Adaptive feature selection for denial of services (DoS) attack

ABSTRACT

Adaptive detection is the learning ability to detect any changes in patterns in intrusion detection systems. In this paper, we propose combining two techniques in feature selection algorithm, namely consistency subset evaluation (CSE) and DDoS characteristic features (DCF) to identify and select the most important and relevant features related DDoS attacks. The proposed technique is trained and tested using the NSL-KDD 2009 dataset and compared with the traditional features selection method such as Information Gain, Gain Ratio, Chi-squared and Correlated features selection (CFS). The result shows that the combined CSE with DCF model overcomes the drawback of traditional feature selection technique such as avoid over-fitting, long training time and improved efficiency of detections. The adaptive model based on this technique can reduce computational complexity to analyze the data when attack occurs.

Keyword: NSL-KDD; Features selection; Intrusion detection; Machine learning