A NOVEL INTRUSION DETECTION SYSTEM USING DATA MINING APPROACHES

Intrusion Detection is the problem of identifying unauthorized use, misuse and abuse of computer systems. Outside attacks are not the only problem, the threat of authorized users misusing and abusing their privileges is an equally pressing concern. Many intrusion detection systems (IDS) utilize a individual classifier algorithm for classifying network traffic as normal or abnormal. Due to the large amount of data, these sole classifier models fail to achieve a high attack detection rate with reduced false alarm rate. In this proposal one of the efficient classifier naive bayes on reduced datasets for Intrusion detection is going to be implemented. The main idea behind this model is to construct a multi class SVM which has not been adopted for IDS so far to decrease the training and testing time and increase the individual classification accuracy of the network attacks. Experimental results show that selected reduced attributes give better performance to design IDS that is efficient and effective for network intrusion detection.