World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:8, No:02, 2014

Incorporating Multiple Supervised Learning Algorithms for Effective Intrusion Detection

Authors : Umar Albalawi, Sang C. Suh, Jinoh Kim

Abstract : As internet continues to expand its usage with an enormous number of applications, cyber-threats have significantly increased accordingly. Thus, accurate detection of malicious traffic in a timely manner is a critical concern in today’s Internet for security. One approach for intrusion detection is to use Machine Learning (ML) techniques. Several methods based on ML algorithms have been introduced over the past years, but they are largely limited in terms of detection accuracy and/or time and space complexity to run. In this work, we present a novel method for intrusion detection that incorporates a set of supervised learning algorithms. The proposed technique provides high accuracy and outperforms existing techniques that simply utilizes a single learning method. In addition, our technique relies on partial flow information (rather than full information) for detection, and thus, it is light-weight and desirable for online operations with the property of early identification. With the mid-Atlantic CCDC intrusion dataset publicly available, we show that our proposed technique yields a high degree of detection rate over 99% with a very low false alarm rate (0.4%).

Keywords : intrusion detection, supervised learning, traffic classification, computer networks
Conference Title : ICCNS 2014 : International Conference on Computer Networks and Security
Conference Location : Barcelona, Spain
Conference Dates : February 27-28, 2014

Open Science Index, Computer and Information Engineering Vol:8, No:02, 2014 publications.waset.org/abstracts/5421.pdf