RESEARCH ARTICLE OPEN ACCESS

Self-Organizing Deployment of Scalable Services In Peer To Peer System

Athira U.K
Department of Computer Science Engineering
Lourdes Matha College of Science and Technology, Thiruvananthapuram
Kerala – India

ABSTRACT

P2P networks are networks in which all peers cooperate with each other to perform a critical function in a decentralized manner. All peers are both users and providers of resources and can access each other directly without intermediary agents**.** Compared with a centralized system, a P2P system provides an easy way to aggregate large amounts of resource residing on the edge of Internet or in ad-hoc networks. File sharing is the dominant P2P application on the Internet, allowing users to easily contribute, search and obtain content. Here a trusted system based on processing the message to maintain a trust value for each node. The node that rely messages more successfully will have higher trusted value such as low mobility and large hardware resources. Based on these trust values we develop a trust- based routing protocol to route messages through the higher trusted nodes to minimize the provability of dropping the messages and thus improve the network performance in terms of throughput and packet delivery ratio.

Keywords:- Trust based value, security, routing protocol, message broadcasting

I. INTRODUCTION

A P2P system is defined as any distributed network architecture composed of participants that make a portion of their resources, such as processing power, disk storage or network bandwidth are directly available to other network participants, without the need for central coordination instances such such as servers or stable hosts. More, simply, a P2P network links the resources of all the nodes on a network and allows the resources to be shared in a manner that eliminates the need for a central host. In P2P systems, nodes or peers of equal roles and responsibilities, often with various capabilities, exchange information or share resources directly with each other. P2P systems can function without any central administration and coordination instance. A P2P network differs from conventional client/server or multi tiered server's networks.

A. Problem Definition

Generation of service facilities in various network locations requires user service provider. A huge majority will be light weight services requiring minimal storage and addressing relatively few users in the proximity of user service provider so that duplication across the network will not be justified. So here the problem formulated as a facility location problem and device a distributed and highly scalable heuristic to solve it.

1.2 Related Works and Contribution

Marsh [11] defines a formal trust model based on socio-logical foundations. An agent uses own experiences to build trust relations and does not consider information of other agents. Abdul-rahman and Hailes [12] evaluate trust in a discrete domain as an aggregation of direct experience and recommendations of other parties. They define a semantic distance measure to test accuracy of recommendations. Yu and Singh's model [13] propagates trust information through referral chains. Referrals are primary method of developing trust in others. Mui et al. [14] propose a statistical model based on trust, reputation, and reciprocity concepts. Reputation is propagated through multiple referral chains. Jøsang et al. [15] discuss that referrals based on indirect trust relations may cause incorrect trust derivation. Thus, trust topologies should be carefully evaluated before propagating trust information. Terzi et al. [16] introduce an algorithm to classify users and assign them roles based on trust relationships. In Aberer and Despotovic's trust model [1], peers report their complaints by using P-Grid [29]. A peer is assumed as trustworthy unless there are complaints about it.

However, preexistence of trust among peers does not distinguish a newcomer and an untrustworthy one. Eigen- trust [3] uses transitivity of trust to calculate global trust values stored on CAN.

1.3 Expected features of proposed system

Introduction of novel centralistic metrics helps to identify a small sub group of candidate service host node and to reduce the accurate view of global demand distribution and save the service migration path towards the location that minimize the cost over the whole network. The proposed system must able to provide high security for all the service that occur between the peers in the network. The services in the proposed system includes transmission of music files, document files messages.

II. PROPOSED SYSTEM

The main contribution of the proposed system is an automatic placement module that copies only on server's host to client that actually needs them. We develop a trust system based on processing the message to maintain a trust value for each node. The node that rely messages more successfully will have higher trusted values such as low mobility and large network resources. Based on these trust values, we develop a trust based routing protocol to route messages through the higher trusted nodes to minimize the provability of dropping the messages and thus improve the network performance in terms of throughput and packet delivery ratio. Thus, the system mainly consists of six modules. They are:

1. Node Generation
2. Service Handling
3. Service allocation
4. Trusted Authority
5. Message Broadcasting
6. Security

2.1 Node Generation

Whenever a node wants a service which can be provided by another node then the node can make a request for the service. All requests that are made by the nodes are satisfied through the trusted authority. The trusted authority will identify which node has the service for which the request is made and the service can be performed. For servicing a node's request, the node has the ability to run the service. Each node is provided with the ability to upload and download information like music files, documents etc.

2.2 Service Handling

In this module, the node create services like file transfer which is a simple service or complex services like transaction of money through online etc. For example, in a credit card system, the money given by the owner is actually taken from the bank and is given to the user. But it is not the bank manager who takes the money or does any transaction instead another third party authority provides the service i.e it act as a service. This module handles all the service available within the peers.

2.3 Service Allocation

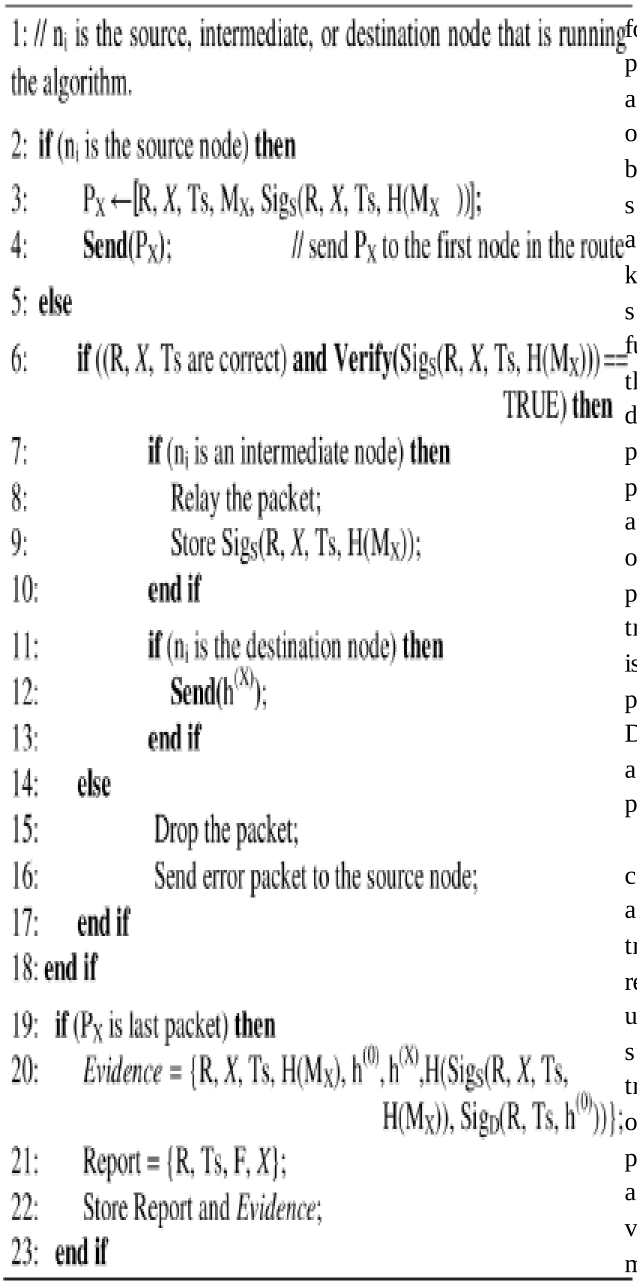
If more than one node request for the same service, then the service is allotted using a service allocation mechanism. There is different service allocation mechanism like first one to request is serviced first, assigning priority to each node and service the request based on the priority. In a peer to peer system, the efficient way to service request or to allocate the service is by using a hop count or through a multi-hop mechanism. Another factor is, whenever a service is allocated, it must be verified that," Is the allocated one actually used by the node". Only the allocated node must use the service, which is allocated to it this is done because the allocation is implemented using the allocation mechanism which ensures the available bandwidth, collision free path etc..

2.4 Trusted Authority

It is the administrator of the whole working of the system. Here the trusted authority can create new node i.e new peer is added to the network only with the help of trusted authority. The trusted authority maintains a list, which contains all the node's details. Hence, if any node from outside the network tries to get service from inside node, then it will be identified by the trusted authority and rejects its entry. If such an outsider node wants a service, then it must first communicate with the trusted authority. Another important functionality of the trusted authority is the ability to generate the topology. It is the duty of trusted authority to decide what topology must be used, which node must come after one particular node, which must be the neighboring nodes etc. In relation, to topology generation, it maintains a neighbor node listing where the neighbors of each node are maintained as a list.

2.5 Message Broadcasting

Message transmission is done using message broadcasting method. Thus the messages are transmitted with the help of neighboring nodes. This is the main part of the thesis work. The algorithm used for message transmission is given below:



```
// $n_i$ is the source, intermediate, or destination node that is running the algorithm.
if ($n_i$ is the source node) then
    $P_X \leftarrow [R, X, Ts, M_X, Sig_S(R, X, Ts, H(M_X))]$;
    Send($P_X$);            // send $P_X$ to the first node in the route
else
    if ((R, X, Ts are correct) and Verify($Sig_S(R, X, Ts, H(M_X))$) == TRUE) then
        if ($n_i$ is an intermediate node) then
            Relay the packet;
            Store $Sig_S(R, X, Ts, H(M_X))$;
        end if
        if ($n_i$ is the destination node) then
            Send($h^{(X)}$);
        end if
    else
        Drop the packet;
        Send error packet to the source node;
    end if
end if
if ($P_X$ is last packet) then
    Evidence = {$R, X, Ts, H(M_X), h^{(0)}, h^{(X)}, H(Sig_S(R, X, Ts, H(M_X)), Sig_D(R, Ts, h^{(0)})$};
    Report = {R, Ts, F, X};
    Store Report and Evidence;
end if
```

Figure 2.1: Algorithm for message transmission

2.6 Security

While transmitting the message security s provided with the help encryption. In this method AES (Advanced Encryption Standard) encryption algorithm is used. AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware.

III. RESULTS AND DISCUSSIONS

Performance analysis involves gathering formal and informal data to help users and service providers define and achieve their goals. Performance analysis uncovers several perspectives on a problem or opportunity, determining any and all drivers towards or barriers to successful performance, and proposing a solution system based on what is discovered. The accomplishment of a given task measured against preset known standards of accuracy, completeness, cost, and speed. In contrast, performance is deemed to be the fulfillment of an obligation, in a manner that releases the performer from all liabilities under the contract. The definition for performance analysis given is: A specific, performance based needs assessment technique that precedes any design or development activities by analyzing the performance problems of a work organization. There are three basic steps in the performance analysis process: Data collection, Data transformation, and Data visualization. Data collection is the process by which data about program performance are obtained from an executing program. Data are normally collected in a file, either during or after execution, although in some situations it may be presented to the user in real time.

The raw data produced by profiles, counters, or traces are rarely in the form required to answer performance questions. Hence, data transformations are applied, often with the goal of reducing total data volume. Transformations can be used to determine mean values or other higher-order statistics or to extract profile and counter data from traces. For The raw data produced by profiles, counters, or traces are rarely in the form required to answer performance questions. Hence, data transformations are applied, often with the goal of reducing total data volume. Transformations can be used to determine mean values or other higher-order statistics or to extract profile and counter data from traces. For example, a profile recording the time spent in each subroutine on each processor might be transformed to determine the mean time spent in each subroutine on each processor, and the standard deviation from this mean. Similarly, a trace can be processed to produce a histogram giving the distribution of message sizes. Each of the various performance tools described in subsequent sections incorporates some set of built-in transformations; more specialized transformation can also be coded by the programmer. Next section gives the comparison between existing and proposed system. The figure shows how the increase in number of nodes in the subgraph influences the access rate.

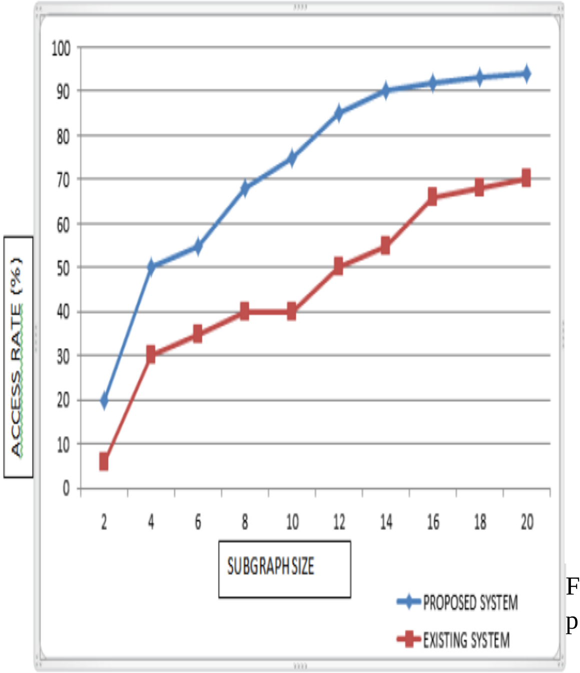


Figure 3.1: Graph showing variation in access rate between proposed and existing system

The figure indicates that as the number of candidate nodes that host the service increases, the service can be accessed within shorter delay. The node selection is done autonomically by the cdsma algorithm. So while comparing with the existing system, the proposed system has high access rate. Access rate is the maximum data rate of a channel between a user site and a network, as defined by the bandwidth of the access link available for data transmission. Here the number of node is increased from 2 to 20 and the access rate in percentage is calculated. It is also seen that as the range of a node is high the time need to access the service is less. This is depicted in fig 3.2, time is calculated in milliseconds. In this system the node can send messages to neighboring nodes. If the destination node is within the range of this node it will get the message. So if the node is connected to more number of nodes, the chance to access the message or service as fast as possible is high. The range of node is an important factor in the performance of the system.

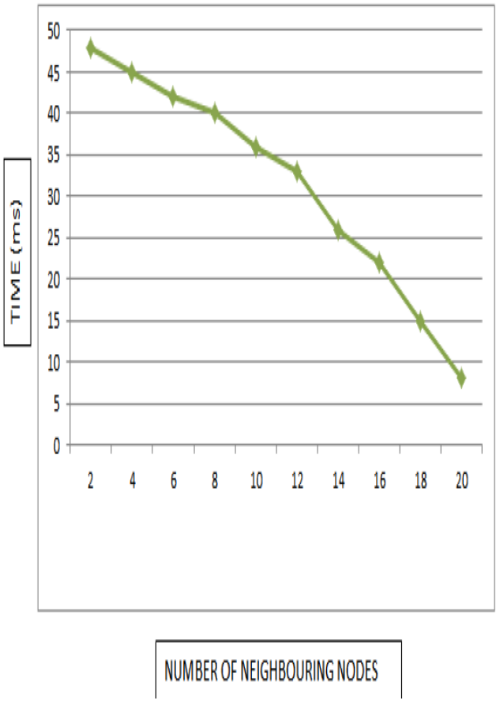


Figure 3.2 : Figure showing variation in speed between proposed system and existing system

IV. CONCLUSION

Thus, the paper discussed about the peer to peer network, proposed system for providing protection in the network. The problem like location facility problem has been fixed with the help of this system. In this system, files like documents, music files can be transmitted. In the future enhancement, by using more secure algorithms the larger files can be transmitted.

REFERENCE

[1] K. Aberer and Z. Despotovic. Managing Trust in a Peer-2-Peer Information System. In Proceedings of the 10th International Conference on Information and

KnowledgEManagement (ACM CIKM) , New York, USA, 2001.

[2] Advogato's Trust Metric (White Paper), http://www.advogato.org/trust-metric.html.

[3] T. Aura, P. Nikander, and J. Leiwo. Dos-resistant authentication with client puzzles. In 8th International Workshop on Security Protocols, 2000.

[4] T. Beth, M. Borcherding, and B. Klein. Valuation of trust in open networks. In Proc.3rd European Symposium on Research in Computer Security – ESORICS '94 , pages 3–18, 1994.

[5] Captcha Project. http://www.captcha.net.

[6] F. Cornelli, E. Damiani, S. D. C. D. Vimercati , S. Paraboschi,and S. Samarati. Choosing Reputable Servents in a P2PNetwork. In Proceedings of the 11th World Wide Web Conference, Hawaii, USA, May 2002.

[7] A. Crespo and H. Garcia-Molina. Semantic Overlay Networks. Submitted for publication 2002.

[8] J. Douceur. The Sybil Attack. In First IPTPS , March 2002.

[9] eBay website. www.ebay.com.

[10] T. H. Haveliwala and S. D. Kamvar. The second eigenvalue of the google matrix. Technical report, Stanford University, 2003

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

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

[13] B. Yu and M. Singh, "A Social Mechanism of ReputationManagement in Electronic Communities,"Proc. Cooperative In-formation Agents (CIA),2000.

[14] L. Mui, M. Mohtashemi, and A. Halberstadt, "A Computational Model of Trust and Reputation for E-Businesses,"Proc. 35th Hawaii Int'l Conf. System Sciences (HICSS),2002.

[15] A. Jøsang, E. Gray, and M. Kinateder, "Analysing Topologies of Transitive Trust,"Proc. First Int'l Workshop Formal Aspects in Security and Trust (FAST),2003.

[16] E. Terzi, Y. Zhong, B. Bhargava, Pankaj, and S. Madria, "An Algorithm for Building User-Role Profiles in a Trust Environment,"Proc. Fourth Int'l Conf. Data Warehousing and Knowledge Discovery (DaWaK),vol. 2454, 2002.

[17] Y. Zhong, "Formalization of Dynamic Trust and Uncertain Evidence for User Authorization," PhD thesis, Dept. of Computer Science, Purdue Univ., 2004.

[18] D.H. McKnight, "Conceptualizing Trust: A Typology and E-Commerce Customer Relationships Model,"Proc. 34th Ann.Hawaii Int'l Conf. System Sciences (HICSS),2001.

[19] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman,"Reputation Systems,"Comm. ACM,vol. 43, no. 12, pp. 45-48,2000.

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