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

Abstract

There are many security issues exist in the P2P network operation process. The existing trust model suffers from various attacks. Latent attacks are often ignored by the trust model. Latent attack has a good hidden, P2P network is a major security risk. But the latent attack has certain characteristics and laws. In this paper, we will introduce a model to against latent attacks. This model has good scalability, can be introduced into other trust model. This model can effectively avoid the latent attack on the basis of guaranteeing the inherent function and efficiency of the model.

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 introduces the proposed trust model. Section 3 presents the simulation environment and gives the experimental results. Section 4 summarizes the conclusion.

2. Trust Model Against Potential Attack

2.1 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.

2.2Program 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.

2.3 Definition of related concepts in the model

2.3.1 Resource importance

Each node in a P2P network has a lot of resources, and the importance of each resource is different. A malicious node may provide ordinary resources multiple times to defraud a high degree of trust and then provide false information on important resources. In order to minimize this behavior, the concept of resource importance is introduced in the model. Each node divides their resource according to the importance. Some resources are important, so the proportion is large, which is the evaluation value of the resources affect the node's trust value accounted for a large proportion. This will reduce the power of latent attacks.

The resource importance in the model is represented by IQ. IQ (i) represents the importance of resource i in the node. The larger the value is, the importance of the resource is greater. The smaller the value is, the importance of the resource is smaller. ，the size of the value is determined by the node itself.

2.3.2 historical volatility

Historical volatility refers to the degree of fluctuation of a node's time and the corresponding trust value. For example, A is the requesting node and B is the node that provides the resource. Now A wants to know the historical volatility of B, first A need to query B's trust value information at local, and then send a broadcast request to query B's historical information from the recommended node, and in accordance with the time and the corresponding trust value to sort. Historical volatility is reflected by two parts: the fluctuation frequency and fluctuation strength. The model needs to calculate the basic fluctuant value of the global trust value that has been ordered, and then calculate the fluctuation frequency and t fluctuation strength. In order to describe the concept of historical volatility more clearly, we can draw the global trust value and time constitute the image. The historical volatility chart introduced in the model actually reflects the concept of historical volatility.

2.3.3 Basic values of fluctuation

In order to reflect the historical volatility better, the model defines a basic value for the historical fluctuation image, called the basic value of the fluctuation, and uses to describe the basic fluctuation value of the j-node.

The calculation formula of the basic fluctuation value:



 represents the trust value obtained from the i-th evaluation of j-node, and m represents the total number of the trust values, which is the total number of times of the trust value for j-node.

The base value is the average value of all trust values. As the time and number of transactions increase, the model needs to update the base value at any time. So the basic value of the fluctuation is dynamically changing.

The base value is used as a reference for the trust value, the fluctuation period and the fluctuation strength are based on the fluctuation base value.

2.3.4 fluctuation frequency

The model defines the number of cycles that fluctuate per unit time as the fluctuation frequency.

The calculation formula of fluctuation frequency:



 Indicates the number of cycles for the node's trust value, Indicates the total time, Indicates the fluctuation frequency of the node.

The fluctuation frequency is used to calculate the trust value of the node as the weight. Since the range of the trust value is between 0 and 1, and the value of the fluctuation frequency obtained by the above formula is not in the range of 0 and 1.In order to introduce the formula into the model, the formula is normalized to obtain the following formula:

 （4.3）

 represents the proportion of the fluctuation frequency for node j in m times transactions to the fluctuation frequency for all transactions. This result is between 0 and 1. The larger the value is , the greater the frequency of the fluctuation is, the more likely the node is the latent attack.

2.3.5 fluctuation strength

The degree of trust value for the node deviates from the basic value is called the fluctuation intensity. The model can identify nodes that may have latent attacks by fluctuation strength.

The model uses the method of calculating the standard deviation to find the fluctuation strength, the formula is as follows:



 represents the fluctuation value of the j node, represents the trust value obtained by the i-th transaction of j node, represents the basic value of the j point, m represents total number of reviews, which is the total number of nodes in the image. Because the value of the trust is between 0 and 1, the value of is between 0 and 0.5. The larger the value is, the farther the image deviates from the base value.

2.4 the establishment of the model

The satisfaction value, recommended trust value and direct trust value involved in the model are calculated using the existing calculation formula.

In the calculation of the global trust value, the model introduces the fluctuation frequency and the fluctuation intensity as the weight to influence the final global trust value.

The model defines the average value of the fluctuation strength and the average of the fluctuation frequency.

 （4.10）

is the average value of fluctuation strength from all nodes that can provide service k.

 （4.11）

is the average value of fluctuation frequency from all nodes that can provide service k.

The model awards or punishes the global trust values of the nodes based on these two values.

Global trust value calculation formula:

 （4.12）

represents the global trust value obtained by node i to node j， are the weight factor, which is the proportion of direct trust value and trust value in the total trust value, +=1，users can set 、 according to their own preferences. When the interaction between nodes is not very frequent, you can focus on direct trust values, which is >；当When the interaction between nodes is very frequent, you can focus on recommended trust values, which is <。When,  is a decreasing function, which is negative feedback. When ,  is a increment function, which is positive feedback；When, is a decreasing function, which is negative feedback. When ,  is a increment function, which is positive feedback.

The model ultimately influences calculating the global trust value by the historical volatility (fluctuation strength and fluctuation frequency) to affects the latent attack.

3 Simulation of the experiment

This chapter will simulate the operating environment of the network node through the Peersim simulation platform. In this experiment, two classic trust models, EigenTrust and PeerTrust, are applied to the Peersim simulation platform, and the model is introduced on the basis of these two classical models. The experiment is carried out in the case of different malicious node rate. We statistics and analyze the change of transaction success rate, the change of Missing alarm rate and false alarm rate, and the change of latent nodes’ global trust value with the period, ultimate draw the conclusion of this paper.

3.1 Setting of simulation parameters

This model is mainly to resist latent attacks, so this experiment will simulate the latent attack environment. The experiment defines an unstructured network and sets up 10,000 nodes. The nodes are divided into normal nodes and malicious nodes (latent attack nodes). The range of the latent nodes is defined between 0 and 0.5. We will adjust the proportion of malicious nodes during the experiment. The number of cycles for the experiment is set to 1000. This setting is conducive to collect a large number of historical information, more likely to reflect the characteristics of latent attacks. To prevent complex iterations during the calculation, we set ttl to 4. We allocate 10 resources for each node, and the proportion of resources is at the range from 0.5 to 0.9 randomly assigned. This setting is to reflect the effect of resource importance in resisting latent attacks.

The specific simulation parameters are set as follows:

|  |  |
| --- | --- |
| Environmental parameters | value |
| Network structure | Unstructured network |
| Total number of nodes | 10000 |
| Node depth | 6 |
| Normal node rate | [0,0.5] |
| Malicious nodes rate | [0,0.5] |
| cycle | 1000 |
| TTL | 4 |
| The number of resources per node | 10 |
| The proportion of resource importance | [0.5,0.9] |

In the simulation also need to set some specific parameters, as shown in the following table:

|  |  |  |
| --- | --- | --- |
| parameter | description | value |
| H | The threshold number of interactions | 100 |
| t | Initial trust value | 0.5 |
| α | Direct trust weight | 0.7 |
| β | Recommended trust weight | 0.3 |
| Ρ | Similarity threshold | 0.3 |

3.2 Simulation results and analysis

3.2.1 Test the accuracy of the model

In order to reflect the accuracy of the model to identify the latent attack, the experiment has tested the false alarm rate and Missing alarm rate.

For the latent attack node we determine by malicious fluctuations. This malicious volatility is dynamic. If the node's fluctuation value is greater than the average fluctuation value, the node is defined as a latent node. If the node's fluctuation value is less than the average fluctuation value, the node is defined as a normal node.

In the experiment with the number of cycles continues to increase, the node's trust value will fluctuate. So the identity of the node will continue to change. We make a collection of normal nodes which are mistaken for malicious nodes. This collection is called false alarm collection. The proportion of false alarm collection in the normal node is false alarm rate. We make a collection of malicious nodes which are mistaken for normal nodes. This collection is called missing alarm collection. The proportion of missing alarm collection in the malicious node is missing alarm rate. The combination of these two indicators can well reflect the accuracy of the model's latent judgment.

Figure 1

The blue line in Figure 1 represents the change of the false alarm rate in EigenTrust model with the different proportions of the latent nodes. The orange line in Figure 1 represents the change of the false alarm rate after introducing this model.

It can be seen from the figure, when the proportion of latent nodes is relatively small, EigenTrust model is more accurate. This is due to that it need to calculate the historical fluctuations after introducing this model. Any node will have fluctuations, there will be fluctuations in the node is greater than the average. So the smaller the proportion of malicious nodes are , the greater the false alarm rate are. And when the proportion of latent nodes becomes larger, the role of this model can be reflected. While in EigenTrust model because there is no latent recognition ability,the false alarm rate will gradually increase with the increase of the proportion of latent nodes.

Figure 2

The blue line in Figure 2 represents the change of the missing alarm rate in EigenTrust model with the different proportions of the latent nodes. The orange line in Figure 2 represents the change of the missing alarm rate after introducing this model.

It can also be seen from the figure that the traditional model does not have the ability to discover the latent nodes. When the node attacks, EigenTrust model is only to punish the node, but can not find the law of its attack. EigenTrust is also very accurate when there are fewer malicious nodes. However, when the proportion of malicious nodes gradually become larger, this model shows a good advantage.

3.2.2 Test the success rate of model transactions

Figure 3

Figure 3 shows the change of the transaction success rate in EigenTrust model and this model with the different proportions of the latent nodes. It can be seen from the image that the transaction success rate in EigenTrust model decreases with the increasing proportion of latent nodes. But this model can find latent nodes, and effectively avoid latent attacks. So that the transaction success rate can maintain a higher level.

Figure 4

Figure 4 shows the change of the transaction success rate in PeerTrust model and this model with the different proportions of the latent nodes. Although the PeerTrust model declines less than the EigenTrust model, the result is still unsatisfactory. The transaction success rate also can maintain a higher level after introducing this model.

As the settings on the latent attack node is theoretically, the lurking attack behavior of latent nodes is obvious. So the transaction success rate of the model is relatively high. But the two classic models are also experimental in the same environment,it is still able to explain the model can be more effective resistance to latent attacks.

3.2.3 Testing of global trust values for latent nodes

Figure 5

Figure 5 shows the change of the global trust value in EigenTrust model and this model with the different proportions of the latent nodes. Initially let the model converge and introduce the parameters of the model after 100 cycles. Select some typical nodes as a reference.

It can be seen from the image, malicious node in EigenTrust model reflects the characteristics of latent attacks. It has great volatility.After the introduction of this model, the volatility is significantly reduced, so the node has become a normal node.

4 Conclusions

In this paper, we analyzed the characteristics of latent attacks and established the corresponding models based on these characteristics. This model introduces the concept of volatility for the calculation of global trust values. Through the adjustment of the global trust value to resist latent attacks. This model is based on the existing classical trust model. So this model has good scalability, can be introduced into other trust model. This model can effectively avoid the latent attack on the basis of guaranteeing the inherent function and efficiency of 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