Abstract

An intrusion detection system (IDS) is an active process or device that analyzes system and network activity for unauthorized entry. Nowadays many intrusion detection systems are developed based on many different machine learning techniques. Some of the models are based on single classifying techniques while some models are based on combining different classifying techniques, such as hybrid or ensemble techniques. The basic task is to classify network activities (in the network log as connection records) as normal or abnormal while minimizing misclassification. Even if different classification models have been developed for network intrusion detection, each classification technique has its vitality and vulnerability. The machine learning based SVM method is a good choice for learning with little volume of data. Whenever new information is added into a system, updating of the old model is required immediately to ensure that the system is properly protected. As retraining may take weeks, or even months, it is impractical to retrain the new model on all available data. Thus, a mechanism is needed to generate an adaptive model that can be updated by cooperation of the old model with the new information. We can take advantage of the clustering based on Bee Colony in updating the models. We propose a new approach of combining SVM and Bee Colony to achieve high quality performance of Intrusion Detection System. Our algorithm is implemented and evaluated using a standard benchmark KDD99 data set. In this paper
experimental result shows that SVM with Bee colony achieves an average accuracy is 88.46%.

References

- Wenying Feng, Qinglei Zhang, Gongzhu Hu, Jimmy Xiangji Huang. 2014. Mining network data for intrusion detection through combining SVMs with ant colony networks, Future Generation Computer Systems.

Index Terms

Computer Science Security

Keywords

Intrusion Detection System (IDS) Data Classification Machine Learning Support Vector Machine (SVM)

Bee Colony.