

An efficient anomaly intrusion detection method with feature selection and evolutionary neural network

ABSTRACT

Recently, with the technological and digital revolution, the security of data is very crucial as a massive amount of data is generated from various networks. Intrusion Detection System (IDS) has been observed to be perhaps the best solution because of its capability to distinguish between attacks that originate within or outside a corporate network. In this study, the most significant features for enhancing the IDS efficiency and creating a smaller dataset in order to reduce the execution time for detecting attacks are selected from the sizeable network dataset. This research designed an anomaly-based detection, by adopting the modified Cuckoo Search Algorithm (CSA), called Mutation Cuckoo Fuzzy (MCF) for feature selection and Evolutionary Neural Network (ENN) for classification. The proposed search algorithm uses mutation to more accurately examine the search space, to allow candidates to escape local minima. Moreover, the value of the solution is evaluated based on the objective function and the Fuzzy C Means (FCM) clustering method used to provide the best results for the overlapping dataset and create the fuzzy membership search domain which includes all possible compromise solutions. A proposed model has been practically used to the problem of intrusion detection as well as been validated using the NSL-KDD dataset. The experimental results reveal that reducing features by selecting and utilizing the most relevant features can improve execution time and at the same time enhance the efficiency and performance of IDS.

Keyword: Intrusion detection systems (IDSs); Multilayer perceptron (MLP); Multiverse optimization (MVO); Cuckoo search algorithm (CSA); Feature selection (FS); NSL-KDD dataset