AN EFFICIENT INTRUSION DETECTION SYSTEM USING GREY WOLF ALGORITHM AND KERNEL EXTREME LEARNING MACHINE CLASSIFIER

P. Nirmaladevi

Assistant Professor, Department of Computer Applications, Nandha Arts and Science College, Erode, Tamil Nadu, India

ABSTRACT

Protecting Data from attackers in a network is an arduous task because of the size and structure of the network. Various Intrusion algorithms have been evolved but fall back in the performance of intrusion detection. A Network Intrusion Detection should be designed in such a way that the proposed algorithm should maximize the detection rate and at the same time, it should minimize false detection. To do this effective manner a machine learning classifier should be used for classification of the features and predicting the presence of intruders in the network. Usually, in a network dataset there will be a huge number of features will be available which will affect the classifier accuracy. Selecting the optimum features and identifying and avoiding the irrelevant and redundant features is a strenuous task. For selecting the optimum features Grey Wolf Algorithm is used. From this algorithm, the leadership quality of grey wolves in selecting and hunting the prey is applied for selecting the features. Network Security can be preserved by using Kernel Extreme Learning Machine (KELM) algorithm in the classifier stage that maximizes the easy detection of malicious attacks and minimizes the false alarm. The proposed GWO-KELM (Grey Wolf Optimization - Kernel Extreme Learning Machine) algorithm is tested for the performance and compared with other algorithms that are used in the Intrusion Detection Systems (IDS). The evaluation results explain that the proposed GWO- KELM based intrusion detection system performs better than the existing techniques.

KEYWORDS: *Network Intrusion Detection, Intelligent Algorithms, Grey Wolf Optimization, Principal Component Analysis, Kernel Extreme Learning Machine*