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

applications, 30(1), 114-132.
classification in adaptive intrusion detection using decision tree. World Academy of Science,
Engineering and Technology, 63, 86-90.
Information Technology, 72(3).
19. Golmah, V. (2014). An efficient hybrid intrusion detection system based on C5.0 and
SVM. International Journal of Database Theory and Application, 7(2), 59-70.
machine for intrusion detection system. IJCAT International Journal of Computing and
Technology, 1(3).
the 20th International Conference on Machine Learning (ICML-03) (pp. 147-153).
applications. World scientific.
IEEE.
network intrusion detection system based on data mining techniques: a survey. In Intelligent
Systems and Control (ISCO), 2014 IEEE 8th International Conference on (pp. 274-280). IEEE.
27. Tribak, H., Delgado-Marquez, B. L., Rojas, P., Valenzuela, O., Pomares, H., & Rojas, I.
(2012, May). Statistical analysis of different artificial intelligent techniques applied to Intrusion
Conference on (pp. 434-440). IEEE.
accurate detection of anomalous network traffic. International Journal for Information Security
30. Information gain in decision trees
32. Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009, July). A detailed analysis of
the KDD CUP 99 data set. In Computational Intelligence for Security and Defense Applications,
detection system based on classification algorithms. International Journal of Advanced
Research in Computer and Communication Engineering, 4(6), 446-452.
intrusion detection through k-means clustering and naives bayes classification. In Proc. 4th Int.
A Cluster based Hybrid Framework for Network Intrusion Detection


Index Terms

Computer Science  

Security

Keywords