ABSTRACT

With the increased amount of network threats and intrusions, finding an efficient and reliable defense measure has a great focus as a research field. Intrusion detection systems (IDSs) have been widely deployed as effective defense measure for existing networks. Detecting malicious activities and unauthorized use of such systems is the main function of IDSs. IDSs detect anomalies based on features that can be extracted from network traffic. There are many features that can be measured from network traffic. However, with high traffic volume and large scale networks; there is a large amount of features to be observed for detection. The problem is that with the huge amount of network traffic many irrelevant features can be measured. These irrelevant features usually affect the performance of detection rate and consume the IDSs resources. Hence, IDS has to meet the challenges of low detection rate, large computation time and complexity. To optimize detection accuracy and to improve the computational time only relevant features that best distinguish between normal and attack traffic should be selected. Therefore, designing a new model for relevant feature selection is one of the important research challenges nowadays. Finding such a model will play a key role in designing and building robust and lightweight IDSs that achieve a fast and reliable training and testing process while preserving high accuracy rates.

This research aims to propose a new model that could efficiently select the set of most relevant features for IDSs. Effectiveness and the feasibility of the proposed model have been verified using KDD'99 intrusion detection benchmark dataset. Results showed that, the set of most relevant features selected using our proposed model achieves high detection rate, high performance rate, low false alarm rate, and fast and reliable detection process.