I.J. Wireless and Microwave Technologies **2012, 1, 17-22**
Published Online February 2012 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2012.01.03

Available online at http://www.mecs-press.net/ijwmt

A Design of Trust Degree Transfer Algorithm for P2P Network

[a] Wang Hao-yu, [b] Ge Tong-min, [c] Ji Xiao-juan, [d] Hu Bao-an

[a] *Automobile Transport Command Department of Military Transportation University Tianjin, the People's Republic of China*
[b] *Military Transportation Department of Military Transportation University Tianjin, the People's Republic of China*
[c ,d] *General Courses Department Military Transportation University Tianjin, the People's Republic of China*

Abstract

The design of mechanism is used to calculate node reliability of incredible P2P network. The mechanism through matrix shows the trust relationship between nodes in the network, through matrix operation realizes the trust transfer process fast, and through a trusted server provides calculation service of trust degree for nodes in P2P network.

Index Terms: P2P Network; Trust Degree; Algorithm

P2P (peer-to-peer) network is also known as peer to peer network. The essential difference between P2P network and C / S (Client / Server) is: in the entire P2P network, information resources are symmetrically two-way transmitted and exchanged between peer entities; each node serves as resources consumer and resources provider at the same time, and nodes in the network have corresponding rights and obligations. Besides providing the user with convenience of shared resources, P2P network has serious safety hidden danger. P2P network needs a trusty and safe environment, thus the trust management technology of P2P network came into being.

1. Introduction

P2P network is a distributed system structure with high extendibility, and peer-to-peer means the same logical status of physical nodes in the network. Its essence is to transfer management from centralized model to decentralized model, and to transfer resource content from server node of C / S (see Figure 1) to ordinary node in P2P network (see Figure 2). This distributed structure makes full use of processing capacity and potential resources of ordinary terminal in the Internet. So far, the structure of P2P network can be divided into three typical kinds of network models, and each model has advantages and disadvantages.

Corresponding author:
E-mail address: [a] 993269458@qq.com, [b] wanghaoyu8668@sina.com, [c] wanghaoyu8668@yahoo.cn, [d]wanghaoyu8669@sina.com

1.1. Centralized Contents P2P Network Structure

The centralized contents P2P network structure is the earliest P2P application model, and because of its centralization, it is considered as non-pure P2P structure. Its processes of user registration and document retrieval are similar to those of traditional C / S model; while its difference is all resources are not stored on the server, but stored in each node.

The centralized contents P2P network structure uses star structure, the peer node in the group connects with the central directory server, and distributes the list of shared files to the server. Resources request node commands the central directory server to retrieve, after getting the response, according to information of network traffic and delay etc, the node selects appropriate resources node to establish connection. Thus resources exchange can be carried out between two peer nodes.

The centralized contents P2P network structure weakens the concept of server in traditional C / S structure, and improves greatly on extendibility and stability. The structure is simple, and with rich shared resources. But it has some unavoidable problems, that is, the central server becomes the network bottleneck and causes copyright dispute on shared resources.

1.2. Pure Distributed P2P Network Structure

The pure distributed P2P network structure is widely known as broadcast P2P network structure. It cancels centralized central server, each user gets random access to the network, and connects with adjacent set of nodes through end to end connection. The request of each node is directly broadcasted to the peer node connected, and is broadcasted from each peer node to the adjacent node connected in the same way, until the requesting node receives response from the requested node or reaches maximum step of flooding, which is defined as a retrieval technology to prevent the system from unrestricted circulation and its value is usually set from 5 to 9. After getting the identity of the node with resources, the node which initiates the request can directly ask for service from such node.

The pure distributed P2P network structure solves the decentralization of network structure. Therefore, it has good extendibility and fault tolerance; but because the resources search algorithm is carried out through flooding and a lot of bandwidth is used to control the information, network congestion is likely to be caused; at the same time, such pure distributed structure is more vulnerable to malicious attacks.[1]

1.3. Hybrid P2P Network Structure

On the basis of the pure distributed P2P network structure, the hybrid P2P network structure introduces the concept of “search node”, and divides node into “ordinary node” and “search node” according to different transaction capabilities. Search node and adjacent ordinary node form an “autonomous cluster”, which uses P2P structure with basis centralized directory structure, and each search node between different clusters is connected through the pure P2P structure.

Super node, absorbing advantages of centralized directory and flooding request model, improves the efficiency of inquiry and uses two-tier framework with search node. It can realize intelligent flooding inquiry, but the vulnerability of the search node may lead to isolation of nodes in the cluster.[2]

2. Evaluation Mechanism of Trust Transfer

2.1. Background Information

Usually, nodes in P2P network accomplish the common goal through cooperation; but in the untrusted environment, to achieve benefit maximum, nodes may violate the cooperation agreement. One of the most typical examples is the vampire problem of file-sharing P2P network, which means node in the file-sharing network downloads data from the network while never uploads data, making full use of network bandwidth and

computing resources. In addition, in the information-releasing P2P networks, some nodes may release illegal information or malicious information (such as viruses, Trojans, etc.) or make DOS attack to arouse abnormality in the network.

To solve the problem caused by untrust between nodes, many P2P networks design a mechanism to evaluate trust relationship between nodes. Thus cooperation between nodes will be selected based on the trust relationship to avoid problems mentioned above.

2.2. Problem Description

Suppose there are n nodes in the P2P network, and each node has certain trust in other nodes of the network, thus this kind of trust can be represented as a real number of [0．．1], where 0 stands for untrust and 1 stands for complete trust. Combining together, these trust relationships can be seen as matrix T，T, and its row i and column j can be seen as the trust degree of node i to node j.

In addition, through interaction with neighbors in the network, each node gets a decision on neighbors' behavior, and such decision can be represented as a real number of[－1．．1], where －1 means neighbors' behavior is totally incompatible with the cooperation agreement and l means neighbors' behavior is totally compatible with the agreement. Combining together, these decisions can form a sparse matrix F, and its row i and column i can show the decision of node i to node j. Unadjacent node in matrix can be identified as a specific number, such as 0, and the data of such node will not be considered in sequent algorithm.

The trust degree evaluation of P2P network can be seen as, within a certain period of time, through collecting behaviors of adjacent nodes, the node generates the matrix mentioned above and estimates the future trust relationship T'according to a priori trust relationship T'. Here is the mathematics description of the problem.

P2P network can be abstracted into a bipartite graph G(V，E) with n nodes, where V is the integration of nodes in the network and E is the integration of communication link in the network. Any node i in graph G(V，E) can get F_{ij}，（＜i，＞j∈E），the probe assessing of j, the adjacent node of i in the network. At the same time, to k, all nodes in G, i has a trust degree assessing, T_{ik}，(i，k∈V) . In the initialization of the entire P2P network, T_{ij} has a priori assumption (initial value); then in the process of network operation, after a certain period of time, evaluation algorithm makes constant impact on T by using F, that is to design a function f and use f（T，F）as the updated value of T.

The following are two essentials of trust evaluation algorithm:

1) Accuracy. That is to say T, the output structure of the algorithm, can measure the trust relationship between nodes correctly.

2) Rapidity. That is to say when the node behavior suddenly changes, the trust relationship between nodes can be adjusted within several time slice, such as if a node in P2P network makes an attack on the network, as a result, the trust degree of the network towards such node should be rapidly declined.

3. Trust Degree Transfer Algorithm

In the algorithm, a "transfer" refers to the process of sending knowledge of a node in the network to the other node in the network. This algorithm defines four modes of transfer (see Figure 3).[4]

1) Transfer element T. Considering trust degree of node i and node j, two nodes in the network, if node i trusts k, an adjacent node of node j, that is to say, to a certain extent, i trusts behavior evaluation that k made towards its adjacent nodes (including j). Based on this consideration, the trust degree between node i and node j can be expressed as:

$$T_{ij} = \sum_{k \in v} T_{ik} \cdot F_{kj} \quad (1)$$

From the entire matrix, transfer element T can be seen as the multiplication of matrix T and matrix F.[3]

2) Transfer element T'. Also considering trust degree of node i and node j, if k, an adjacent node of j, trusts i, that is to say, to a certain extent, i trusts behavior evaluation that k made towards its adjacent nodes (including j). Based on this consideration, the trust degree between node i and node j can be expressed as:

$$T_{ij} = \sum_{k \in v} T'_{ik} \cdot F_{kj} \tag{2}$$

From the entire matrix, transfer element T'can be seen as the multiplication of transpose matrix of T and matrix F.

3) Transfer element TT'. Also considering trust degree of node i and node j, if k, an adjacent node of j, to some extent, shares the same "trust mode" with i, that is to say, node i and node j share trust in a lot of nodes, and to a certain extent, i trusts evaluation that k made towards its adjacent nodes (including j). This kind of transfer can be expressed as:

$$T_{ij} = \sum_{k \in v} \{ \sum_{u \in v} T_{iu} T'_{uk} \} \cdot F_{kj} \tag{3}$$

From the matrix, this transfer mode can be seen as the multiplication of TT'and matrix F.

4) Transfer element T'T. Transfer element T'T is similar to transfer element TT', but is different from the direction of the trust relationship. Its transfer formula is:

$$T_{ij} = \sum_{k \in v} \{ \sum_{u \in v} T'_{iu} T_{uk} \} \cdot F_{kj} \tag{4}$$

That is the multiplication of T'T and matrix F.

It is clear that the four kinds for transfer elements mentioned above transfer the node evaluation a step forward along the trust direction. But in practice, just one-step transfer is not enough, usually it is required to transfer information of one node to more distant nodes to realize the rapidity mentioned. Therefore, the whole process of transfer can be described by the following formula.

When the trust degree assessing of the entire network needs to be updated, calculating transfer matrix P, and calculating matrix T_{new}, the new evaluation matrix, from matrix T, the old evaluation matrix.

$$T_{new} = \alpha T + (1 - \alpha) P \times F \tag{5}$$

Where $0<\alpha<1$ is the sensibility parameter of transfer algorithm towards reaction of probe; the higher α is, the lower sensibility of evaluation towards probe will get.

And P is obtained as follows:

$$P = \sum_{k=1}^{n} \lambda^k (\mu_1 T + \mu_2 T' + \mu_3 T'T + \mu_4 TT')^k \tag{6}$$

Where λ is the time decrement factor, μ_1, μ_2, μ_3, μ_4 are four impact factors of transfer element and can be adjusted according to the actual need of the network.

In P2P network, to use the algorithm mentioned above, firstly, supposing a trusted server TS to calculate and update evaluation value of all nodes in the core network; then distributing evaluation value to all nodes in the network. After each time slice, according to the unified algorithm, all nodes in the network will quantify the behavior of all neighbors detected within the time slice to form a vector to estimate the behavior of surrounding nodes (i.e. any row in F), and transfers to TS. After receiving data from all nodes, TS carries out the algorithm, and gets matrix T, the evaluation matrix between nodes in the network, and then distributes to corresponding node.

4. REFERENCES

[1] Chen Xiangyun. Trust Management Research on P2P Network. Jiangsu Communication. 2009.
[2] BEKSON T. Skype Security Evaluation. Anagram Laboratories. 2005.
[3] GUHA R, KUMAR R, RAGHAVAN P, et al. Propagation of Trust and Distrust. WWW. 04 : Proceedings of the 13th international conference 0n Wodd Wide Web . New York , NY , USA. ACM. 2004. 403-412.
[4] BuCHERGGER S , BOUDEC J . L . A P . obust Reputation System for Mobile Ad—hoc Networks. EPFL, IC Technical Keport IC／2003／50, 2003.

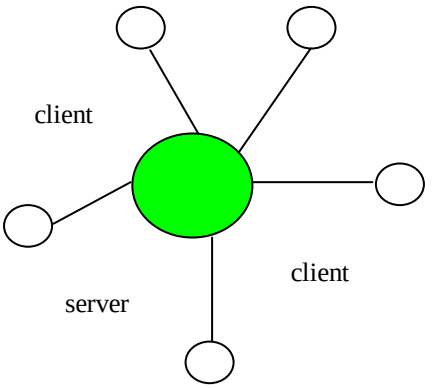


Figure 1 Network Structure of C / S

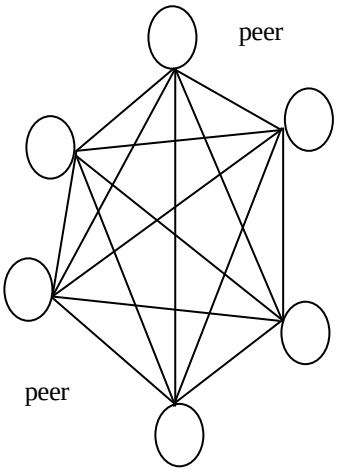
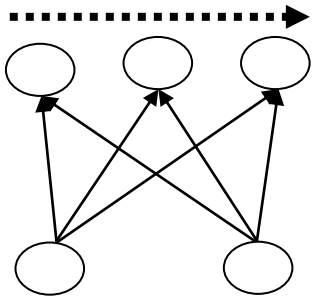
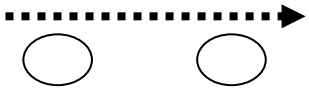


Figure 2 Network Structure of P2P

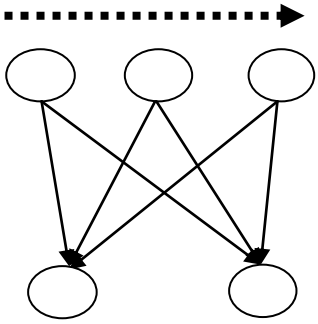
Transfer Element T



Transfer Element TT'



Transfer Element T'



Transfer Element T' T

Figure 3 Transfer Element