Abstract

With the wide adoption of internet, there lies threat to sensitive information being shared on the network. An intrusion can be defined as an act or a number of acts in a sequence that either cause a compromise or intend to compromise the information. These intrusions need somehow to be detected so that the harm caused by them may be prevented. A system that keeps looking for activities in a computer or a network to detect intrusions is called an Intrusion Detection System (IDS).

Many novel methods of intrusion detection involve the use of Soft Computing tools. Soft Computing (SC) is a collection of methods used for developing intelligent systems for the problems for which conventional techniques have not given low cost or complete solutions. Artificial Neural Networks (ANN), Fuzzy Logic theory (FL) and Genetic Algorithm (GA) represent the most common tools of soft computing. The capability of soft computing tools to tolerate imprecision, partial truth, uncertainty and ability to provide low solution costs to real world
problems and computationally intelligent problems are the obvious reasons which has made this approach widely accepted in field of Intrusion Detection.

In this research work, we have collected about thirty papers to study how different soft computing tools and techniques can be utilized to develop efficient and robust Intrusion detection Systems.

References


Index Terms

Computer Science          Networks

Keywords

Soft Computing, Fuzzy Logic, Genetic Algorithm, Intrusion Detection System (IDS)