World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:12, No:08, 2018

Machine Learning Methods for Network Intrusion Detection

Authors : Mouhammad Alkasassbeh, Mohammad Almseidin

Abstract : Network security engineers work to keep services available all the time by handling intruder attacks. Intrusion Detection System (IDS) is one of the obtainable mechanisms that is used to sense and classify any abnormal actions. Therefore, the IDS must be always up to date with the latest intruder attacks signatures to preserve confidentiality, integrity, and availability of the services. The speed of the IDS is a very important issue as well learning the new attacks. This research work illustrates how the Knowledge Discovery and Data Mining (or Knowledge Discovery in Databases) KDD dataset is very handy for testing and evaluating different Machine Learning Techniques. It mainly focuses on the KDD preprocess part in order to prepare a decent and fair experimental data set. The J48, MLP, and Bayes Network classifiers have been chosen for this study. It has been proven that the J48 classifier has achieved the highest accuracy rate for detecting and classifying all KDD dataset attacks, which are of type DOS, R2L, U2R, and PROBE.

Keywords : IDS, DDoS, MLP, KDD
Conference Title : ICCCNT 2018 : International Conference on Computing Communication and Networking Technologies
Conference Location : New York, United States
Conference Dates : August 27-28, 2018