Abstract

Computer networks have experienced an explosive growth over the past few years and they become the targets of the hackers and intruders. Within network security, there is a task of intrusion detection. An intrusion detection system's main goal is to classify activities of a system into two major categories: normal and suspicious (intrusive) activities. Intrusion detection systems usually specify the type of attack or classify activities in some specific groups. The objective of this work is to incorporate several soft computing techniques into the classifying system to detect and classify intrusions from normal behaviors based on the attack type in a computer network. Among the several soft computing paradigms, neuro-fuzzy networks, fuzzy inference approach and genetic algorithms are investigated in this work. A set of parallel neuro-fuzzy classifiers are used to do an initial classification. The fuzzy inference system would then be based on the outputs of neuro fuzzy classifiers, making final decision of whether the current activity is normal or intrusive. Finally, in order to attain the best result, genetic algorithm optimizes the structure of our fuzzy decision engine. The experiments and evaluations of the proposed method were performed with the KDD Cup 99 intrusion detection dataset. This work shows that our proposed method can be effective in intrusion detection compared with similar models and increases detection rate with respect to false alarm rate. Main ability of the proposed system is that the current system is configurable in a specific situation. Also the proposed system can be effective in environments in which sample distributions in different categories of attacks in training data significantly differ from each other.