Abstract

Nowadays, as information systems are more open to the Internet, the importance of secure networks is tremendously increased. New intelligent Intrusion Detection Systems (IDSs) which are based on sophisticated algorithms rather than current signature-base detections are in demand. In this paper, we propose a new data-mining based technique for intrusion detection using an ensemble of binary classifiers with feature selection and multiboosting simultaneously. Our model employs feature selection so that the binary classifier for each type
of attack can be more accurate, which improves the detection of attacks that occur less frequently in the training data. Based on the accurate binary classifiers, our model applies a new ensemble approach which aggregates each binary classifier’s decisions for the same input and decides which class is most suitable for a given input. During this process, the potential bias of certain binary classifier could be alleviated by other binary classifiers’ decision. Our model also makes use of multiboosting for reducing both variance and bias. The experimental results show that our approach provides better performance in terms of accuracy and cost than the winner entry of the ‘Knowledge Development and Data mining’ (KDD) ’99 cup challenge. Future works will extend our analysis to a new ‘Protected Repository for the Defense of Infrastructure against Cyber Threats’ (PREDICT) dataset as well as real network data.

References

- MIT Lincoln Laboratory, "DARPA intrusion detection evaluation", http://www.ll.mit.edu/IST/ideval/, MA, USA.
- J. R. Quinlan, "C4.5: programs for machine learning", Morgan Kaufmann Publishers,
New Strategy for detecting Intrusion by using c4.5 algorithm

1993.

Index Terms

- Computer Science
- Computational Intelligence

Keywords

- Intrusion Detection
- Data Mining
- Ensemble Approach
- Feature Selection
- Multiboosting