revert back the data to the concerned peer. The author Pathak [P01] proposed a public key authentication system to overcome the Byzantine problem in P2P systems and carried out their work by calculating the correct authentication in a majority of the group and labels them as trusted group. But this type of system is prone to Sybil attack.

The author MujtabaKhambatti [M02] proposed an economical and simple algorithm using role of each peers and then compute the trust relationship among the peers to solve the snags present in the previous methods.

B.QUALITY OF SERVICE BASED MODEL

The QoS parameters largely depends of the most important attributes related to the size, memory and speed of the network and it is enumerated clearly here under,

1. Transmission Speed of the peer
2. Memory size available in the peer
3. Accessing capacity of the peer

The peers are grouped according to the three attributes mentioned above and the frequently accessed contents are classified as CLASS A and the less frequently accessed contents are classified as CLASS B. The dense group which is frequently accessed (group with high speed, memory and accessing capacity) is routed hierarchically to implement Qos based topology.

Here an algorithm is needed to find the optimum route to transmit the content and a new route discovery algorithm is used to determine where the requested content is present. The main aim of the routing algorithm is to reduce the communication cost related to speed, memory and access cost. The routing algorithm comprises of the following fields namely,

1. Peer ID (PID)
2. Query ID (QID)
3. Number of Queries (NOQ)
4. Result (R)

Let us consider that a peer forwards a query Q to its neighbors, initially the node N1 assigns a rank to each of its neighbors based on their profile and to calculate the rank of the each node, then the node ranks are compared and the resultant is obtained from the following formula,

$$\text{Rank (Ni, Q)} = \sum_{i=0}^{m} R(N, Qi)^{\alpha}$$

h

ere R is the number of result obtained for the node N for query Qi and the node with higher number of results has a higher rank that is summed for all the results as shown in the above formula. The power value present in the formula is used to provide more weightage to the ranked nodes as the power value is set to 1, all the queries in the nodes are uniformly counted and if the power value is set to zero, the query which provides the results alone is counted whereas the rest of the queries are omitted.

The working of the ranking is enumerated here in this section. When a request is made, the peer checks its own data and confirms the presence of the content data. If the data is not present in its own archive, the peer forwards the request to the denser group.

The denser group receives the request and reverts back with an acknowledgement packet to the requestor to confirm that the request is received by the group. The acknowledgement packet will contain the time at which the request is arrived and the weightage or priority of the request.

The requestor receives the acknowledgement packet from the denser group and selects the best peer with the highest rank by applying the ranking formula shown previously.

The request peer then checks the reputation of the best peer using fidelity score described in the FidelityScore algorithm. The best peer receives the conformation packet and then the data is delivered without any lags.

C. PROPOSED FIDELITY SCORE MODELS

Most of the present approaches are based on identifying the trust of the peer present in the peer to peer network. The proposed fidelity score algorithm initially validates the trustworthiness of the peer before the data is either transmitted or received. To accomplish this, fidelity index corresponding to the data delivered successfully and time taken to deliver the data is found as shown in the following section.

FI = (DSD / DT) x TNR

Where DSD is the data successfully delivered, DT is the delivery time taken and the TNR is the total number of request made by the peers.

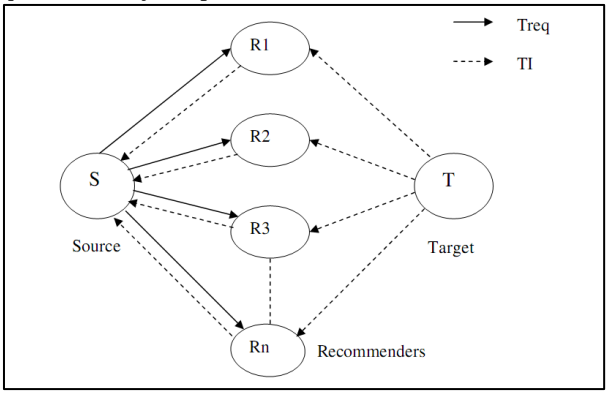

Fig.1. Calculating the fidelity using the recommenders in P2P networks

From the Fig.1, the aggregated fidelity index AFI value is calculated for all peers and it is found to be,

$$\textbf{AFI} = \sum_{i=1}^{n} \boldsymbol{FIi}$$

The source sends a request and the recommenders R1, R2,…Rn sends their recommendations to the source and the individual peer fidelity index is computed and sent to the source. This FI is used to calculate the AFI as shown in the Fig.1.The aggregated FI determines two levels AFI(L) the lower limit and AFI(U) the upper limit. Any values below this AFI(L) is regarded as non-loyal peers and no traffic is passed through them and no data is accepted or transmitted. The peer AFI values which are in the range between AFI(L) and AFI(U) is considered partially loyal and if the peer AFI value is higher than AFI(U) then the peer is considered fully loyal and all the data are accepted from these peers. The fidelity score algorithm is showcased in the Fig.2.

Algorithm FidelityScore

1. The target peer is found by the source peer using the query
2. The recommender peers is selected by the source from the recommended list.
3. The request is sent via packets to all the recommenders
4. The recommenders forward their corresponding Fidelity Index of the target to the source.
5. The source computes the AFI for the FI's sent from the recommenders.
6. Two levels AFI(L) and AFI(U) is found
7. IF(AFI <AFI(L)) then
   The target peers is not loyal and discard it.
8. ELSE IF(AFI >=AFI(L) and AFI <=AFI(U)) then
   The target peer is partially loyal
9. ELSE IF(AFI >AFI(U)) then
   The target peer is fully loyal
10. END IF

Fig.2. Pseudo code of the fidelity score calculation algorithm

III. RESULT AND DISCUSSION

The experimental evaluations are carried out by simulation method and NS2 simulator tool is utilized to test the performance of the proposed fidelityscore algorithm. Here bit torrent packet levels are used for the simulation and a very simple topology with 20 peers is utilized for the simulation as shown in the Fig.3.In the Fig.3, the nodes 1, 2 and 3 are routers and they are connected directly to permit several upload and download capacities and more importantly to test the delay occurred during the transmission.Three important metrics are measured during the simulation and they are,

1. SDP ratio – successfully delivered packet ratio which provides the number of successful downloads/receptions made by the peers.

2. Delivery Delay – this is measured as the time delay taken by the peers while forwarding the query and receiving the results from the target peer.

3. Packet drop – this is measured as the number of packets lost during the transmission.

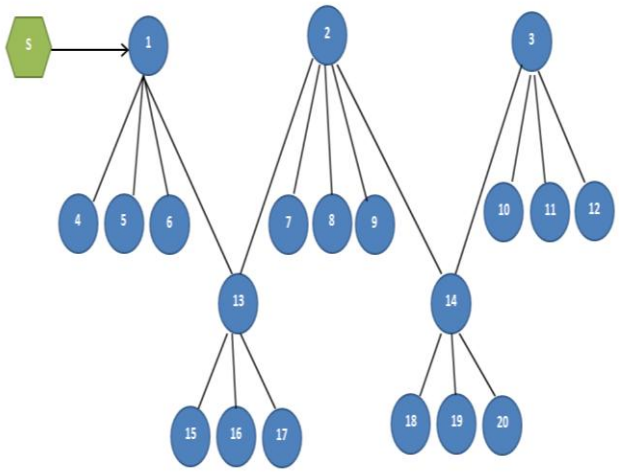

Fig. 3. P2P topology used in the simulation

The experiment is carried out for reliable and non-reliable nodes based on the SDP and rate of transmission ranging from 300 KB to 1 MB as shown in the Fig.4.

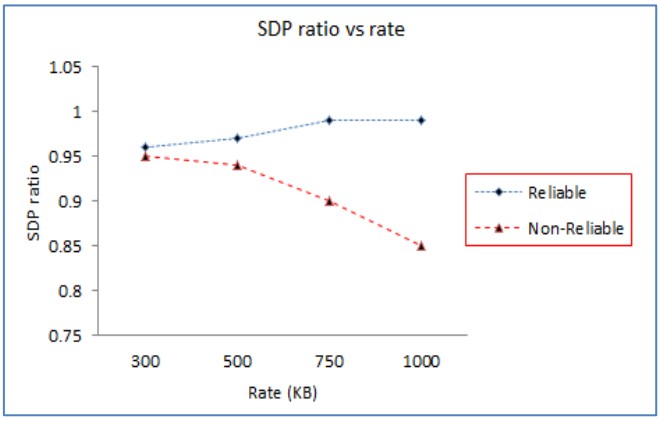

Fig.4. SDP ratio versus rate comparison

From the Fig.4, it is quite clear that the reliable system which utilizes the fidelity score algorithm performs well and as the rate of the packet speed is increased the successful packet delivery ratio is proportionately increased and making the proposed approach better and efficient.

The proposed reliable approach outscored the non-reliable existing method and when the rate is increased, the delivery delay occurred is reduced and there by the speed at which the content is transferred is lightning fast.The non-reliable approach performed quite badly as the rate is increased steadily the number of packets dropped also increases and this decreases the overall efficiency of the system.

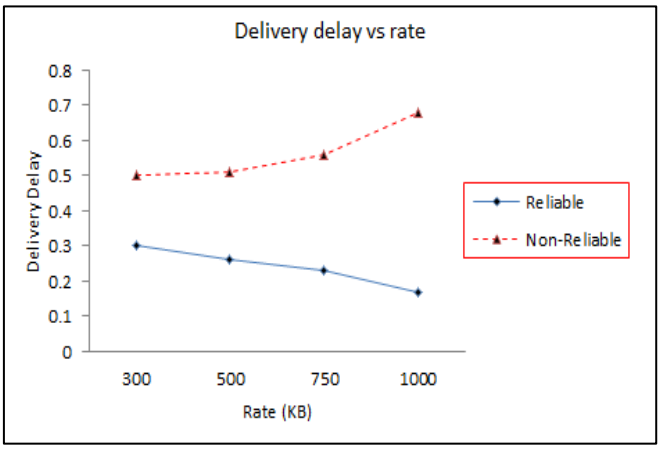

Fig.5. Delivery delay versus rate comparison

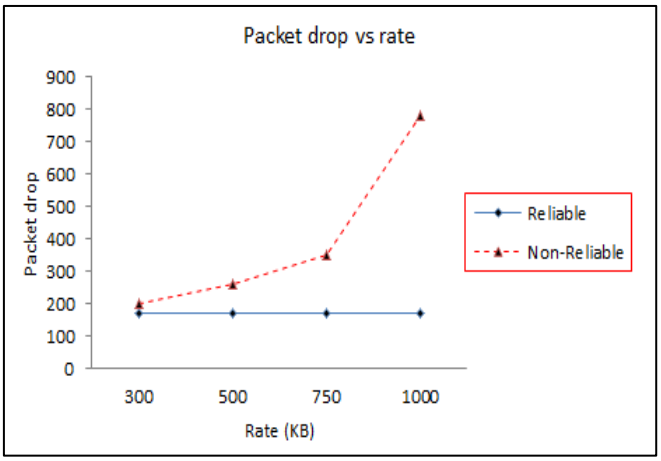

Fig.6. Packet drop versus rate comparison

The same experiment is carried out with the introduction of varying number of fraudulent peers and the SDP ratio and delay is checked for the proposed algorithm and the result is displayed in the Fig.7 and 8.

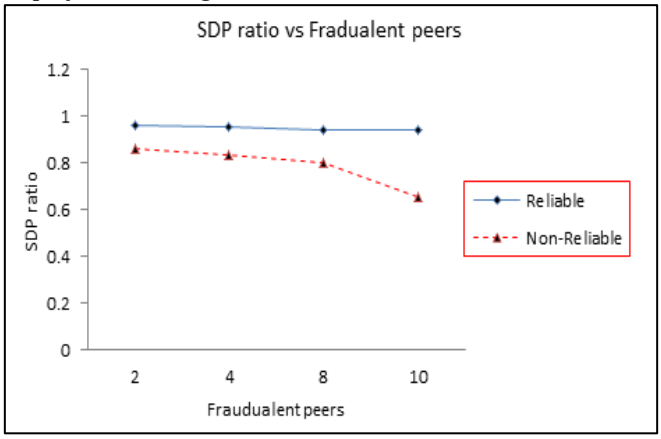

Fig.7. SDP ratio versus fraudulent peers

From the Fig.7, if the numbers of fraudulent or deceitful nodes are increased, the non-reliable approach success ratio decreases considerably and spoils the overall efficiency of the system.

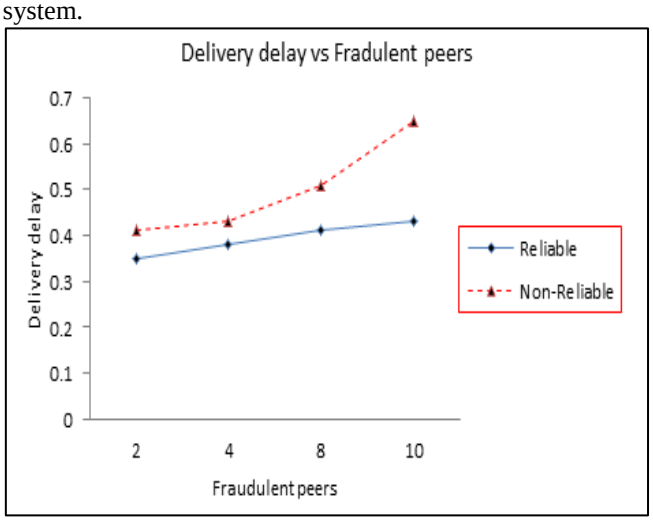

Fig.8. Delivery delay versus fraudulent peer comparison

IV. CONCLUSION

In this paper a new method using the fidelity score is devised and this method scrutinizes the peer credibility before the data is received or transmitted to avoid the unwanted attacks on the precious data present in the P2P network. The fidelity index is calculated after analyzing the SDP ratio, delivery delay and the number of packet dropped from the peers. The fidelity index is maintained in the recommender nodes and the aggregated FI value is calculated (AFI(L) and AFI(U)) and if the AFI value calculated falls above the AFI(U) then the peer is fully trusted and the data is transmitted or received without any doubt. The experimental evaluation showcased that the proposed approach achieved a high SDP ratio and a low delay and packet drops.

REFERENCES

1. [C01]B. Cohen, "*Incentives Build Robustness in BitTorrent*", Workshop on Economics of Peer-to- Peer Systems, Berkeley, CA, USA, June 2003.
2. [J01] Jan Seedorf, "Security Challenges for Peer-to-Peer SIP", IEEE Network, September/October 2006.
3. [M01]B. Mortazavi_ and G. Kesidis,"*Cumulative Reputation Systems for Peer-to-Peer Content Distribution*", pp. 1546-1552, 2006, IEEE.
4. [M02]MujtabaKhambatti, ParthaDasgupta, Kyung Dong Ryu, "*A Role-Based Trust Model for Peer-to-Peer Communities and Dynamic Coalitions*", Second IEEE International Information Assurance Workshop (IWIA'04), pp. 141-154, April 2004.
5. [P01]V. Pathak, L. Iftode, "*Byzantine fault tolerant public key authentication in peer to peer systems, Computer Networks*". Special Issue on Management in Peer to Peer Systems: Trust, Reputation and Security, 50(4):579 596, March 2006.
6. [T01]Thomas RepantisVanaKalogeraki, "*Decentralized Trust Management for Ad - hoc Peer to Peer Networks*", ACM, MPAC: Vol.182, Proceedings of the 4th international workshop on Middleware for Pervasive and Ad-Hoc Computing (MPAC 2006), USA.