Abstract

Information systems need to be constantly monitored and audited; analysis of security event logs in heavy traffic networks is a challenging task. In this paper we considered Differential
Intrusion Detection Model based on Differential Evolution

Evolution for the intrusion detection problem. We used NSL_KDD dataset for our experiments which is derived from the standard KDD CUP 99 Intrusion Dataset. We also provided the comparative results of the differential evolution with the state of the art classification algorithm like SVM. We reduced the dimension/features of the NSK_KDD datasets using rough set algorithm and ran DE and SVM this increased the speed of the evolutionary algorithm without compromising the detection rate.

References


Index Terms

Computer Science Security

Keywords

Common Intrusion Detection Framework (CIDF)
Differential Evolution (DE)
Support Vector Machines (SVM)