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.

2. Related work

3. Trust Model Against Potential Attack

3.1 Analysis of Latent Attack

Latent attack is an attacking behavior in P2P networks. The malicious node first goes to the normal transaction after entering the network, providing good service and resources. Malicious nodes publish malicious resources or provide malicious comments after accumulating high trust values. So that the trust value of malicious nodes will be reduced. But after falling to close the malicious value, they began to provide good services and resources. Malicious nodes re-accumulate evaluation values, so repeated.

Such malicious nodes have a certain latency during the attack, intermittently provide malicious resources and services. This attack is more subtle than the simple attack. This kind of aggressive behavior may obscure the fraudulent behavior of the malicious node by the positive feedback obtained from the normal service, thus maintaining a high degree of trust.

Latent attack has the following characteristics:

1. Intermittent

Intermittently including behavioral intermittent and time intermittent. Behavioral intermittent is reflected in the alternating process of receiving the positive feedback and negative feedback. In order to prevent the trust value is quickly reduced, malicious node will silence for some time and then attack. This is time intermittent. This intermittent attack may be considered to be wrongly handled, so it is difficult to be concerned.

1. Hidden

Behavioral intermittent reflect the hidden of latent attacks. Lurking attacks can make the network inadvertently appear malicious resources and malicious evaluation. It is difficult for a network to target publishers of malicious behavior. The network can not quickly locate the publisher of malicious behavior and immediately reduce the trust value of malicious nodes ,will bring a lot of security threats.

3.2Program Imagine

In view of the characteristics of the latent attack described above, the following points are put forward：

1. The purpose of this program is to reduce the impact of latent attacks on the network.
2. We are only positioning nodes that may have malicious attacks based on some specific characteristics, and we can not be sure that the node is a malicious node. So we do not use extreme means to remove the node.
3. It is possible that only nodes with latent attacks have high quality resources. This attack behavior compared to other attacks is only relatively large hidden, as the means of attack are the same. Therefore, after finding the attack node, the network needs to use the incentive mechanism to make it become a good node.

The specific idea of the program

Some of the undefined concepts mentioned in the scenario will be specified in the next section.

First, the network needs to collect all the information that each node interacts with other nodes, and record the trust values that have been obtained. The network then observes the volatility of historical evaluation values based on time and trust values. The network locates nodes that may have latent attacks based on the degree of volatility and penalizes the node nodes appropriately. If the appropriate punishment can not make the node tend to normal, but the attack more frequently, the network will quickly reduce the node's trust value and remove. As the network needs to collect historical information, the model can not be introduced immediately, need to run for some time. Lurking attacks also take some time to hide, so this does not conflict with the introduction time of the model. The way to deal with latent attacks is relatively independent. The network needs to find the trust value of the node first and then feedback. So the model has a very good portability. It can be applied to other existing models, inherit the advantages of existing models to extend the lack of the model.

3.3 Definition of related concepts in the model

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