Abstract

In this implemented project, using open nature of Peer to Peer systems that helps to expose the malicious activity. Building trust relationships among peers can reduce attacks of malicious peers. Peers create its own trust network in their proximity by using local information available and do not try to learn global trust information. Based on trust information it classifies the peers whether peer is trustworthy or not. In this paper used the technique called Self Organizing Trust Model (SORT) that aims to reduce malicious activity in Peer to Peer system by establishing trust relations among peers in their proximity. Trust information is evaluated based on service, trust values of each peers and it is based on past interactions. Which one peer having highest trust ratio that is computed using service and trust values of earlier interaction that peer to be selected for next interaction. This trust information helps to build a secure environment to transmit a packet. Simulation experiments on a file sharing application show that the proposed model can mitigate attacks on different malicious behavior models. In the experiments, good peers were able to form trust relationships in their proximity and isolate malicious peers.
References


Index Terms

Computer Science  Networks

Keywords
Peer to Peer system, Trust Management, Security, Establishing Trust Information, Past Interaction