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
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.

- S. Peddabachigari, A. Abraham, and J. Thomas, “Intrusion detection systems using
decision tress and support vector machines,” International Journal of Applied Science and

- D. Barbara, N. Wu, and Suchil Jajodia, “Detecting novel network intrusions using Bayes

- D. Barbara, J. Couto, S. Jajodia, and N. Wu, “ADAM: A tested for exploring the use of
data mining in intrusion detection,” Special Interest Group on Management of Data (SIGMOD),

- N. B. Amor, S. Benferhat, and Z. Elouedi, “Naïve Bayes vs. decision trees in intrusion
detection systems,” In Proc. of the 2004 ACM Symposium on Applied Computing, New York,

Journal of Computer Science and Network Security (IJCNSNS), Vol. 7, No. 12, December 2007,
pp. 258-263.

system,” In Proc. of the 16th International Conference on Neural Information Processing,
December 2009.

- Y. Freund, and R. E. Schapire, “A decision-theoretic generalization of on-line learning and
119-139.


- Mukkamala S, Sung AH, and Abraham A, “Intrusion detection using an ensemble of
167-182.

- Chebrolu S, Abraham A, and Thomas JP, “Feature deduction and ensemble design of

- C. Elkan, 2007, Result of the KDD’99 Knowledge Discovery Contest


- A. D. Joshi, “Applying the wrapper approach for auto discovery of under-sampling and
over-sampling percentages on skewed datasets,” M.Sc. Thesis, University South Florida,
Tampa, 2004, pp. 1-77


Index Terms

Computer Science  Security
Key words

- Boosting
- Naïve Bayesian Classifier
- Intrusion Detection
- Detection Rate
- False Positive