Abstract

Intrusion detection is a process of identifying the Attacks in the networks. The main aim of IDS is to identify the Normal and Intrusive activities. In recent years, many researchers are using data mining techniques for building IDS. Due to the non-linearity and quantitative or qualitative network data traffic IDS is complicated. For making the IDS efficient we have to choose the key features. Support Vector Machine (SVM) gives the potential solution for IDS problem. SVM suffers by selecting the suitable SVM parameters. Here we propose a new approach using data mining technique such as SVM and Particle swarm optimization for attaining higher detection rate. PSO is an Optimization method and has a strong global search capability. The SVM-PSO Method is applied to KDD Cup 99 dataset. Free parameters are obtained by standard PSO for support vector machine and the binary PSO is used to obtain the best possible feature subset at building intrusion detection system. The propose technique has major steps: Preprocessing, Feature Reduction using Information Gain, Training using SVM-PSO. Then based on the subsequent training subsets a vector for SVM classification is formed and in the end, classification using PSO is performed to detect Intrusion has happened or not. The experimental result shows that SVM-PSO acquire high detection rate than regular SVM Method algorithm.
References

- Matthew Settles, "An Introduction to Particles Swarm Optimization"; department of Computer Science, Idaho University.
- Jun Wang, XuHong, Rong-rong, Tai-hang Li, "A Real time Intrusion detection system based on PSO-SVM", proceedings in IWISA Qingdao, China, November 21-22, 2009.

**Index Terms**

Computer Science

Security

**Keywords**

Intrusion detection system; Information Gain; Support Vector Machine (SVM); Particle Swarm Optimization (PSO)