The research of P2P trust model about the lurks attack behavior

1 Introduction

P2P network technology has become one of the hottest topics in Internet and computer field, and has carried on the preliminary attempt in various fields. 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.

After the analysis of the problems existing in the P2P network, we found some secure problems  can easily be detected and be contain by some means . There are some problems are difficult to be detected and solved in P2P network ,these attacks tend to have latent and hard to find, so this kind of attack is the way which is more common and more aggressive. 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.