Abstract

One of the dominant properties of a global computing network is the incomplete information available to principals about each other. In such an environment hard security measures such as cryptography and certification fail to address the possibility of one or more interaction partners becoming malicious and causing undesirable effects. Soft security measure such as trust, reputations and other social controls are used for the detection of such partners and avoiding interaction with them. Many computational trust and reputation models have been developed. From the perspective of design methodologies of these models, they may have a policy based trust, credential based trust or probabilistic trust models. In the probabilistic models, a principal A evaluates a quantitative measure for trust in other principal B using the history of B's behavior. Among these models, beta model and HMM based models are common. The current beta based systems are limited by the fact that they assume a fixed probabilistic behavior for each principal. Hidden Markov Models can be used to model dynamic behavior. An HMM can be either discrete or continuous. Continuous HMM can be again with single continuous Gaussian distribution or with mixture of Gaussians. In both the cases, knowing the number of system states beforehand is an important requirement. In most of the HMM models for dynamic system, number of states is arbitrarily given a value, if no information is available in advance. Another problem with the Gaussian mixture model is deciding the parameters of the mixing distributions. We have explored clustering as a solution to these problems. The efficiency of the two models are analyzed and compared on a test dataset. The accuracy of the single Gaussian density distribution is found to be more than the model based on the mixture of Gaussian distributions.