Abstract

Content-Centric Networks (CCNs) have recently emerged as an innovative trend to overcome many inherent security problems in the IP-based (host-based) networks by securing the content itself rather than the channel through which it travels. In this network architecture new kinds of attacks - ranging from DoS to privacy attacks - will appear. Therefore, it is becoming necessary to design a flexible and powerful mechanism to be able to detect them in an intelligent manner the first time they are employed. In this paper, a novel anomaly detection system has been proposed to detect known and previously unknown types of attacks using an efficient unsupervised learning engine that utilizes clustering with the optimal number of clusters, high detection rate, and low false positive rate in the same time over the CCN traffics flows. This paper compares the performance of five different clustering algorithms in the proposed anomaly detection system including K-means and Farthest First as Partitioning clustering, Cobweb as Hierarchical clustering, DBSCAN as Density-based clustering and Self Organizing Map (SOM) as Model-based clustering. Results show that DBSCAN method is the most efficient one for this purpose since it outperforms the other ones in terms of high detection rate and low false positive rate in the same time.

Index Terms

Computer Science  Data Processings

Keywords

Content-centric networking  Anomaly Detection  Clustering Analysis