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 .