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.
Filtering Intrusion Detection Alarms using Ant Clustering Approach

- Przemyslaw kazienko & Piotr Dorosz (2003), "Intrusion Detection Systems (IDS)"; apos; Part 2 Classification, Methods and Techniques. IT FAQ.
- Rachman, (2005), "Baseline analysis of security data." Securimine Software Inc; www.securimine.com
- Monmarche & Slimane, 1999, "On improving clustering in numerical databases with artificial ants"; Advances in Artificial Life, pp. 626-635.
- Lumer & Faieta, 1995, "Exploratory database analysis via self-organization";
- Shanfei Li & Wei Huang, 2010, "An Improved Ant-Colony Clustering Algorithm Based On the Innovational Distance Calculation Formula"; Third International Conference
on Knowledge Discovery and Data Mining, pp. 342-346, 2010.

**Index Terms**

Computer Science  
Security

**Keywords**

Intrusion detection system  alarm filtering  ANTClass  ant clustering  intruders' behaviors  
false alarms.