AN ADAPTIVE P2P TOPOLOGY EVOLVEMENT MODEL BASED ON INTEREST SIMILARITY

Li Yang, Changyou Xing, Yusen Zhang, and Jinshuang Wang

Institute of Command Automation,
PLA University of Science and Technology
Nanjing, China
xcy@plaust.edu.cn

ABSTRACT

To improve the resource location efficiency and guarantee resource download quality of nodes in P2P systems, we propose a node Interest bias based P2P Interest domain partition mechanism, give the concept of Interest similarity as well as its computation method, and then present an adaptive P2P topology evolvement model ISPT based on interest similarity ISPT. In ISPT, by computing interest similarity of each other, nodes with similar interest bias and service trust value are connected as neighbors. Since nodes that have similar interest are more likely to share resources, ISPT improves node resource query response efficiency, and provides an incentive mechanism to encourage node offer more contribution so as to get better service. Simulation results show that ISPT improves the efficiency and security of P2P topology effectively.

KEYWORDS

Peer to peer network; Topology model; Interest domain; Trust; Interest similarity

1. INTRODUCTION

More than half of today's Internet traffic is generated by P2P applications, which have great influence on Internet performance. However most of current P2P applications use randomly connected overlay topology, which has low resources location efficiency, and cannot defend malicious attack effectively. Thus how to organize peers to form an effective overlay topology in a P2P system becomes an urgent problem. Current studies show that peers in a P2P system have different interest bias, and peers that have similar interest are more likely to get services from each other (i.e. find the required resources to download) [1]. As a result, if organizing these peers together during constructing P2P overlay network, the resource location time can be decreased, and download success ratio can also be increased among peers with similar interest.

On the other hand, P2P system has open and anonymous features, which results in the fact that malicious nodes and free-riders can exist in the system. These peers have negative impact on system security and efficiency, and thus to decrease such impact, the difference of

DOI : 10.5121/ijcnc.2010.2605

peer trust value must be considered when constructing overlay network topology. Though there are some kinds of P2P topology construction methods that take peer trust into consideration, most of them consider peer behaviors in different domains as a whole, and thus the trust granularity is too coarse grain to describe the behavior details of peers in different interest domains. In [3] the authors proposed a domain trust based topology adjustment method, but nodes had to maintain different topologies for each interest domain, which results in high topology maintenance cost. Besides, the correlation of different interest domain is also hard to describe in that method.

To solve these problems, we give the concept of interest domain partition as well as interest similarity, and then propose an Interest Similarity based adaptive P2P Topology evolvement model ISPT. In ISPT, each peer declares its interest domain bias and maintains a service trust vector that represents its service trust value in each interest domain. Before constructing overlay network topology, the interest similarity values between nodes are calculated firstly, and then place nodes with similar interests together. By this means the resource location efficiency can be increased, and peers are given incentives to provide better service to others so as to get positive position in the overlay topology. Besides, malicious peers are repelled to network edge as punishment for their malicious behaviors. Simulation results show that ISPT is better than current typical topology construction method when taking both security and efficiency into consideration.

The rest of this paper is organized as follows. Section 2 provides a brief introduction of related works; Section 3 gives the basic concept of Interest similarity as well as its computation method, and provides the Interest similarity based P2P topology evolvement method ISPT; Section 4 gives some evaluation metrics of P2P network topology, and then evaluates the performance of ISPT by simulation; Finally section 5 concludes the paper, and gives a brief discussion on future works.

2. RELATED WORKS

Interest based P2P topology construction models try to connect nodes have similar interest together when constructing overlay topology, so as to increase the resource location efficiency. One of the key problems of Interest based topology construction models is how to determine interest similarity between different nodes, and typical determination metrics of current models include capability of nodes answer other nodes' query [4], and resource query similarity between different nodes [5]. Srip showed that if a peer has content that peer H_i is interested in, then the probability of it has other resources that peer H_i is interested in is also much higher, thus they proposed a model to connect nodes have similar interest so as to construct interest based resource query shortcut [1].

Cohen et al. proposed that peers stored similar files had similar interest, and they connected these peers to construct an associative overlay topology, which improved the capability of locating rare resources effectively [6]. In BestPeer system, each peer connected peers it thinks most valuable to it [7]. Condie connected each node with nodes that it can download resources with high probability, so as to decrease resource location latency [8]. Zhou et al proposed that node interest was determined by its resource bias, and they introduced interest to describe the statistics relationship between resource and topology [9]. Sardar et al propose a new protocol for building and repairing of overlay topologies based on the formation of interest-based super peers [10]. Giancarlo propose a self-organizing interest-based community: users in the same cluster share a subset of common items and are probably interested in other files popular in the cluster [11].

However, current interest based topology models are unfair to high trustable nodes, and they also cannot defend free-riders and malicious attacks effectively.

To reflect topology fairness, regarding nodes with similar interest bias, high trustable nodes should have superior position in the overlay topology. Thus, node trust should be taken into consideration when constructing overlay topology. Besides, there are many node trust calculation model nowadays [12-17], most of which are hot research topics. Though authors of [2, 3] used both interest bias and trust to help topology constructing, the trust metric granularity of [2] is too coarse grain to describe trust differences of nodes in different domains, and thus it cannot defend malicious nodes behaviors efficiently. [3] proposed a domain model to describe node interest bias, and it also used ontology similarity to measure the interest correlation between different domains. But the model in [3] has to maintain a logical topology for each interest domain, which increases the system complexity. Besides, correlations between different interest domains are also hard to describe, which decrease the computation accuracy of domain trust.

3. Interest Similarity based Topology Model

Figure 1 describes the resource query process of peers in unstructured P2P system. When peer H_i wants to acquire some resource, it will firstly query its neighbors using flooding methods. For each neighbor of H_i, it will return the information to H_i if having such queried resources; otherwise it will forward the query message to its neighbors instead. Since peers have similar interest are more likely to share resources with each other, by organizing peers with similar interest as neighbors, we can increase hit rate of resource query effectively, and thus decrease network query message traffics.

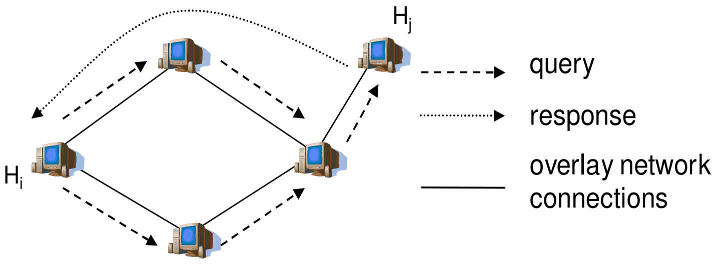

Figure 1. Resource query in unstructured P2P networks

If there are malicious peers in the system, they can cheat H_i by answering that they have the queried resource and provide a fake resource to H_i, but the upper query process cannot determine whether a response is true or fake. In order to solve such problem, P2P trust mechanisms are introduced to identify malicious nodes. Generally node has different trust values in different domains, for example some nodes like to share music with others, and thus they are more trustable in music domain. Others like to share software, and thus we should prefer to download software from these nodes. However, current P2P trust models accumulate trust values of nodes in different domains together, and use this accumulated value to help constructing overlay network topology. This method is unfair to high trustable nodes in specific domain, and by accumulating trust values in different domains together, it also hides malicious behaviors of nodes in specific domain, and thus decrease resource locating efficiency as well as response quality. To solve these problems, we propose an interest similarity based adaptive P2P topology evolvement model named ISPT, which takes both node interest bias and trust values in each interest domain into consideration, and uses domain service trust vector to describe behavior details of nodes in different domains. ISPT organizes nodes with similar interest bias and similar service trust value vectors as neighbors in overlay network topology, and thus increases the resource location efficiency as well as resource response quality.

Figure 2 gives the basic features of ISPT: resources are classified into different interest domains according to the pre-definitions, such as music, movie, math, computer, et al. Each node states its interest domains bias when joining the system, and maintains an interest domain service trust vector, in which each dimension represents the service trust value of the node in a specific domain. Service trust value is 0 means the node has no interest in such domain or it provides no effective resources to other nodes in such domain. The interest similarity between every two nodes can be calculated using their domain service trust vector, and each node will select nodes that have more similar service trust vector with it as neighbors. In this model, the key concepts include interest domain partition, domain service trust value, and domain service trust vector and interest similarity. We will discuss each of them in the following sections, and give the detailed description of ISPT.

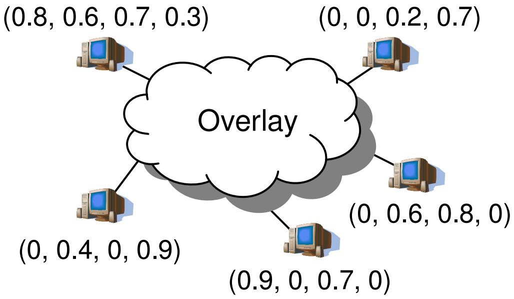

Figure 2. domain service trust vector

3.1. Computation of Interest Similarity

Suppose there are *n* kinds of resources in a P2P network, $U = \{C_1, C_2, ..., C_n\}$, and each kind of resource is corresponding to an interest domain, thus there are *n* interest domains in the network. Node H_u is interested in *m* kinds of resources in ***U*** ($m \le n$), and we use a m-dimension vector $\boldsymbol{I_u}$ to describe the interest bias of node H_u, $I_u = \{C_k \mid C_k \in U, k \le n\}$, thus $I_u \subseteq U$. Each node H_u declares its interest bias vector $\boldsymbol{I_u}$ when joining the system, and this vector can also be adjusted dynamically. After each transaction, the transaction nodes will give trust evaluation of each other in the specific transaction domain. According to the concept of interest domain and the trust computation methods proposed in [13], we firstly give the related definitions of interest domain trust under the condition of multi interest domain.

Definition 1 Domain Connection Trust: For any nodes H_u, H_v and H_j, if H_u and H_j are neighbors, and the query message of H_u for some resources in interest domain C_k arrives H_v through H_j, then we can define the domain connection trust of H_u to H_j $W_{uj}(k)$ as follows.

```
if download successful
    $W_{uj}(k) = W_{uj}(k) + 1;$
else
    $W_{uj}(k) = W_{uj}(k) - 1;$
```

Definition 2 Domain Recommendation Trust: For any two nodes H_u and H_v, suppose $S_{uv}(k)$ and $F_{uv}(k)$ represent the number of successful and unsuccessful transactions in interest domain C_k, and $R_{uv}(k)$ represents the domain Recommendation trust value of node H_u on H_v in interest domain C_k, then we have

$$R_{uv}(k) = \frac{\max(S_{uv}(k) - F_{uv}(k), 0)}{\sum_{m} \max(S_{uv}(k) - F_{uv}(k), 0)} \tag{1}$$

Definition 3 Domain Service Trust: For any nodes H_u and H_v, suppose $T_u(k)$ and $T_v(k)$ represent the domain service trust value of node H_u and H_v in interest domain C_k. Then

$$T_u(k) = \sum_{v} (R_{vu}(k) \times T_v(k))$$

(2) **Definition 4 Domain Service Trust Vector**: For any node H_u, the domain service trust vector $\vec{T}_u$ can be represented as follows.

$$\vec{T}_u = \{T_u(k) \mid C_k \in I_u\} \tag{3}$$

Domain recommendation trust value records the local trust evaluation of a node H_u to node H_v according to transaction behaviors history of them in a specific interest domain, and domain service trust value of H_u describes the behavior trust of node H_u in a specific interest domain, which is the accumulation value of all nodes' evaluations to node H_u in a specific domain. Domain service trust vector represents the service trust value of nodes in each interest domain.

Definition 5 Interest Similarity: Interest similarity represents the similarity between node's domain service trust vectors. For any two nodes H_u and H_v, we use the cosine function to measure the similarity between two service trust vectors. Suppose ITS_{uv} represents the Interest similarity between H_u and H_v, then:

$$ITS_{uv} = \frac{\sum_{k=1}^{n} T_u(k) \cdot T_v(k)}{\sqrt{\sum_{k=1}^{n} (T_u(k))^2 \cdot \sum_{k=1}^{n} (T_v(k))^2}} \tag{4}$$

In which $T_u(k)$ and $T_v(k)$ represent the domain service trust value of node H_u and H_v in interest domain *C*. From the definition we can see that for any two peers H_u and H_v, if the number of same interest domains is large, and the service trust value in each interest domain is similar, then the similarity value computed through equation (4) will also be large. Thus through equation (4) we can find out nodes with similar domain service trust, and then organize them together.

3.2. P2P Topology Evolvement Model based on Interest Similarity

Based on the upper definitions, we propose the topology model ISPT as follows, which includes processes of new nodes join network, resource query and download, topology maintenance, and we will describe each of them in detail. Suppose $N(H_u)$ represents neighbors set of node H_u, and $Num(H_u)$ represents the upper threshold of the number of node H_u's neighbors.

(a) When joining the network, each node declares its interest bias vector. Since node accumulates no trust value at this time, ISPT only uses node interest bias similarity (the number of same interest domains between the two nodes) to choose neighbor nodes. The basic operation is shown as follows.

```
function JoinNetwork() {
    R:=Random set of random IP addresses
        from pong server;
    R1:= Sort peers in R by number of same
        Interest Domain in descending order;
    foreach $H_v \in R1$ do
    if Connect_request($H_u$,$H_v$)=true then
        Add_neighbor($H_v$);
    if $|N(H_u)| \geqslant Num(H_u)$ then
        return;
}
```

(b) During the transaction, nodes can be divided into query peers and response peers. The operations of node H_u as query peer are shown as follows.

(b.1) Initiate the query request, and send resource query messages to all neighbors using flooding method.

(b.2) After receiving response messages, H_u will select a node H_v from the response nodes set to download resource according domain service trust value.

(b.3) Update the domain recommendation trust value of H_u to H_v and domain connection trust of related intermediate node between H_u and H_v according to download status.

(b.4) Announce the updated domain recommendation trust value of H_u to node H_v.

(b.5) Update overlay network topology.

The core operation of upper process is the last 3 steps, which is described as follows.

```
function Topology_Adjust() {
   if download_satisfactory then {
      $S_{uv}(k)=S_{uv}(k)+1$; //increase $S_{uv}(k)$ to node $H_v$ in $C_k$
      if $H_u$ query msg arrives $H_v$ through $H_j$
            $W_{uj}(k)= W_{uj}(k) +1$;
      if (not neighbor($H_u$, $H_v$) and ($S_{uv}(k)$-$F_{uv}(k) \geqslant C_{Threshold}$))
         Add_Neighbor($H_v$); //add $H_v$ as neighbor
       Report the recommendation trust to node $H_v$ in $C_k$
    }
   else {
      $F_{uv}(k)=F_{uv}(k)+1$; // increase $F_{uv}(k)$ to node $H_v$ in $C_k$
      if $H_u$ query msg arrives $H_v$ through $H_j$
           $W_{uj}(k)= W_{uj}(k) - 1$;
      if(neighbor($H_u$, $H_v$))
        Disconnect($H_v$); //disconnect node $H_v$
      else if($W_{uj}(k)<W_{Threshold}$)
         Disconnect($H_j$); // disconnect node $H_j$
      Add_Neighbor(null); //add new neighbor
   }
```

In which adding neighbor Add_Neighbor procedure includes two kinds of operations: adding a known node as neighbor, or selecting nodes from the system as neighbor according to interest similarity criterion. The main operation steps of this procedure are shown as follows.

```
function Add_Neighbor($H_v$) {
   if($H_v$==null)
      Find node $H_v$ with largest $ITS_{uv}$ ;
   else if $|N(H_u)| \geqslant Num(H_u)$ {
      Find node $H_m$ with smallest $ITS_{um}$;
      Disconnect($H_m$);
   }
  Add node $H_v$ as neighbor;
}
```

The operations of node H_v as response peer are shown as follows.

(c.1) Response the query message, and provide download to query peer H_u according to H_u's request.

(c.2) Update the domain service trust value of itself according to domain recommendation trust announced by peer H_v.

(c.3) Announce the updated domain service trust value.

From the upper discussion we can see that ISPT has the following advantages:

- When constructing topology, nodes select neighbors according to interest bias similarity, and thus it can combine nodes with similar interest together, and help decreasing resource location time.

- During the transaction, the topology is updated adaptively according to node interest similarity, thus the node behaviors in each specific domains are preserved. Nodes are given incentives to provide better service to other nodes in order to get better service and favorable position in the topology, which reflects the topology fairness. Besides, malicious nodes are repelled to network edge, and thus the harmfulness that they can do to the system are decreased as much as possible.

4. EXPERIMENTS RESULTS AND ANALYSIS

In order to evaluate the performance of ISPT model, we firstly give the typical evaluation metrics for P2P network topology model, and then we implement ISPT based on the query cycle simulator developed by Stanford University [18], finally the performance of ISPT and APT is compared using the upper metrics.

4.1. Evaluation Metrics

(1) Network Average Cluster Coefficient. This metric quantifies the nodes cluster effect of a specific model. If there are *N* nodes in the network, equation (5) gives the definition of network average cluster coefficient.

$$C = \frac{1}{N} \sum_{i=1 \ldots N} \frac{2E_i}{k_i(k_i - 1)} \tag{5}$$

In which k_i represents the number of neighbors of node H_i, and E_i represents the number of logical connections between the k_i neighbors (that is, the number of neighbors of node H_i's neighbors). Larger network average cluster coefficient value means better cluster capability of nodes that have similar interest, which can help decrease resource location time.

(2) Content Similarity. This metric measures the content correlation degree between two nodes. For any nodes H_i and H_j, if there are *n* kinds of resources (That is, the number of system interest domain is *n*), and the ratio of the number of share files by node H_i in interest domain *k* and its total number of share files is c_{ik} , then we define the content similarity between node H_i and H_j as follows.

$$S(i,j) = 1 - \frac{1 - \sum_{k=1}^{n} | c_{ik} - c_{jk} |}{2} \tag{7}$$

Based on this definition, if ***P*** represents network nodes set, and *N*(*i*) represents neighbor set of node H_i, then the average node content similarity of the system is defined as follows.

$$avgS = \frac{1}{|P|}\sum_{i\in P}\sum_{j\in N(i)} S(i, j) \tag{8}$$

(3) Connection Ratio. This metric describes the probability of nodes have same content similarity are neighbors. If the number of node that have content similarity *p* is *N*, and of which *M* pairs are neighbors, then we define the connection ratio of content similarity *p* is

$$LR(p) = \frac{M}{N} \tag{9}$$

For a specific nodes set with content similarity *p*, The higher of *LR*(*p*), the better of its cluster effect.

(4) Network Query Traffic. This metric describes the average number of duplicate query messages when node initiates a query. Since each node will forward the query message to its neighbors unless it has the requested resource, smaller network query traffic means higher resource location efficiency of the model.

(5) Average Malicious Path Length. This metric describes the average distance between malicious nodes and good nodes in the system, and thus it also represents the repulsion effect of malicious nodes in the system. The longer of average malicious path length is, the better of malicious nodes being repelled to network edge.

$$avgMPL = \frac{1}{|M|}\sum_{i\in M}\left(\frac{1}{|P\setminus M|}\sum_{j\in P\setminus M} SP(i, j)\right) \tag{10}$$

In which ***P*** is the network nodes set, ***M*** represents malicious nodes set of the system, $P\setminus M$ represents good nodes set of the system, and $SP(i, j)$ represents shortest path length between node H_i and H_j.

4.2. Performance Analysis of ISPT

Table 1 describes the simulation experiment parameters, and in each simulation experiment we run 180 round, and we run the total experiment 5 times to compute the average results.

Table 1. Simulation Parameters.

Network Parameters	Number of good nodes	100
	Initial number of good node neighbors	3
	Number of malicious nodes	10
	Initial number of malicious node neighbors	5
	Max number of node connections	10
	TTL of query message	3
Content Distribution	Content distribution model of good nodes	Zipf
	File distribution model of good nodes	Same as [4]
	Total number of content types	20

	number of content for good node	≥6
Node Behavior	Probability of malicious node answer query	20%
	Probability of malicious node return fake file	100%
	Download source selection algorithm	domain service trust based probability algorithm

Based on simulation results, we use performance evaluation metrics proposed in section 4.1 to compare the performance of ISPT and APT.

Figure 3 describes the average cluster coefficient comparison between the two models. From Figure 3 we can see that under the condition of each node maintains at most 10 neighbors, after running a while, the cluster coefficient of ISPT is near 0.55, but that of APT is only 0.25, which shows that ISPT can organize nodes that have similar interest together much better, and thus it helps increase node resource query hit rate, and decrease the resource location time.

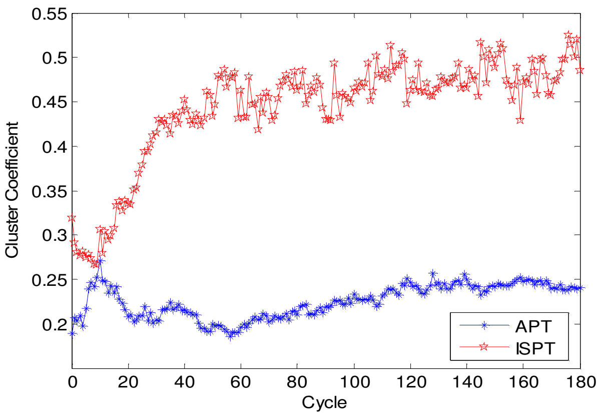

Figure 3. Network average cluster coefficient

Figure 4 shows the average content similar value between neighbor nodes, from which we can see that at the beginning of topology construction, the content similarity of ISPT is about 0.4, but that of APT is only about 0.25. As the increase of time, the average content similar values of both models are increased too, but that of ISPT is always higher than that of APT. The main reason is that after each transaction, both models use the accumulated trust value as standard of selecting new neighbors, and thus nodes that transact with each other more times and have similar contents become neighbors with each other. However, APT accumulates node behaviors in all interest domains into a whole trust value, and ignores the behavior details of node in each specific domain. ISPT uses interest domain trust vector to maintain the behavior details in each domain, and thus it can get the more accurate content similarity.

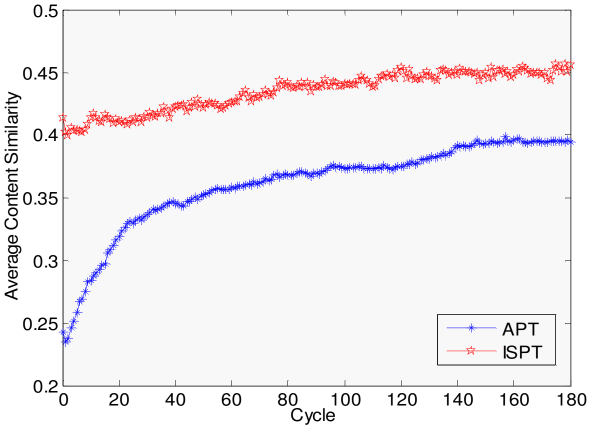

Figure 4. Average content similarity of neighbor nodes

Figure 5 describes the node content similarity based connection ratio. We can see that when the content similarity is smaller than 0.5, the connection ratio of APT is larger than that of ISPT, but when the content similarity is larger than 0.5, the result becomes contrary. This phenomenon means that in ISPT nodes with high interest similarity are more likely to be neighbors with each other. The key reason is that ISPT uses interest similarity to construct overlay topology, nodes that have higher content similarity are more likely to transact with each other, and thus the query hit rate is increased. On the contrary, APT has no such features.

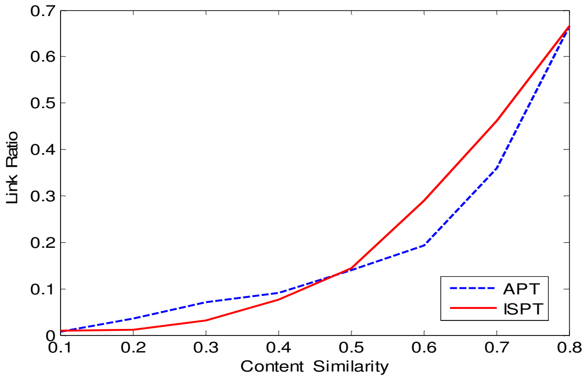

Figure 5. Content similarity based connection ratio

Figure 6 shows that the number of ISPT query messages in each query cycle is much smaller than that of APT. The main reason is that ISPT has a better similar interest node cluster feature, and node can find requested resources within a smaller query scope, thus the query traffic in the network is decreased effectively. When taking APT into consideration, each query message has to be forwarded a large number of times before reach the node that has requested resource. Thus the number of APT query message is much larger than that of ISPT under the same condition, and it wastes network resources as well as resource locating times compared with ISPT.

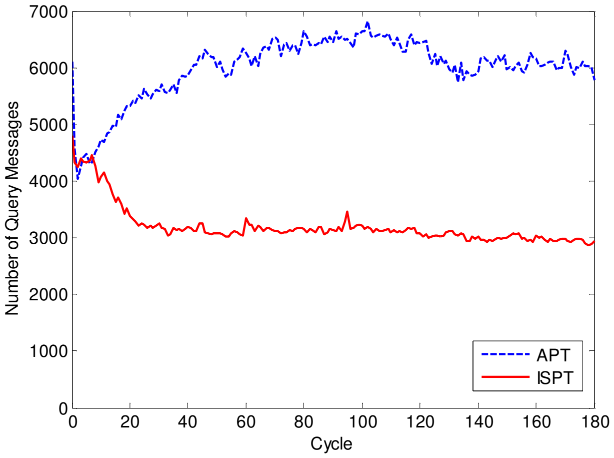

Figure 6. Query message traffic

Figure 7 shows the malicious path length comparison of ISPT and APT when malicious nodes answer query messages with probability 0.5. Because all malicious nodes are repelled to network edge, and there is no connection between good nodes and malicious nodes after 100 round simulations (we use the length 6 to represent unreachable), Figure 7 only gives performance comparison of the two models in first 100 rounds. At the beginning, APT uses maximum node degree principle to designate neighbors for good and malicious nodes, but ISPT only uses such principle to designate neighbors for malicious nodes, and for good nodes it uses the number of same interest domain as criterion to cluster nodes. Thus the initial vision field of malicious nodes in ISPT is smaller than that in APT, which decreases the initial average malicious path length of ISPT. As the construction of nodes service trust, malicious nodes are repelled to network edge, and thus the average malicious path length keeps on increasing. Besides, since both interest and trust take effectiveness in ISPT, malicious nodes can be discovered and repelled to network edge more effectively.

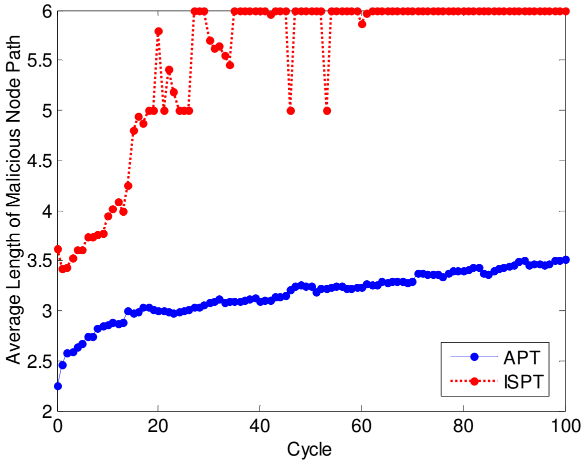

Figure 7. Average malicious path length

From the upper discussion we can conclude that ISPT is better than APT in increasing network cluster coefficient, increasing connection ratio of nodes with similar contents, decreasing network query traffic and repelling malicious nodes to network edge. The key reason of such results is that through interest domain partition, ISPT takes nodes interest bias into consideration at the beginning of topology construction, and it organizes nodes with similar interest as neighbors, so that resource location efficiency is high at the beginning. During the topology maintenance stage, ISPT pays attention to both node interest bias and node trust similarity in each interest domain, and thus it can increase the cluster coefficient effectively, and strengthen the capability of repelling malicious nodes to network edges.

5. CONCLUSIONS

To help increase the resource location efficiency and guarantee resource download quality in unstructured P2P systems, we give the concept of interest domain partition and interest similarity, and then propose a node interest similarity based adaptive P2P topology evolvement model ISPT. Based on different interest bias and trust variance of nodes in P2P system, ISPT organizes nodes that have similar interest bias and domain service trust as neighbors, and thus increase the system resource location efficiency. Besides, by using interest similarity metric during neighbor selection stage, ISPT can also defend malicious nodes attacks and give nodes incentives to provide better service to others so as to get good position in the overlay network topology. Analysis and simulation results show that ISPT is more effective than typical P2P topology model APT both in efficiency and security metrics. Since in this paper we only pay attention to the overlay topology construction process, and do not give further discussion on problems related to interest domain trust model. In the further work, we will study on how to construct recommendation based P2P trust model using information provided by ISPT.

REFERENCES

[1] Sripanidkulchai K, Maggs B, and Zhang, H (2003) "Efficient content location using interest based locality in peer-to-peer systems", IEEE Infocom 2003. San Francisco: IEEE Press.

[2] Condie T, Kamvar S D, and Garcia-Molina H, (2004) "Adaptive peer-to-peer topologies", 4th International Conference on Peer-to-Peer Computing 2004. New York: IEEE Computer Society Press. pp53-62.

[3] Zhang Q, Zhang X, and Liu J R, (2007) "An efficient adaptive evolvement protocol for peer-to-peer topologies", Journal of Software, Vol. 18, No. 2, pp400–411.

[4] Ramanathan M K, Kalogeraki V, Pruyne J. (2002) "Finding good peers in peer-to-peer networks", IEEE International Parallel and Distributed Processing Symposium 2002. Fort Lauderdale: IEEE Computer Society.

[5] Iamnitchi A I. (2003) “Resource Discovery in Large-Scale Distributed Enivorments”. Ph.D Thesis. The University of Chicago, 2003.

[6] Cohen E, Fiat A, and Kaplan H, (2007) “Associative Search in Peer-to-Peer Networks: Harnessing Latent Semantics”, Computer Networks, Vol. 51, No. 8, pp1861-1881.

[7] Huang W, Huang M, Chen J, (2003) “A novel peer-to-peer system based on self-configuration”. Journal of Software, Vol. 14, No. 2, pp 237-246.

[8] Condie T, Kamvar S D, Garcia-Molina H. (2004) “Adaptive peer-to-peer topologies”. IEEE International Conference on Peer-to-Peer Computing 2004 . Zurch: IEEE Computer Society.

[9] Zhou X B, Zhou J, Lu H C, and Hong P L, (2007) “A layered interest based topology organizing model for unstructured P2P”, Journal of Software, Vol. 18, No. 12, pp3131–3138.

[10] Sardar K, Ashraf K, and Laurissa N T, (2009) “Interest-Based Self Organization in Group-Structured P2P Networks”, IEEE CCNC2009. Las Vegas: IEEE Press. pp1237-1241.

[11] Giancarlo R, and Rossano S, (2009) “A peer-to-peer recommender system based on spontaneous affinities”, ACM Transactions on Internet Technology, Vol. 9, No. 1, pp1-34.

[12] Dai Z F, Wen Q Y, and Li X B, (2009) “Recommendation Trust Model Scheme for P2P Network Environment”, Journal of Beijing University of Posts and Telecommunications, Vol. 32, No. 3, pp69-72.

[13] Kamvar S D, Schlosser M T, and Hector G M, (2003), “The EigenTrust Algorithm for Reputation Management in P2P Networks”, WWW 2003. Budapest: ACM Press. pp640-651.

[14] Li J T, Jing Y N et al. (2007) “A Trust Model Based on Similarity-Weighted Recommendation for P2P Environments”. Journal of Software, Vol. 18, No. 1, pp157-167.

[15] Peng D S, Lin C et al. (2008) “A Distributed Trust Mechanism Directly Evaluating Reputation of Nodes”. Journal of Software, Vol. 19, No. 4, pp946-955.

[16] Hu J L, Wu Q Y et al. (2009) “Robust Feedback Credibility-Based Distributed P2P Trust Model”. Journal of Software, Vol. 20, No. 10, pp2885-2898.

[17] Shi Z G , Liu J W et al. (2010) “Dynamic P2P trust model based on time-window feedback mechanism”. Journal of Communications , Vol. 31, No. 2, pp120-129.

[18] Query Cycle Simulator, http://p2p.stanford.edu/www/qcsim.htm.