A Novel Combined Method for Network Intrusion Detection Systems Aimed at Detecting Novel Attacks

Intrusion Detection Systems are important tools in computer networks security. To date, many practical methods have been proposed using data mining techniques, however, presence of novel is not considered in most of the proposed method. As the presence of novel attacks in the real world is unavoidable, proposing methods that consider novel attacks is crucial in this area of research. In this paper, a combined method has been presented for Network Intrusion Detection Systems using K-NN and K-Means clustering algorithm. A threshold has been used for detection of novel attacks. The proposed method is superior to a hybrid method in the literature that does not consider novel attacks, in which K-means clustering algorithm and K-Nearest Neighbor(K-NN) algorithm have been combined, in terms of accuracy, detection rate, and false alarm rate.


Index Terms

Computer Science

Networks

Keywords

Network Intrusion Detection, Hybrid Learning, Network Security, Data Mining