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.

P2P network can make people communicate easier, more direct, more sharing and interaction, really eliminate the middlemen, which is decentralized, high efficiency, easy extensibility and robustness, etc. Social people from all walks of life view of peer-to-peer (P2P) were mixed, however, each node in the decentralized network need to be protected, if a node is attack is likely to spread to the entire network, so the security hidden danger is worthy of concern.

P2P network still exist many traditional network attacks in the process of application, attacks against network layer such as routing attack, ARP attack, the rogue client, rogue server, etc. In addition, there are hacking, tampering and forgery to the data, impersonation, forged false identities, and many other attacks, which are require the introduction of a firewall, proxy servers, intrusion detection, and a variety of technologies such as identity authentication, ciphertext transmission protection; The decentralized characteristics of P2P ,which make each node is equal. The attacker can invade of a node and spread to the whole network, which leads to its availability and safety hidden trouble in many aspects;  The nodes in P2P networks lack of proper trust mechanism and incentive mechanism, lead to can't make a better selection and punish failure node; Nodes in P2P network join and exit frequently can lead to jitter of local network and inconsistent of resources; There are serious copyright problems in P2P network. Usually we use the trust model mechanism to strengthen the security of P2P network, there are many attacks in the P2P trust model means:

Denigrate: Denigrate behavior in malicious nodes provide a very low value for the nodes provided resources after got good resource, to reduce the trust value of nodes, or give a low value at the time of recommendation, to reduce the recommendation trust values of evaluation node.

Cheating: In general trade process, malicious nodes respond to the request of, using the way of deception to provide request service node with a virus or waste resources, make the request service node result in transaction failure.

Conspiracy: Multiple malicious nodes proceed malicious activities together in network, for giving malicious value to reduce good nodes’ trust value rapidly, for giving good value to raise malicious nodes’ trust value rapidly, then providing false information in the transaction to destroy network.

Reentrant: After malicious nodes providing false information many times, their  trust value lower than trading threshold and there will be no node deal with them, then malicious nodes will exit and use new identity rejoined the network to become a new node, by getting the initial trust value malicious nodes can participate in calculation. We can through the record of node information to let malicious nodes join in the blacklist, resetting initial value to resist malicious nodes.

Latent type attack: Latent type network attack [41-42] is a confrontational network attack, by means of concealment, disguise or conceal in the legal normal network data, by this way to avoid the safety inspection from the host and network, to long-term stay in network and monitor the victim host, achieve the goal of continued to steal information or long-term control using. Latent type of cyber attacks emphasis has the following several aspects:

Network correlation: Latent type attack activities should be carried out in a network with activities, need to active in a large network stored a lot of important information or a wide range of node for important information on trading behavior. Only cheating activity nodes, attack would have the effect of damage, so malware on a single host does not belong to the category of this concept.

Concealment：The latent concept is just the embodiment of concealment, concealment type network attack features embodied in disguise or hidden in the invasion of the way and communication behavior. Malicious nodes parasitize in hosts of the network using a hidden way in the process of invasion, most of the time to hide their own behavior, when there is a special important trade information, monitor or attack, and cause the attacker could not detect. So the denial of service attack, attack through scanning the unconventional port and attacks which victims can detect, does not belong to this category.

Controllability: The attacker remote control the host  through the network to operation, record, upload the specified information, a general sense of worms and viruses will expose their own behavior at the time of the attack, the host will immediately perceive virus, so there is no controllability, does not belong to this category.

Purpose: Lurks attack in order to continue to steal confidential information or control and using the victim for a long time, forming numerous zombies node. So the backdoor of ordinary procedure, Trojan to steal personal information and malicious blackmail software does not belong to the category.

Latent attack is a kind of attack means which is the most secretive and most difficult to find, it performance for attacker first provide good resources to raise their trust value then provide malicious information. At the time of their trust value close to the threshold value, malicious node began to provide good information push up trust value, and repeat intermittent behavior. This attack with confidentiality, can't locate nodes, there will be the spread of malicious resources, so great harm to the network. The paper made improvements on the basis of the EigenTrust and PeerTrust, make model can resist latent attacks, improve the success rate of transactions between network nodes.

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