**Improving intrusion detection using genetic algorithm**

ABSTRACT

Intrusion Detection System (IDS) is one of the key security components in today's networking environment. A great deal of attention has been recently paid to anomaly detection to accomplish intrusion detection. However, a major problem with this approach is maximizing detection rate and accuracy, as well as minimizing false alarm i.e., inability to correctly discover particular types of attacks. To overcome this problem, a genetic algorithm approach is proposed. Genetic Algorithm (GA) is most frequently employed as a robust technology based on machine learning for designing IDS. GAs are search algorithms which are based on the principles of natural selection and genetics. GA functions on a number of possible solutions using the principle of survival of the fittest with the aim to generate better approximations to solve a particular problem GA is facing. The validity of this approach is verified using Knowledge Discovery and Data Mining Cup 1999 (KDD Cup '99) dataset. The experimental results demonstrate that the proposed approach outperforms the existing techniques, with the detection rate of attack and false alarm rates of 95.7265 and 4.2735, respectively.

**Keyword:** Genetic algorithm; Intrusion detection system; False positive; False negative; Detection rate; Rule set