ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: Oriental Scientific Publishing Co., India.
www.computerscijournal.org

ISSN: 0974-6471
June 2013,
Vol. 6, No. (2):
Pgs.55-59

Trust and Caching Technique for Intelligent Semantic Query Routing in P2P Networks

U.V.ARIVAZHAGU[1] and S.SRINIVASAN[2]

[1] Computer Science & Engineering Sathyabama University Chennai, (India).
[2]Professor & Head of the Department in Computer Science & Engineering ,
Anna University ,Regional Centre , Madurai, (India)
Corresponding author E-mail : arivu12680@gmail.com

(Received: May 16, 2013; Accepted: June 14, 2013)

ABSTRACT

The P2P routing protocol is affected from the fact that queries need to reach the largest number of peers to enhance the chances to locate the target file and messages should be low as possible We propose trust based query routing technique for P2P Networks. Initially the node with maximum trust value is chosen as cluster head. These cluster heads are designated as trust managers. Each peer maintains a trust table which gets updated once it gets feedback from the trust manager about the resource requested peer. If the update denotes that the node is reachable and trusted, the routing is performed. Otherwise its echo time is verified again to decide the re-routing process. By simulation results, we show that the proposed work offers secured and reliable routing. This peer to peer network is carried out without using a caching mechanism to store the data packets while routing. To achieve this caching mechanism we have proposed methods for caching the data packets in the peers and also to replace these data packets with the new data packets in the next routing process.

Keywords: Query Routing Trust Routing, Trust Manager ,Peer to Peer Networks,

INTRODUCTION

In our previous approach[11], we have proposed an Intelligent Semantic Query Routing Technique, where the peers are initially formed into clusters and elect a cluster head (CH). CHs communicate with their neighbor CHs via Gateways and carries out the searching process. Every CH maintains the list of recent queries, corresponding query hits along with the results. Once the list overflows, a replacement policy is adopted to maintain the recent query list. Though cluster based routing reduces the overhead and delay, if the requested item is not present in the current cluster, it has to fetch the data from the other cluster. If the destination node is located far away from the source cluster head, it will increase the delay. Every ant agent approaches the cluster head (CH) in search of resources by launching the semantic queries. The agent records the routes that have been selected and each time it finds a resource, the data is fedback via the route established. If resource is available, it updates the table and feedbacks via the available route. Else, it enquires the neighboring CH and selects the matching peers. The rank of each peer is calculated based on query hit and cosine similarity. Then the peer with the higher rank will be selected for fetching the resource. The proposed approach doesn't let the peer, know how secured is the requested peer is, to extract the resources.

Literature Review

Huaiqing Lin et al., [1] have proposed a CL-PKC-Based secure group communication scheme and this proposed approach has two rounds and requires constant pairing operation per user. In the original construction of CL-PKE, the KGC must ensure that the partial key is delivered securely to the correct entity, while this requirement is canceled in our scheme. The main advantage of this approach is that avoids the escrow problem in identity-based cryptosystem and the secure delivery of private keys.

CAI Biao et al., [2] have proposed a structured topology for trusts management in portable P2P network based on DHT (discrete hash table), in which includes trust management strategies and peer operations on certain DHT circle. And also the authors have proposed a trust-computing model for the structured P2P network and the main trust decisions in the structured network are introduced too. And the advantage of this approach is that it will have information, which peers can join or leave at anytime and anywhere to address the portability in a portable P2P network.

Mohamed Hefeeda et al., [6] have proposed pCache method which is design and evaluation of a complete, running, proxy cache for P2P traffic. pCache transparently intercepts and serves traffic from different P2P systems. A new storage system is proposed and implemented in pCache. This storage system is optimized for storing P2P traffic, and it is shown to outperform other storage systems. In addition, a new algorithm to infer the information required to store and serve P2P traffic by the cache is proposed. The advantage of this approach is that this method saves the bandwidth usage and also reduces the load on the backbone links.

Jing Zhao et al., [7] have proposed a novel asymmetric cooperative cache approach, where the data requests are transmitted to the cache layer on every node, but the data replies are only transmitted to the cache layer at the intermediate nodes that need to cache the data. This solution not only reduces the overhead of copying data between the user space and the kernel space, it also allows data pipelines to reduce the end-to-end delay. They have also studied the effects of different MAC layers, such as 802.11-based ad hoc networks and multi-interface-multichannel-based mesh networks, on the performance of cooperative cache. The advantage of this approach is that it can significantly reduce the data access delay compared to the symmetric approach due to data pipelines.

Mei Chen et al., [12] have proposed a cluster-based reputation model (CBRM). The model is consisted by reputation mechanism for realizing the security transaction and the network topology structure of CBRM adopts the cluster, so efficiency of reputation management is noticeably raised. In order to improve security, reduce the network traffic brought by management of reputation, and enhance stability of cluster, when we select reputation, the average historical online time, and the network bandwidth as the elementary components of the comprehensive performance of node.

Trust Based Query Routing Technique Overview

In our proposed extension, we propose a trust based query routing technique for P2P Networks. Initially the node with maximum trust value is chosen as cluster head. These cluster heads are designated as trust managers. At the time of implementing the trust routing decision, every peer has to maintain trustable table. This table includes all the information about the peers in the network like IP address of the peer, key of the trust manager, trust score and also the tables tells is the peer is reachable or no. The table will be updated once a peer node gets feedback from the trust manager about the resource requested peer. If the update denotes that the node is reachable and trusted, the routing is performed. Otherwise its echo time is verified again to decide the re-routing process.

Cluster formation

The steps involved in the cluster formation are as follows :

Step 1

Each peer node (N_i) deployed in the network broadcast the hello message to its neighboring peer nodes.

Step 2

Based on the Hello Message, each N_i identifies itself and also maintains the neighbors list (NL).

Step 3

After obtaining trust values of all neighbor peer nodes, the node verifies the trust value with the trust threshold (T_{Th}).

```
If $T(x) > T_{Th}$
Then
    $N_i$ declares itself as CH immediately.
    $N_i \xrightarrow{CL\_REQ} NL$
End if
```

Step 4

Upon hearing the CL_REQ, the neighboring nodes in NL sends join reply message to N_i to join the cluster.

Secured Routing

In order to perform routing process in secured manner, we consider trust secured routing technique into consideration. In this technique, each peer is assigned with x-bit identifier using trusted hash function. It is assumed that the identifier length x should be large. This is done to generate the probability of two peer nodes hashing to the similar key as small (negligible value).

Secure Information Table

During implementation of trust routing decision, each peer maintains the trust table.

Node ID: Identity of the node.
IP Address: IP address of the node
Key: The key estimation is described in the next section.
AS: It illustrates whether the node is reachable or not.

```
1)      If AS = ASY
Then
Currently i^th peer is reachable from the TM
End if
2)      If AS = ASN
Then
        i^th peer is not attainable from TM.
End if
```

Trust Routing

Each CH_i acts as trust manager (TM_i) which manages the identifier and trust information of its cluster members.This technique offers secure and reliable routing. Through this technique, it is easier to identify whether the peer failure has occurred or if any peer leaves/joins the cluster. we extend the trust routing work with an asymmetric cooperative cache approach [7] for the cache mechanism and an intelligent caching mechanism for cache replacement policy for the new data packets entry which is known as SPACE [9] (Systematic P2P Aided Cache Enhancement). Through this way the peers in the network stores the data in their cache and replace them when the new data packets make entry during the routing. The advantage of this approach is that the network cost can be reduced by storing the data packets during the routing i.e. if any data packets required more than once or if any data packets lost during the routing it becomes easy to retrieve those data packets from peer's cache. Also the delay between the peers can be reduced.

RESULTS

Simulation Setup

This section deals with the experimental performance evaluation of our algorithms through simulations. In order to test our technique, the NS-2 simulator [9] is used. NS-2 is a general purpose

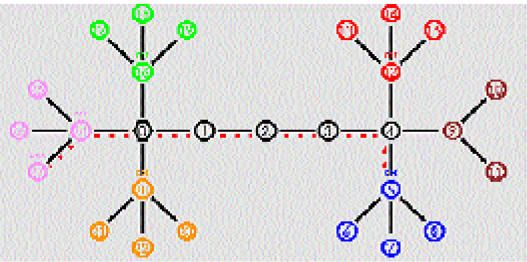

Fig.1: Network Topology

simulation tool that provides discrete event simulation of user defined networks. We have used the BitTorrent packet-level simulator for P2P networks[10].

A network topology is only used for the packet-level simulator. We use a topology shown in Fig 1 for our simulation. In this topology, peer nodes form 5 clusters with elected cluster head (marked as CH). The clusters are marked with different colors. Each CH is connected to an access router. The requested information is fetched from the best peer by the source peer. Ant agents are deployed in each peer for intelligent searching. We compare our Trust Based Intelligent Semantic Query (TBISQ) routing technique with existing Cluster Based Intelligent Semantic Query (CBISQ) technique [11].

Based on Error Rate

For the peer failure management, we apply exponential error model on the links between two peer. We vary the error rate as 0.1, 0.2, 0.3, 0.4 and 0.5. The response delay and packet drop are measured. When the error rate is increased, it increases the packet drop in that particular path. Due to these drops retransmission of failed packets increases, resulting in increased delay.Fig 2 and 3 give the result of delay and packet drop, respectively, when the error rate is increased. It can be seen that the delay and drop of TBISQ is significantly less than CBISQ, because of the failure management technique of TBISQ.

Based On Queries

In our second experiment, the number of queries issued by each source is varied from 1 to 5 for different set of files. The matching peers are selected from the set of trusted peers and the response delay and received packets are measured. In each cluster, one peer is deployed with malicious behavior.

From the Fig 4, it can be seen that the response delay involved in TBISQ is significantly less than that of CBISQ. Fig 5 show that the packets received when the queries are increased. From the figure, we can see that TBISQ more packets received than CBISQ. This is due to the selection of trusted peers for the queries.

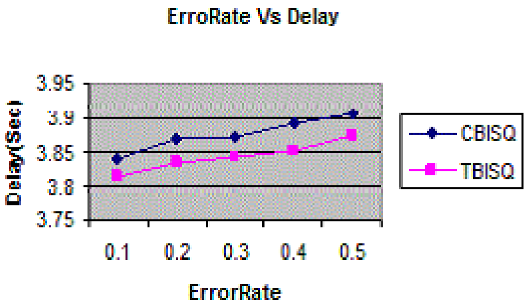

Fig. 2: Error Rate Vs Delay

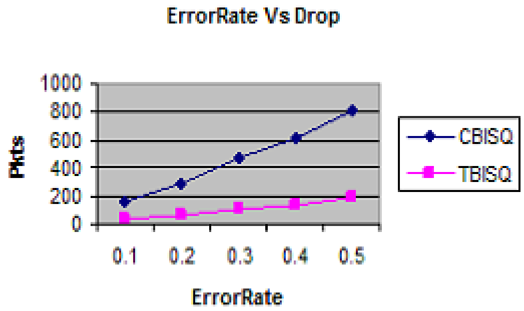

Fig. 3: Error Rate Vs Drop

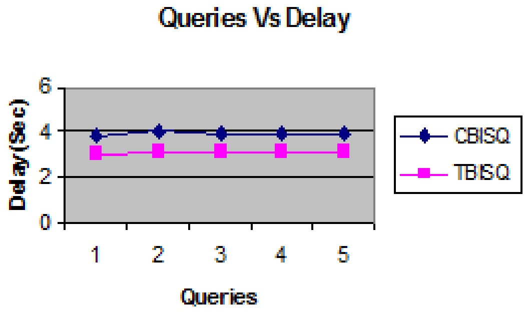

Fig.4 :Queries Vs Delay

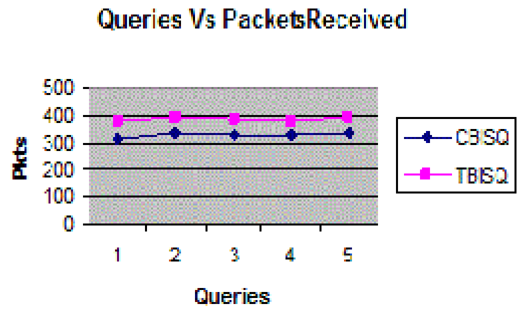

Fig.5: Queries Vs Packets Received

CONCLUSION

In this paper, we have proposed trust based query routing technique for P2P Networks. Initially the node with maximum trust value is chosen as cluster head. These cluster heads are designated as trust managers. At the time of implementing the trust routing decision, every peer has to maintain trustable table. If the update denotes that the node is reachable and trusted, the routing is performed. Otherwise its echo time is verified again to decide the re-routing process. Simulation results show that the proposed technique reduces the average response time and the packet drops due to failure and attacks, when compared to the existing technique. To achieve this caching mechanism we have proposed methods for caching the data packets in the peers and also to replace these data packets with the new data packets in the next routing process. The proposed work of caching mechanism with simulation results will be discussed in future work.

REFERENCES

1. Huaiqing Lin, Zhengbing Hu and Yonghong Zhou, "An Efficient Secure Multicast Communication for P2P Network", *Journal of Networks,* **6: 3**, (2011).
2. CAI Biao and LI Zhishu, "Computing and Routing for Trust in Structured P2P Network", *Journal of Networks*, **4: 7** (2009).
3. Quang Hieu Vu, "SPP: A Secure Protocol for Peer-to-Peer Systems", The Second International Conference on Advances in P2P Systems, (2010).
4. Mei Chen, Kenji Kita, and Xin Luo, "Cluster-Based Reputation Model in Peer-to-Peer Network", *International Journal of Machine Learning and Computing*,**1:4**, (2011).
5. Joonhyun Bae, Seunghun Lee, and Sangwook Kim, "VegaNet: A Peer-to-Peer Overlay Network for Mobile Social Applications", The 13th IEEE International Symposium on Consumer Electronics, (2009).
6. Hefeeda, Mohamed, Cheng-Hsin Hsu, and Kianoosh Mokhtarian. "Design and evaluation of a proxy cache for peer-to-peer traffic." Computers, IEEE Transactions on 60.7 : 964-977 (2011).
7. Zhao, Jing, Ping Zhang, Guohong Cao, and Chita R. Das "Cooperative caching in wireless p2p networks: Design, implementation, and evaluation." Parallel and Distributed Systems, IEEE *Transactions* on 21.2 : 229-241(2010).
8. José Santiago, Auguto Casaca and Paulo Rogério Pereira, " Multicast in Delay Tolerant Networks using Probabilities and Mobility Information", Journal on Ad hoc and wireless sensor networks, (2009).
9. Network Simulator: http:///www.isi.edu/nsnam/ns
10. Kolja Eger,Tobias Hoßfeld, Andreas Binzenhofer,"Efficient Simulation of Large-Scale P2P Networks:Packet-level vs. Flow-level Simulations", in proceedings of 2nd Workshop on the Use of P2P, GRID and Agents for the Development of Content Networks, pp: 9-16, (2007).
11. U. V. Arivazhagu and S. Srinivasan, "Cluster Based Intelligent Semantic Query Routing Technique in Peer to Peer Networks", *European Journal of Scientific Research*, ISSN 1450-216X **83 :1** , pp.15-24 (2012).
12. U.V.Arivazhagu Dr.S.Srinivasan ,International Journal of Cloud Computing and Services Sciences ,"Minimization of Delay for Query processing in Peer to Peer Networks",ISSN-2089-337 **1:2** (2012).
13. U.V.Arivazhagu Dr.S.Srinivasan, International Journal of Advanced Scientific and Technical research,"A Novel approach of Intelligent Query Routing Technique in Peer to Peer Network", ISSN:2249-9954 **4:2**, (2012).
14. U.V.Arivazhagu Dr.S.Srinivasan Intermational Conference on Advance Computing ,MIT University Chennai,"Ant Colony Optimization of Semantic Query Routing in Peer To Peer Networks " published in IEEE Conference publication
15. U.V.Arivazhagu Dr.S.Srinivasan International Conference on Modern Trends in Informnation Technology, Kulalampur, Malaysia ," Study of Cluster based approach and Security Query Routing in Peer to Peer Network" published in *international Journal of Computer Science and Electronics Engineering (IJCSEE)* **1:1** ISSN 2320–4028 (Online) (2013).