World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:14, No:12, 2020

Filtering Intrusion Detection Alarms Using Ant Clustering Approach

Authors : Ghodhbani Salah, Jemili Farah

Abstract : With the growth of cyber attacks, information safety has become an important issue all over the world. Many firms rely on security technologies such as intrusion detection systems (IDSs) to manage information technology security risks. IDSs are considered to be the last line of defense to secure a network and play a very important role in detecting large number of attacks. However the main problem with today's most popular commercial IDSs is generating high volume of alerts and huge number of false positives. This drawback has become the main motivation for many research papers in IDS area. Hence, in this paper we present a data mining technique to assist network administrators to analyze and reduce false positive alarms that are produced by an IDS and increase detection accuracy. Our data mining technique is unsupervised clustering method based on hybrid ANT algorithm. This algorithm discovers clusters of intruders' behavior without prior knowledge of a possible number of classes, then we apply K-means algorithm to improve the convergence of the ANT clustering. Experimental results on real dataset show that our proposed approach is efficient with high detection rate and low false alarm rate.

Keywords : intrusion detection system, alarm filtering, ANT class, ant clustering, intruders' behaviors, false alarms
Conference Title : ICSRD 2020 : International Conference on Scientific Research and Development
Conference Location : Chicago, United States
Conference Dates : December 12-13, 2020