Computer Communications 33 (2010) 997–1004

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

A secure model for controlling the hubs in P2P wireless network based on trust value

Yuhua Liu [a], Naixue Xiong [b], Yuling Li [a], Kaihua Xu [c], Jong Hyuk Park [d,*], Chuan Lin [e]

[a] Department of Computer Science, Huazhong Normal University, Wuhan, China
[b] Department of Computer Science, Georgia State University, Atlanta, GA, USA
[c] Research Center of the Digital Space Technology, Huazhong Normal University, China
[d] Department of Computer Science and Engineering, Seoul National University of Technology, Republic of Korea
[e] School of Mathematics and Statistics, Wuhan University, China

ARTICLE INFO

Article history:
Received 27 July 2009
Received in revised form 19 November 2009
Accepted 13 January 2010
Available online 4 February 2010

Keywords:
Free riding
Incentive
Peer-to-peer
Pyramidal structure
Security

ABSTRACT

Recently a lot of efforts are focused on the most promising solutions in future communication environments with information and communication security technologies. As a result of anonymity and contribution resources voluntary of nodes in P2P wireless network, the overwhelming nodes lack enthusiasm when they provide service, which is easy to cause free riding phenomenon. Thus, it leads to the emergence of hubs. Due to the existence of hubs in P2P wireless networks, the network becomes much more vulnerable because of great reducing in defending against coordinated attacks.

Therefore, in this paper we provide a secure model for controlling the hubs in P2P network based on trust value. In detail, this paper proposes a model based on trust value of nodes against vulnerability, which not only takes into account a node's connections, but also gives full consideration about a node's trust value. The calculation of trust value is broken down to various types of resources. In accordance with the type of pre-transaction resources, the nodes that have higher trust value and fewer connections are chosen to make transaction. Simulation results demonstrate that this model can encourage nodes to participate in sharing recourses with other nodes in the network actively, and simultaneously it can avoid generating hubs effectively. Our model could improve the ability of defending against coordinated attacks, and also could enhance the network robustness and stability.

© 2010 Elsevier B.V. All rights reserved.

1. Introduction

Recently positive efforts are focused on the most promising solutions in future communication environments with information and communication security technologies. Here we are interested in a secure model for Peer-to-Peer (P2P) network, which breaks the traditional Client/Server (C/S) mode. In this network, each node is equal logically, which is both a provider and recipient of resources [1]. P2P file sharing business has exceeded the World Wide Web (WWW) [2], and becomes one of the most important internet application systems in the world. However, this pattern of work has a number of drawbacks. For example, the design philosophy of P2P wireless network is to improve the network efficiency by using the network bandwidth fully and developing the potential of each node as possible as it can. However, as a result of anonymity and contribution resources voluntary of nodes in P2P wireless network, the overwhelming nodes lack enthusiasm of providing service since a single node is to only attempt to maximize its own network effectiveness. Thus, it is easy to cause free riding phenomenon. In this network, a large number of nodes just use the network resources without contributing anything, and only a small number of nodes in network provide resource, which will lead to the emergence of hubs. That is, a small number of nodes own many connections, while the majority has only few connections. The existence of hubs may cause the entire network's ability of defending against coordinated attacks to decrease greatly, and increase the vulnerability of the network [3]. In addition, the anonymity and openness of P2P wireless network make the issue of network security becoming increasingly prominent [4], which can be seen from the performance of providing reliable services or fraud acts [5], it is necessary to regulate the users' behavior in network through the trust value.

Therefore, in this paper we propose a model against vulnerability based on trust value. Compared with the traditional models, our model has below characteristics:

* Corresponding author. Tel.: +82 2 970 6702.
E-mail addresses: yhliu@mail.ccnu.edu.cn (Y. Liu), nxiong@cs.gsu.edu (N. Xiong), parkjonghyuk1@hotmail.com, hyuks2005@paran.com (J.H. Park), chlin@whu.edu.cn (C. Lin).

0140-3664/$ - see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2010.01.028

(1) The calculation of trust value is broken down to various types of resources. We will take high trust value for type of resources as a factor while selecting service provider, which ensures the success rate of downloading resources.
(2) The accumulation of trust value needs a number of successful transactions, which can prompt nodes providing high quality resources. Thus, it can avoid free riding phenomenon and fraud actions.
(3) We take into account the node's connections, select nodes that have higher trust and fewer connections to make transaction. This can avoid generating hubs effectively, improve the ability to defend against coordinated attacks, and also enhance the network robustness and stability.

The rest of this paper is organized as follows. Section 2 gives the research status. In Section 3, we propose the model based on trust value against vulnerability in P2P wireless network. Section 4 shows the analysis of vulnerability against model. In Section 5, we give the simulation analysis to demonstrate that our model is effective. Finally, Section 6 presents the conclusions and future work.

2. Research statuses

Scientists have found that the distribution of nodes' connection in P2P wireless network follows the "power-law distribution" [6], i.e., for an existing network, new nodes prefer to connect to the nodes that already have more connections. As time goes by, these nodes have more connections than the others, which may lead to the formation of hubs. In addition, the existence of free riding phenomenon, which makes network only have a small number of network nodes to provide resources, is also one of the reasons to lead to generate hubs. Once a hub fails or quits from the network, it will affect the P2P system significantly [7]. Thus the existence of hubs in the network will reduce the performance and quality of service of P2P system, and also make the network more vulnerable.

Literature [8] has reported the results of network traffic measurement in the Gnutella system in 2001. This article points out that nodes maintain an average of 3.4 connections in the Gnutella peer-to-peer network, while the maintain connections of a small number of enthusiasm nodes maybe reach the thousands, or even tens of thousands, and the connections of nodes distribute similarly to power law. However, the actual distributions curve of degrees differs from the power law distribution due to some nodes owning too small connections. The great differences of nodes' maintaining connections with the number of free-riders reported in [9] have the consistency.

At present, the controlling mechanisms on hubs mainly focus on restricting the behavior of the users for the single node, such as incentive mechanisms [10,11], the game theory [12], social networks or economic models and other methods of controlling strategy [13], in which incentive mechanism is one of the most popular means of researching and controlling the hubs. The most common measure of this method is through designing the utility function to calculate the contribution value of nodes, awarding the uploading behavior by increasing its contribution value and punishing the downloading acts by reducing its contribution value, then in accordance with the contribution value to determine the node whether is free rider and decide whether the download request can be met. However, such a strict method may make some of the free-riders lose interests on the system and thus it reduces the number of its users, which acts against the purpose to let the system develop more continually and healthily. The utility function only takes into account the total number of the shared files, the total size of the shared files, the degree of the shared data and other factors, though some of the literature in order to be more equitable, it also considers the node's hardware facilities, such as CPU and network bandwidth. However, many of them ignore the major issues of the quality of the files and regard all trading activities as a successful transaction.

In addition, another noteworthy research perspective in P2P wireless network is to control the network's logical topology structure to avoid generating the hubs. Literature [14] has proposed a hierarchical strategy to deal with the hubs in P2P wireless network, that is, when catching out a node v_i going to become a hub in the network, it should find out the resources that have the most request connections from all the resources that v_i is sharing and search out other nodes that are sharing this resources in the network by starting from the node v_i. From these nodes, then the most two excellent nodes are selected to support more remainder connections as the left child and right child (standby nodes) of the node v_i, form a multilayer binary tree in logic structure to control the hubs. But when choosing standby nodes, it just considers the remainder connections of a node and the distance between nodes, without concerning the node's trust value, which may result in nodes to have low trust value and no resources or unreliable resources are offered as standby nodes, thereby it reduces the efficiency of the network.

3. The model against vulnerability in P2P wireless network

3.1. The ideology of against vulnerability model

P2P wireless network is a collaborative system, the nodes can choose their own interactive objects, and can exchange services or resource. The choice of interactive objects to some extent determines the quality of interaction, as well as reliability. Trust value can be calculated in P2P wireless network, which enable node gains trust value of candidates before making transaction, then the node that have higher value and fewer connections is chosen as a across-node object. Thus, using trust value can improve the quality of services and could inhibit the activities of malicious nodes, as well as the spread of malicious content.

Definition 1. P2P wireless network will be expressed as $G(V,E)$, *where G is a network graph which is composed by a set of nodes* in which V is the nodes set and *a set of edges E* is the edges set, $v_i, v_j \in V$ $(i,j = 1,2,\ldots,n)$, n is the number of the nodes in G, and the number of the nodes connected to a node is called the node's connections. A node v_i sends the transaction request to a node v_j, then v_i will select the node who has higher trust value and fewer connections to inhibit the free riding phenomenon, to distribute network traffic, and to avoid the formation of the hubs. At the same time, it can increase the success rate of downloading, can use network resources fully, can improve network performance efficiently, and can enhance the network robustness and stability.

3.2. Node's trust value for type of resources

In 1994, Marsh described the formal problem of trust firstly, and then he divided content and level from the concept of trust, and posed a mathematical model of the trust metric from subjectivity of trust [15]. In 1996, Blaze et al. first put forward the "trust management" concept [16] in order to address the internet security issues. After that, different scholars from different angles, different applications of the trust model and trust management techniques carried out deep research [17,18]. The definition of trust is given in the X.509 specification of ITU-T Recommendation standards (x.509, section 3.3.23): Entity "A" trusts entity "B" when "A" assumes that "B" will behave exactly as what "A" expects [19].

Download English Version:

https://daneshyari.com/en/article/446725

Download Persian Version:

https://daneshyari.com/article/446725

Daneshyari.com