Abstract

In this paper, we introduce a new learning algorithm for adaptive intrusion detection using boosting and naïve Bayesian classifier, which considers a series of classifiers and combines the votes of each individual classifier for classifying an unknown or known example. The proposed algorithm generates the probability set for each round using naïve Bayesian classifier and updates the weights of training examples based on the misclassification error rate that produced
Adaptive Intrusion Detection based on Boosting and Naïve Bayesian Classifier

by the training examples in each round. This algorithm addresses the problem of classifying the large intrusion detection dataset, which improves the detection rates (DR) and reduces the false positives (FP) at acceptable level in intrusion detection. We tested the performance of the proposed algorithm with existing data mining algorithms by employing on the KDD99 benchmark intrusion detection dataset, and the experimental results proved that the proposed algorithm achieved high detection rates and significantly reduced the number of false positives for different types of network intrusions.

Reference

- Dewan Md. Farid, Nguyen Huu Hoa, Jerome Darmont, Nouria Harbi, and Mohammad


- Y. Bouzida, and F. Cuppens, “Detecting known and novel network intrusions,” Security
Adaptive Intrusion Detection based on Boosting and Naïve Bayesian Classifier

and Privacy in Dynamic Environments, 2006, pp. 258-270.
- C. Elkan, 2007, Result of the KDD’99 Knowledge Discovery Contest

Index Terms

Computer Science

Security
<table>
<thead>
<tr>
<th>Key words</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Boosting</td>
<td>Naïve Bayesian Classifier</td>
<td>Intrusion</td>
</tr>
<tr>
<td>Detection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detection Rate</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>False Positive</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>