Abstract

An Intrusion Detection System (IDS) is very important to safeguard computer networks against confidentiality, integrity and availability breaches. Detection effectiveness of an IDS is characterized by high detection accuracy, high detection rate and low false positive rate. Many existing Anomaly-based Intrusion Detection Systems (AIDS) are ineffective and fail to distinguish between normal and abnormal data. This affects the detection accuracy and generates a high false alarm rate. Therefore, this paper has proposed a new AIDS based on Supervised and unsupervised methods that effectively detects attacks with a low false positive rate. The proposed approach consists of ensemble clusters with an efficient clustering technique, and enhancing the capability of the detection classifier by utilizing an efficient method. Experimental results showed an improvement in the detection accuracy which scored 97.0% on the overall accuracy and 0.03 % on the false positive rate for all classes of network traffic. Hence, this validates the proposed GSA-based AIDS.

References
Anomaly Intrusion Detection System based on Unlabeled Data

Index Terms

Computer Science  Security

Keywords

Network Intrusion Detection, ensemble clusters, unlabeled data.