The architecture of certain class of services, such as distributed computing, distributed storages or content delivering networks shifts from the traditional client-server model to more scalable and robust peer to peer networks. Providing proper protection to such complex, open and anonymous systems is very complicated. Malicious peers can cooperate and develop sophisticated strategies to bypass existing security mechanisms. Recently, many trust management systems for P2P networks have been proposed. However, their effectiveness is usually tested only against simple malicious strategies. Moreover, a complex comparison of resistance of a particular method is missing.

In this thesis, we (1) propose a new trust management system called BubbleTrust and (2) develop a simulation framework for testing trust management systems against various malicious strategies. Our simulation framework defines several criteria which determine the success of each malicious strategy in the network with a given system. We present results of four trust management systems that represent main contemporary approaches and BubbleTrust.