New Scheme to Identify Intrusion Outliers by Machine Learning Technique

Abstract

In network administration, computers and network systems need to be protected against malicious attacks. The success of an intrusion detection system depends on the selection of the appropriate features in detecting the intrusion activity. The selection of unnecessary features may cause computational issues and reduce the accuracy of detection. In the existing work, a novel detection approach is used through a one-class learning algorithm based on support vector machine classification. It can be also used in a Bayesian framework to estimate the posterior class probabilities of test data with unknown class. This algorithm can detect the system anomalies and monitor the health of a system. It does not allow updating the training data with new information. Therefore, the accuracy of the algorithm is low for the test data. The proposed work aims to improve the performance of attack detection and to reduce the false-alarm rate using hybrid classifier. This approach effectively identifies the set of attacks such as Denial of Service, Probe, and User to Root and Remote to Local attacks. In addition, an Experimental evaluation is carried out to compare the performance of existing classifier with the proposed Decision tree-Bayesian network classifier.
New Scheme to Identify Intrusion Outliers by Machine Learning Technique

References

- Huy Anh Nguyen, Deokjai Choi, "Application of Data Mining to Network Intrusion Detection: Classifier Selection Model&qu...".
- Jiawei Han and Micheline Kamber, "Data Mining: Concepts and Techniques", 2nd Edition, University of Illinois.
- Sudipto Banerjee and Andrew O. Finley (2009), "Bayesian Linear Models", University of Minnesota, U. S. A.
- WEKA: Data Mining Software in Java (2008), ttp://www.cs.waikato.ac.nz/ml/weka
- F. Angiulli, S. Basta, and C. Pizzuti, "Distance-based detection and prediction of outliers", IEEE Transactions on Knowledge and Data Engineering, vol. 18, no. 2, pp. 1-15.

Index Terms

Computer Science
Security

Keywords