The Research on Lurks Attack Behavior of Trust Model in Peer-to-Peer Networks

1 Introduction

Peer-to-peer (P2P) networks are networks in which all peers cooperate with each other to perform a critical function in a decentralized manner [5]. -P2P network technology has become one of the hottest topics in the Internet and computer field and has made a preliminary attempt in various fields. P2P network technology is widely used in file sharing, collaborative computing, instant messaging, streaming media and other fields. In the application process of P2P network technology, there are some security problems caused by its own characteristics, such as tapping, forgery, tampering and so on. Therefore, the introduction of effective trust model is a common method to solve security problems in P2P networks.

The existing trust model is divided into two categories, one is the global trust model and the other is the local trust model. The classical representatives of these two types of trust models are the EigenTrust trust model and the PeerTtust trust model. Most of the current trust model is based on the original classic model. These models introduce additional factors as weights to adjust the accuracy of the trust value. In terms of trust value acquisition, they are also based on direct and indirect two parts. But in the resistance to attack a lot of models are flawed. The existing trust model focuses only on the node's one-time attack. These trust models can only deal with some obvious malicious defamation and conspiracy attacks of the special circumstances. They ignored a number of intermittent attacks. This means of attack is the potential attack.

For some obscure latent attacks, many models can not handle well. This paper mainly analyzes the potential attack and finds its characteristics. Then based on these characteristics, this paper designs an improved trust model. This paper introduces the concept of historical volatility to locate latent attack nodes. Historical volatility refers to the degree of fluctuation of a node's time and the corresponding trust value. This paper defines the value of historical volatility and the map of historical volatility to embody the concept of historical volatility. The trust model proposed in this paper can effectively locate the nodes in the network that may have latent attacks, and then punish the nodes. The model is extensible and can be introduced into other models to make the network more secure.

The paper is organized as follows. Section 2 discusses the related research. Section 3 introduces the proposed trust model. Section 4 presents the simulation environment and gives the experimental results. Section 5 summarizes the conclusion.

5. Milojicic D. S., Kalogeraki V. and Lukose R. “Peer-to-Peer Computing”, Tech Report: HPL- 2002-57, http://www.hpl.hp.com/techreports/2002/HPL-2002-57.pdf