Abstract

With the rise in storage and manipulation of sensitive data over networks and the colossal growth of network-based-services, security of network systems is being increasingly threatened. The necessity to create an efficient intrusion detection mechanism to detect cutting-edge cyber-attacks has become a daunting task for both the research community and the network industry. Various state-of-the-art methods have been employed in regards to solving this issues, Data-Mining being one of the most effective approaches. However, the generalization ability of individual data mining algorithms has limitations, and hence detecting complex attacks remains a daunting task. In such a context, this paper presents a novel hybrid technique based on the combination of both clustering and classification data mining approaches for developing an effective network intrusion detection system (NIDS) with increased accuracy and reduced false alarm rate. The models are trained and tested using the NSL-KDD intrusion detection dataset and information gain based feature reduction is used. In the result, a comparative study between different data mining classification methods after clustering is presented. Finally, it is
experimentally prove that the proposed method is considerably more effective compared to some contemporary hybrid intelligence approaches.

References

A Cluster based Hybrid Framework for Network Intrusion Detection


**Index Terms**

Computer Science  
Security

**Keywords**