P2P File Sharing Technique to Improve Qos in Manets

S. Ch. Vijaya Bhaskar, Ch. Samson, D. Muninder
Assistant Professor, Department of IT, MVSR Engineering College, Hyderabad

Abstract – As of late, P2P systems have turned into a point of convergence in the business. The P2P arrange is open and mysterious, giving the chance to false records, malevolent assaults and different noxious acts, so its trust and security issues have risen. Our definitive point is to enhance the document imparting framework to lessened record seeking expense and postponement. In past few years, personal mobile devices such as laptops and smart phones have been more and more popular. MANETs comprising of advanced gadgets, hubs are always showing signs of change the area, framing separated MANETs with artful gadget experiencing. In this paper, we propose a P2P Information-based secured document sharing framework, specifically RFS, for detached MANETs. In this paper, we overhaul our base work by using proposition to pick the partners. The system uses an interest extraction count to decide a center point's favorable circumstances for Information-based record looking without including beguiling center point. Each get-together has one Global pioneer for each known remote social occasion, which fills in as the expansion to the get-together.

Keywords- P2P, security, file sharing, load balancing.

I. INTRODUCTION

Shared (P2P) is a conveyed application design that appropriates undertakings or workloads among peers, where in each associate has level with assets and equivalent significance. Distributed (P2P) organize is made when at least two gadgets are associated and their assets are shared without experiencing a different server. A P2P framework can be an unrehearsed affiliation—a couple of PCs related through a Universal Serial Bus to trade records. Colleagues are also supported individuals in the application. Each contraption (workstation, propelled cell phones) in the framework is implied as a center point. The proprietor of each center in a P2P framework would apportion a little measure of its benefits - , for instance, plate amassing, sort out exchange speed, or taking care of energy - to be made direct available to each other center point in the framework, thusly without the prerequisite for central coordination by servers or stable hosts. An unadulterated P2P arrange does not have the prospect of clients or servers but instead just center points that all the while fill in as both "clients" and "servers" to interchange center points on the framework. Exactly when appeared differently in relation to the ordinary client to server indicate where simply the server supplies (send) and clients consume (get). Advanced P2P structures are going past the season of partners doing similar things while sharing resources, and are scanning for various sidekicks that can gain remarkable resources and capacities to a virtual assembling in this way empowering it to participate in more imperative endeavors past that can be refined by solitary allies, up till now are worthwhile to each one of the mates. Hybrid Peer-2-Peer structures enable such establishment center points to exist routinely called super hubs. Wired Peer to Peer archive sharing structures have recently ended up being productive model for record sharing among countless. As the compact mechanized devices are passed on by people that when in doubt have a place with certain social associations, in our build paper, authorities focused in light of the P2P record sharing in an isolated MANET cluster containing adaptable customers with relational association properties. In this paper, we focused on the security in record looking for framework.Due to P2P system's privacy and open qualities, it's confounded to locate a viable and workable strategy to take care of P2P organize security issues. Customary system security advances are additionally hard to apply to the P2P arrange. This paper likewise proposed a P2P notoriety show in light of the client record sharing conduct attributes.

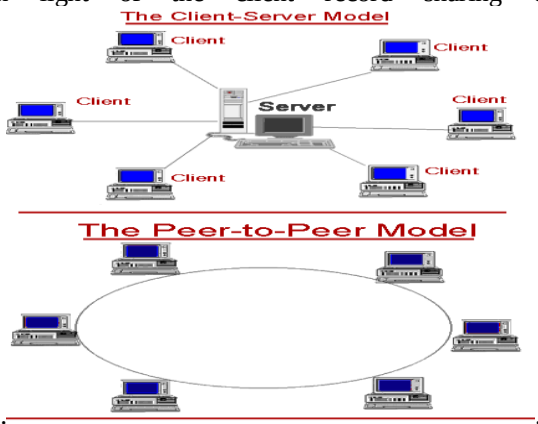

Fig.1: peer to peer and client/server model

II. RELATED WORKS

In this paper [1], creator proposed an approach that utilizations consolidated notorieties of hirelings and assets, giving more educational surveying's and beating the constraints of worker based just arrangements. Worker notorieties are related with the hireling identifier, which must be alter safe.

In this paper [2], creator proposed a Bayesian system based trust show and a technique for building notoriety in view of suggestions in peer-2-peer systems. Since trust is multi-faceted, peers need to create separated trust in various parts of other companions'

capacity. The companion's needs are diverse in various circumstances. Contingent upon the circumstance, an associate may need to think about its trust in a particular part of another companion's capacity or in various viewpoints.

In this paper [5], creator proposed P2P document sharing framework in view of Swarm Intelligence for MANET, alluded to as P2PSI, which utilizes a half and half push-and-force approach. In the ad procedure, each record holder consistently communicates a notice message to advise encompassing hubs about what documents are to be shared. The disclosure procedure finds the coveted document, and leaves the pheromone to help resulting seek demands. The excellence of P2PSI is that it can adjust to progressively changing topology and find close-by document holders auspicious. This paper thought about the half and half strategy to lessen the overhead, however occasional notice and receptive looking both are expanded the overhead in unique nature.

A) Summary of existing framework

In past model, there is no confided in server to approve the companion. At same time trust component is expected to rebuff peers that display vindictive conduct and moreover, an entrance control system is created to secure the documents sharing p2p arrange. In that model, every framework stores the experience of document partaking in its own memory for sometime later. In this write, peer think about transfer peer whether great or awful, which as of now downloaded document from that associate, another companions just considering the notoriety in that transferring peer, it might opportunities to hack by malignant hub . What's more, there is no time determination, so it'll make some issue in exchange.

B) Previous work synopsis

In flooding-based strategies misuses the versatility of hubs inside a geographic territory to scatter web Information among neighbors. It utilizes nearby communicating for Information seeking and sets up Information lists on hubs along the answer way to direct consequent looking. In another strategy each record holder routinely communicates a notice message to illuminate encompassing hubs about its documents. These flooding-based strategies deliver high overhead because of broadcasting. In spite of the fact that the commercial based strategies diminish the overhead of flooding-based techniques, yet despite everything they create high overhead to advertise and can't ensure the achievement of document looking because of hub portability. Despite the fact that Cache/Replication-Based Methods enhance document accessibility, hubs in these techniques latently sit tight for substance they are keen on as opposed to effectively seek records, which may prompt pursuit delay. Content Place characterizes social relationship-based groups and an arrangement of substance storing strategies. In particular, every hub computes an utility estimation of distributed information it has met in light of the information's goal and its associated groups, and reserves the information with the best most noteworthy utilities. Be that as it may, above strategies primarily center around spreading productions to coordinated supporters. In this manner, these strategies can't be connected to record looking straightforwardly.

III. PROPOSED WORK

In our proposed methodology, the record is collected in light of the nonstop looking for frames concerning the reports. In our proposed framework, we are pondering the separated MANET as social occasion. In our proposed structure, we misuse particular sorts of center point conveyability for record sharing. We portray total Local pioneer and Global pioneer center points in the viewpoint of a relational association. A get-together Local pioneer is a fundamental and popular center in the social occasion. In our procedure, we are enhancing the present model with some change. In our proposed exhibit we are showing following things P2P rep show, Trusting buddy, Evaluate peer, Dictionary get the opportunity to control. More secure than existing model and it satisfies the requirements of access control for p2pfile sharing system. In our work, peers send reputation request to peers interfaced already, which decreases organize development standing out from flooding-based techniques. Additionally, each partner broadens its place stock in associate with time and can get more strong recommendations from partners.

A) MODULES

We have divided our proposed technique into small modules, they are given below, Network design (Global leader Node, Local leader Node, Member node), Group Formation (File type, File searching), Own risk model, P2P rep model, Trusting peer, Evaluate peer, Volunteer recommendation.

B)Network Design:

Each node can act with any one of the three different properties according to situation. 1) Global leader Node (The node which capable to collect the neighbor foreign group information. This node can connect the different groups to share the file). 2) Local leader Node (The node which is stable in the group, and contacting to the group node frequently. These nodes which are capable to collect the information of file availability in own group.) 4) Normal node (The node which maintaining only the own information)

C) Group formation:

In this module, we needed to store up the center points, in light of archive Information. The social occasion course of action depends upon the record information; get-together of people contains the particular kind of archives. So the social event will be surrounded in light of the record openness and looking for technique to improve the report looking system. In this module, we needed to seclude the archive looking for design into two sub-modules, the

record request will be done by the interest orchestrated record looking count. In this module, the Local pioneer assembles the information of report openness in the social event. So if any part needs the record archives then the centers can ask to the Local pioneer is called intercommunity report chasing and recuperation. In case looking for archive information isn't available in Local pioneer center point, the record may open in other social occasion. That report information will be assembled by using Global pioneer center point from other social occasion. In the intercommunity looking estimation, a coordinator maps a request to the remote gathering that is well while in transit to contain the addressed record. Like the intercommunity look step, the coordinator also uses the multi copy sending framework, i.e., it passes on a request to agents having the most hoisted closeness with the inquiry to enhance the adequacy of the sending

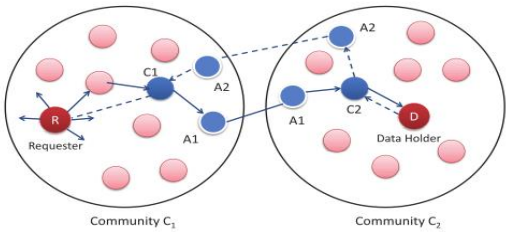

Fig.2: Example model of different properties of network devices

D) Own risk model

The greater part of the hubs in arrange not having some other hub data at introductory time. In this manner hub can't accept wilt hub is great or terrible The asking for companion will choose the transferring peer in view of the downloading understanding (record measure, parcel estimate, transmission capacity designation, add up to term to transfer the document).

$$st_{lm} = \frac{sh_{lm}}{sh_{max}}\left(cb_{lm} - {}^{ib_{lm}}/_{2}\right) + \left(1 - \frac{sh_{lm}}{sh_{max}}\right) r_{lm} \qquad (1)$$

E) P2P rep model

The notoriety metric measures a more peculiar's dependability in view of suggestions. On the off chance that hub discovers number of associate width indented record then its need to affirm wilt peer is great or awful, so it will demand to all companion about indented peer. By accepting proposal from different associates, hub can compute the notoriety esteem. The asking for companion will choose the best associate in light of higher notoriety esteem (if possess downloading history is low)

$$r_{lm} = \frac{[\mu_{sh}]}{sh_{max}}\left(ecb_{lm} - {}^{eib_{lm}}/_{2}\right) + \left(1 - \frac{[\mu_{sh}]}{sh_{max}}\right) er_{lm} \qquad (2)$$

F) Trusting peer

In this model, we are acquainting the strategy with acknowledge the trust based companion determination. On the off chance that asking for peer effectively accomplished more exchange then it can trust the companion with less number of proposal. In light of possess history esteem, the hub will choose the best companion to download the record

$$rt_{ln} = \frac{rh_{lp}}{rh_{max}}\left(rcb_{lp} - {}^{rib_{lp}}/_{2}\right) + \frac{rh_{max} - rh_{lp}}{rh_{max}} r_{lp} \qquad (3)$$

G)Enhanced volunteer recommendation:

In our base model, they have considered the constraining the quantity of downloader's to keep up the possess reliability in different associates. In base model, if constrain is crossed then the transferring associate will overlook the req. To locate the great companion, requester needs to invest the greater part of the energy in proposal checking. We have upgraded base model to determine the issue of deferral. In this module, if constrain is crossed then the hub will check the exceedingly confided in peer with asked for document.

On the off chance that companion discovered then hub will produces volunteer proposal If any volunteer suggestion is gotten, at that point the hub will check recommender is exceptionally confided in hub or not. On the off chance that yes then the hub won't make Recom_req, straightforwardly it will download the document from prescribed hub. In this module, the hub assesses the associate in two ways, 1) Service based, 2) Recommendation based. After each download, the peer will verify the agreement with final download level. Based on the performance, service info will be updated. After receiving recommendation from number of peer, the node will verify the peer's bad recommendation by comparing all recommendation. Then new value will be updated. By checking service and recommendation, the best peer will be considered for file download and recommendation.

Determination of best specialist co-op may over-burden few companions while different associates having same assets are sit out of gear. A heap adjusting system is executed in this work, to use the assets of qualified great associates. In this strategy, each associate's synchronous tasks are constrained to a most extreme. In the event that an associate achieves its most extreme number of concurrent activities, rather than just dismissing the approaching solicitations, it proposes another great companion having a similar asset to the administration requester. Thus, this strategy stays away from time required for the administration requester to locate another great specialist co-op and furthermore lessens the system traffic.

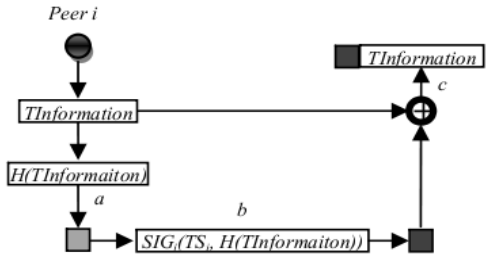

Fig.3: file sharing request

ALGORITHM:

U_c *is Uploading count,*
$N_{L_{Th}}$ *is Max up limit threshold*
W_p *is working period*
NW_p *is non working period*
B *bandwidth,* B_{U_R} *bandwidth upload reserved,*
B_{us} *bandwith used*

STEP 1
If (peer has to download file)
1. Generate file request and send
2. Wait for reply and good per selection for a time

STEP 2
If (any peer received the request)
1. Check for upload limit (ENHANCEMENT)

$$U_c = \begin{cases} 0, & At\ initial \\ \sum_{l=1}^{n} xl, x = 1, n = 1,2,3..n \end{cases}$$

If (limit is not crossed)

$U_c \leq N_{L_{Th}}$

1. If (file found)
   Set the bandwidth possibilities
   $B = B_m - (B_{U_R} * Rand) - B_{us}$
   Give reply
2. else
   Ignore

If (limit is crossed)

$U_c > N_{L_{Th}}$

1. check for good peer

$$st_{lm} = \frac{sh_{lm}}{sh_{max}}\left(cb_{lm} - {}^{ib_{lm}}/_{2}\right)$$

For each $j \epsilon Ai$
If $St_{lm} > S_{Th}$ found
Recom ***m***
else
Ignore **m**

STEP 3
If (request received)
1. add peer in to lis
   1. $P_l \cup P_{List}$
2. send recommendation request to all other peers

STEP 4
If (recommendation request received)
1. Checks the history
   1. For-each $H_l \epsilon SH_{List_m}$
      a. if (info found)
      Send recommendation info
      b. else
      Ignore

STEP 5
If (recommendation received)
1. add the recommendation info in to a list $R_m \cup R_{List}$

STEP 6
If (best peer recommendation received)
1. send data request
2. collect the data
3. set the satisfaction
   $= W_p/(W_p + NW_p)$

STEP 7
If (data request)
1. check crossed the limit
   $U_c > N_{L_{Th}}$
   I. If crossed limit
      a. send objection message

STEP 8
Time out for check best peer
1. filter the recommendation by SORT algorithm
2. Select best peer

IV. RESULTS

We have tested our proposed network with popular simulation tool called NS2. We have utilized the Single PC with design of 20 GB Hard circle space, 1 GB RAM, programming's Linux OS (Ubuntu 10.04) and NS2.34. We have composed the program by TCL (Front End dialect). We mimicked our proposed framework with two sorts of results. One is Nam and Xgraph.

In this section, we presented main result steps in fig 5-9, which shows the different packets used in the trust management process.

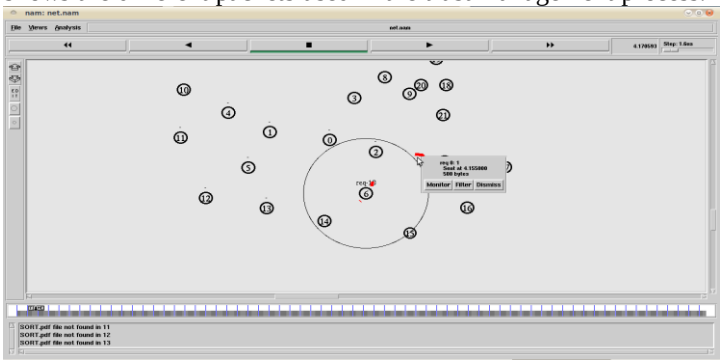

Fig.4: File searching request

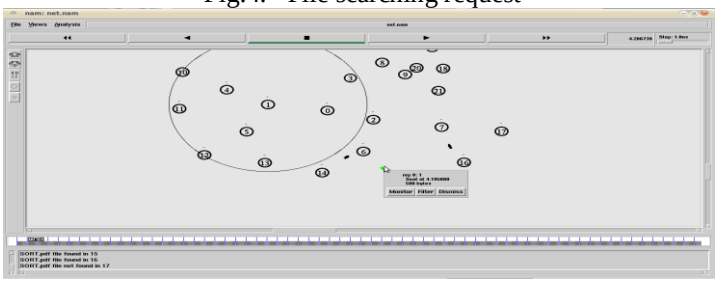

Fig.5: File available reply

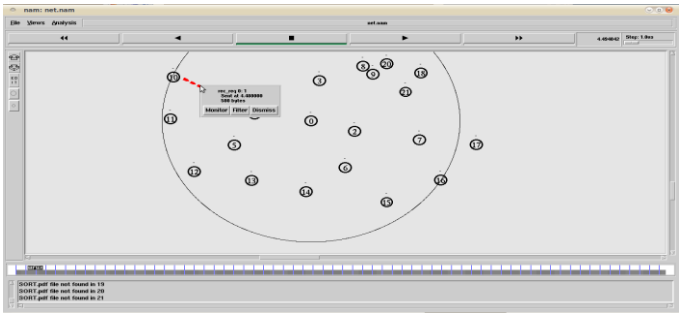

Fig.6: Requesting for best peer recommendation

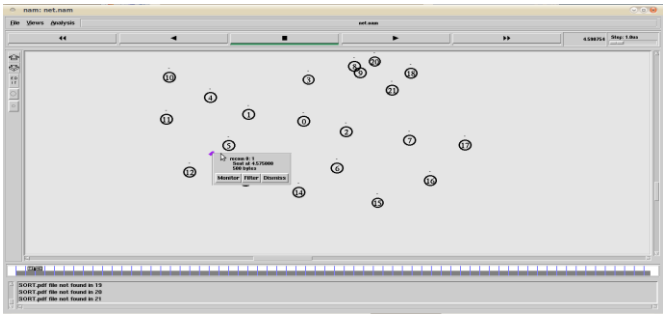

Fig.7: Recommendation ion about best peer

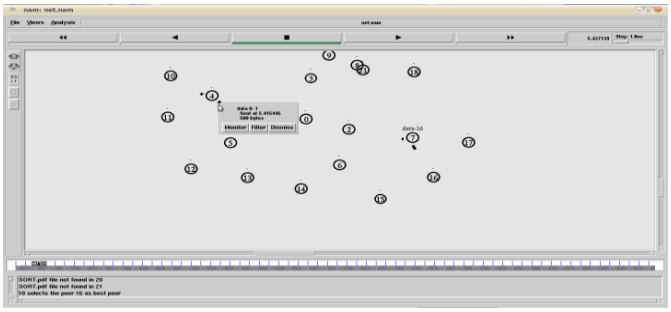

Fig.8: Download the file from best peer

The graph (10 & 11) shows packet delivery and overhead comparison. From graph we can know our proposed system works well in un-trusted environment

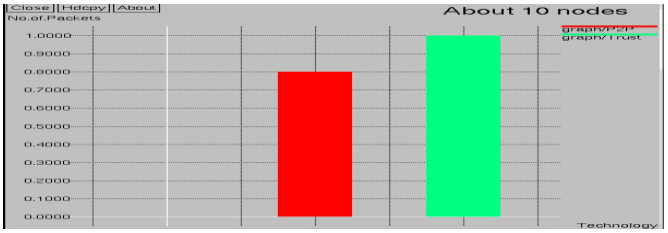

Fig.9: Pkt delivery graph with basic p2p and trust based P2P

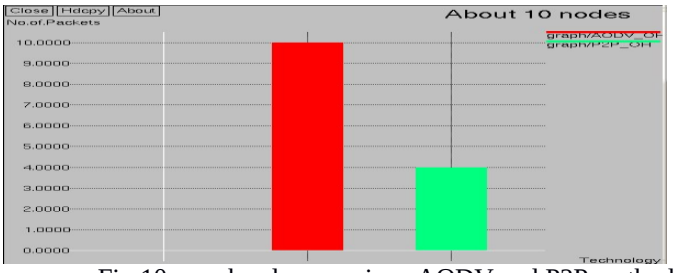

Fig.10: overhead comparison AODV and P2P method

V. CONCLUSION

In our proposed method, the file is Information based on the frequent query processes regarding the files. In our proposed technique, we are considered the disconnected MANET as group groups. And we have implemented less overhead file searching system and we have tested successfully. The problem of identifying wrong recommendations is reduced in this work. It reduces the service based attacks and it also reduces the recommendation based attacks if there are not more than 50% malicious nodes in the P2P network. It uses three types of metrics, service, and reputation and recommendation trust metrics to create a trust network in a peer's proximity. This work also implements the load balancing mechanism to utilize the network resources effectively. When the best service provider in the network reaches its maximum number of simultaneous operations, it suggests another good peer having the same service to the service requester. Hence, the time required for service requester to choose a different peer is reduced.

It helps reducing large amounts of attacks but, this work does not solve all the security issues of a P2P network. This issue should be focused in future work to use the trust model in various applications. Future work may consist of using different load balancing algorithms to reduce the delay of getting a resource.

VI. REFERENCES

[1]. A.A. Selcuk, E. Uzun, and M.R. Pariente, "A Reputation-Based Trust Management System for P2P Networks," Proc. IEEE/ACM Fourth Int'l Symp. Cluster Computing and the Grid (CCGRID), 2004.

[2]. K. Hoffman, D. Zage, and 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.

[3]. R. Zhou and K. Hwang, "Power trust: A Robust and Scalable Reputation System for Trusted Peer-2-Peer Computing," IEEE Trans. Parallel and Distributed Systems, vol. 18, no. 4, pp. 460-473, Apr. 2007.

[4]. Ahmet Burak Can, Member, IEEE, and Bharat Bhargava, "SORT : A Self-Organizing Trust Model for Peer-2-Peer Systems," IEEE Trans. Dependable and Secure Computing, vol. 10, no. 1, Jan-Feb. 2013.

[5]. Cheng-Chang Hoh and Ren-Hung Hwang "P2P File Sharing System over MANET based on Swarm Intelligence: A Cross-layer Design",. 2007

[6]. S. Marsh, "Formalising Trust as a Computational Concept," PhD thesis, Dept. of Math. and Computer Science, Univ. of Stirling, 1994.

[7]. A. Abdul-Rahman and S. Hailes, "Supporting Trust in Virtual Communities," Proc. 33rd Hawaii Int'l Conf. System Sciences (HICSS), 2000.

[8]. Yu and M. Singh, "A Social Mechanism of Reputation Management in Electronic Communities," Proc. Cooperative Information Agents (CIA), 2000.

[9]. Z. Despotovic and K. Aberer, "Trust-Aware Delivery of Composite Goods," Proc. First Int'l Conf. Agents and Peer-2-Peer Computing, 2002.

[10]. R. Zhou, K. Hwang, and M. Cai, "Gossiptrust for Fast Reputation Aggregation in Peer-2-Peer Networks," IEEE Trans. Knowledge and Data Eng., vol. 20, no. 9, pp. 1282-1295, Sept. 2008.

[11]. B. Ooi, C. Liau, and K. Tan, "Managing Trust in Peer-2-Peer Systems Using Reputation-Based Techniques," Proc. Fourth Int'l Conf. Web Age Information Management, 2003.