Application of an AODE Based Classifier to Detect DOS Attacks

Levent Koc and Alan D. Carswell,

Center for Security Studies, University of Maryland University College, Maryland, USA

Summary

Digital forensics often utilize network intrusion detection systems based on various data mining methods to detect and collect evidence on intrusion events such as Denial of Service (DOS) attacks. Findings of our experiments reveal that a classification model based on averaged one-dependence estimators (AODE) can be used for this purpose. AODE is an extension of Naïve Bayes method which relies on conditional independence assumption. A multiclass classifier model based on AODE is proposed for accurate detection of DOS attacks. Results of the experiments using KDD'99 intrusion detection dataset indicate the proposed classifier based on AODE model performs better than the classifier model based on traditional Naïve Bayes method in terms of accuracy to detect DOS attacks.

Key words:

Averaged one-dependence estimators (AODE), Naïve Bayes classifier, Denial of service (DOS) attack, Intrusion detection system (IDS)

1. Introduction

Data breaches become one of the important topics of digital forensics. Intrusion investigation is a specialized subset of digital forensic investigation which is concentrated on determining the nature and scope of unauthorized access, and usage of computer systems. The acquired intrusion detection systems data might come from one or more network elements and it might be centrally collected or distributed based on the network configuration. Besides the network packet dumps, it can have inferred and correlated data which manifest itself as network intrusion alerts [1].

Intrusion detection systems are generally based on two major detection principles: 1) signature detection and 2) anomaly detection. Signature detection relies on a learning algorithm that is trained by a dataset in which each network packet is categorized as either an intrusion or a normal event. Even though the algorithm cannot detect new attacks that were not included in the training set, it can be automatically retrained with the new attack instances through a new training. Anomaly detection generally relies on building the models of normal network events and detecting the events that deviate from these models. Although this method can detect new types of attack events because it only relies on known normal events, this method has disadvantages of high rate of false alarms due to previously unobserved normal events. There are also hybrid models which utilize both signature detection and anomaly detection principles to improve the detection performance [2].

Based on where the intrusion detection occurs, intrusion detection systems' are categorized in two types: 1) host based, 2) network based. The host based intrusion detection system will only protect its own local (host) machine. The network based intrusion detection system allows the intrusion detection process distributed along the network. For example, using the agent based technology; a distributed system will protect whole network. In this approach intrusion detection system might control or monitor network firewalls, network routers or network switches as well as the client machines [2].

The order and scope of the data collected can also depend on the investigated case. For example, a network intrusion detection system log may link an event to a host. The linked host audit logs may link the event to a certain account. The host based intrusion detection system log may indicate what actions that user performed. The process of gathering and correlating the data might be automated using tools such as centralized logging and security event management software [3].

The data mining, specifically classification, is one of the most common approaches applied to the intrusion detection problem. Our research study proposes a network intrusion detection model built on a signature based multiclass classifier to detect network attacks specifically denial of service (DOS) attacks. This classification model is based on averaged one-dependence estimators (AODE) [4] which is an extension of naïve Bayes model [5]. Naïve Bayes is one of the most popular and simple data mining methods. Both AODE and naïve Bayes models are applied to many domains successfully including to the intrusion detection. Brief introduction to both models and existing research are presented in the Related Works section of this article.

Our experimental research study findings indicate that our AODE classifier based intrusion detection model detects DOS attacks better than the traditional naïve Bayes classifier based model in terms of accuracy. Classic KDD Cup 1999 intrusion detection dataset (KDD'99) [6] is used in our experiments. Although the KDD'99 dataset has some debated drawbacks [7], its use in testing new claims on intrusion detection problem is very common [8]. A brief discussion on KDD'99 dataset and the introduction of our

Manuscript received February 5, 2015
Manuscript revised February 20, 2015

experimental intrusion detection model including the feature selection and discretization methods applied are offered in the Research Method section. This section also presents the results and analysis of our experiments. The last section is allocated for conclusion with a brief summary of our research study, its findings and possible future work.

2. Related Work

Since 1980s, there is significant progress on the research and application of data mining specifically classifier methods for the signature detection based network intrusion detection systems [9-11].

Classification is one of the most common approaches in data mining. It relies on constructing a classifier from a given set of training instances which consist of attributes a_1, a_2,…,a_n from the attribute sets represented by A_i where $i=1,2,\ldots,n$ and class labels from class set C.

In the intrusion detection domain, each instance is represented by a network event, for example a TCP packet; each attribute of this instance is represented by the attribute from this network event. In the training set, each instance is labeled as one of the classes, in our context, normal or attack event. Attacks can be assigned to more granular classes such as denial of service (DOS), probe, remote to local user (R2L) and user to root (U2R).

Since our intrusion detection model based on naïve Bayes and its extension AODE classifier models, next section allocated for the discussions of these two classification approaches.

2.1 Naïve Bayesian Classifiers

Naïve Bayes classifier model is the simplest form of Bayesian Network classifier. Its popularity comes from its simplicity which relies on the independence of attributes assumption. If a Bayesian classifier is defined as:

$$arg \max_{c \in C} P(c)P(a_1, a_2, \ldots, a_n|c). \quad (1)$$

Then, with the assumption that all attributes are independent given the class, then, naïve Bayes classifier can be defined as:

$$arg \max_{c \in C} P(c) \prod_{i=1}^{n} P(a_i|c) . \quad (2)$$

With this assumption in naïve Bayes, none of the attribute nodes have any parent from attributes nodes, but each attribute node has the class node as its parents as shown in the Figure 1. The simplicity brought by the assumption of independence of attributes in naïve Bayes classifier method also provides savings in terms of computational cost. That is the reason naïve Bayes is widely used in many problem domains successfully especially in the domains that have datasets which support the independence of attributes assumption.

The performance of the naïve Bayes method decreases as the dependency among the attributes in a dataset increases. In the last couple of decades, researchers have put significant effort to relax the assumption of independence of attributes of the naïve Bayes method to increase the accuracy. These efforts include the tree-augmented naïve Bayes (TAN) [12] and averaged one-dependence estimators (AODE) [13].

Figure 1 Naive Bayes Classifier Structure

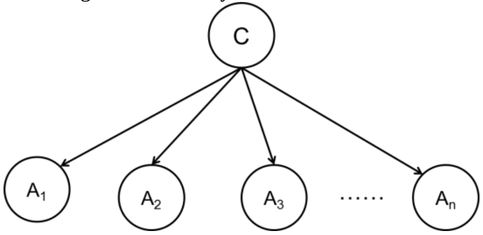
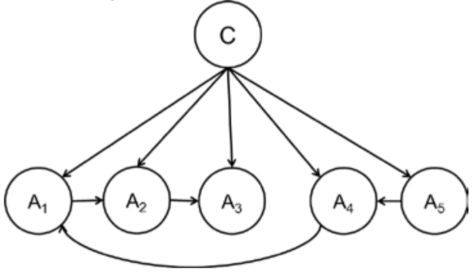


Figure 2 ODE Classifier Structure



Averaged one-dependence estimators (AODE) approach [4] is one of the recent enhancements on naïve Bayes model. It relies on the averaging the predictions of qualified one-dependence estimators in which each attribute has one correlated attribute as illustrated in Figure 2. To reduce the prediction variance, bagging method [14] is used. Experiments on multiple datasets in the Yang [15] study produced favorable performance results for the AODE model compared to traditional naïve Bayes model. AODE classifier model is applied to several problem domains including biomedical [16], spam filtering [17] and network intrusion detection [13].

2.2 Application of Naïve Bayesian and AODE Classifiers to Intrusion Detection Problem

Bayesian classifiers including the naïve Bayes classifier model and its extended models are frequently used in the intrusion detection domain. One of the earlier implementations of the Bayesian method in intrusion detection domain is Barbara study [18] which is called Audit Data Analysis and Mining (ADAM). ADAM is based on an anomaly detection system built upon pseudo-

Bayes estimators to estimate the prior and posterior probabilities of new attacks. These probabilities are used to construct a naïve Bayes classifier for classifying normal and attack events without prior knowledge about new attacks [18].

In more recent studies, extended models of the naïve Bayes are applied to the intrusion detection problem including the TAN classifier which is implemented using the KDD'99 dataset [12], the AODE classifier which is implemented using a subset of KDD'99 dataset called NSL-KDD 99 [13]. In the AODE binary classifier modelled in this study, Group Method for Data Handling (GMDH) algorithm is used for feature selection. Binary classifiers only predict if a network event is normal or anomalous.

Our application of AODE classifier to intrusion detection differs from the Baig study [13] so that our model is based on multiclass classifier rather than binary classifier; our model uses original KDD'99 dataset rather than NSL-KDD 99 dataset; our model is built upon AODE along with the discretization method called Entropy Minimization Discretization (EMD) and feature selection method called consistency-based filter (CONS) rather than GMDH method.

3. Research Method

Based on the promising results observed in earlier studies, our intrusion detection model utilizes the AODE classifier. We test our claims that intrusion detection system model based on AODE multiclass classifier provides better accuracy than the one based on traditional naïve Bayes classifier on KDD'99 dataset.

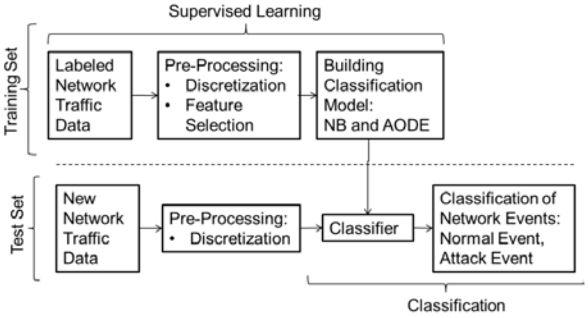
3.1 Dataset

KDD Cup 1999 dataset is one of the few publicly available network intrusion detection dataset and it is the only available labeled dataset appropriate for supervised learning models like the one built in our study. It is widely used in network intrusion detection domain to analyze the performance of the intrusion detection models.

Since its introduction in MIT Lincoln laboratory for the evaluation of DARPA KDD Cup 1998 intrusion detection challenge, there are few studies published to analyze the dataset and some of these studies debate its limitations [7]. Regardless of these discussions, it is widely recognized as benchmark and baseline for intrusion detection research. As most intrusion detection researchers do, we use this data set to test our claims. A worthy introduction and analysis of this dataset is available in the study [7].

While the training set has 494021 instances, the test set has 311029 in the 10% KDD'99 dataset we used. Each instance contains 34 continuous, 7 discrete and total 41 attributes. Since naïve Bayes and AODE classifier models work only with discrete variables, our research model, as illustrated in Figure 3, requires a pre-processing step for discretization of the continuous variables.

Figure 3 Research Model



The pre-processing step in our model includes a discretization step based on the Entropy Minimization Discretization (EMD) method which is built on the minimum entropy heuristic required to discretize continuous features. It selects a cut point for discretization based on the class entropy of the candidate partitions; this cut point is then recursively applied to the created intervals until the stopping condition, which is based on the minimum description length (MDL) method, is reached [19].

Because KDD'99 dataset contains high number of attributes, as most of the data mining methods applied to this domain, naïve Bayes and its extensions suffers from the high data dimensionality issue. One method to resolve this issue is to select a subset of the attributes to apply the model. Our model utilizes a feature selection method called consistency-based filter (CONS) as part of the pre-processing phase.

The CONS method [20] utilizes an inconsistency criterion that specifies the extent to which the dimensionally reduced data can be accepted. In each round, it generates a random subset and more consistent set is recorded [21].

3.2 Experiments and Results

As implementation of the research model illustrated in the Figure 3, we executed our simulation experiments using Weka tool [22]. We applied two-tailed t-test with a 95% confidence level to compare the models in our study.

Consistent with our framework, we applied supervised *discretize*() method for EMD discretization of the continuous variables of the 10% KDD'99 dataset. After discretization, we proceed with the feature selection step by applying the consistency subset filtering with the default values. Seven attributes count, *dst_host_srv_count*, *dst_host_same_srv_rate*, *dst_host_diff_srv_rate*, *duration*, *service* and *src_bytes* were selected.

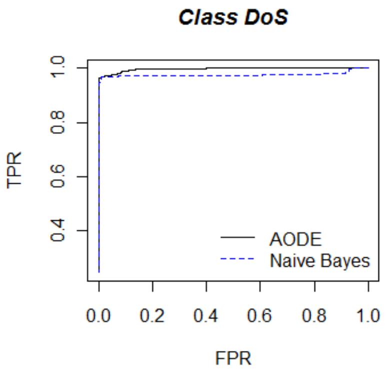
After the pre-processing step, we built our classifier models for naïve Bayes and AODE classifiers by using our preprocessed dataset. A widely accepted method, 10-fold cross-validation was applied to accurately reflect the given training data used to build the classifier models. This method divides the dataset into 10 random subsets, In 10 iteration, 9 out of this 10 subsets is used for training and 1 subset used for testing. The mean of the results of the 10 iteration reflects the overall accuracy. This step concludes the supervised learning, in other words training part, of our model in the Figure 3. In the testing part, after the pre-processing of the test dataset, built classifier models for AODE and naïve Bayes are applied to the test set.

Table 1 Test results for the detection performance of class DOS

Model	***Accurac y***	***Error Rate***	***AUC***
Naïve Bayes	0.9618	0.0382	0.9760
AODE	0.9677	0.0323	0.9970

Accuracy, the error rate and area under receiver operating characteristics (ROC) curve are used to evaluate the performance of detecting the DOS attacks in our study. These measures are commonly accepted to summarize and compare the classifier performance [23]. Accuracy is the rate of correctly classified instances, and the error rate is the rate of misclassified instances. A ROC graph illustrates relative tradeoffs the true positive and false positive results. It is generally used for cost benefit analysis. A method is used to reduce the representation of the ROC graph into a singular scalar value to measure and compare classifier performance. This method relies on the calculation of the area under the ROC curve (AUC) [24].

Figure 4 ROC graph for detection of class DOS



As seen in the Table 1, the experiment results indicate AODE based intrusion detection model's accuracy is 0.9677, error rate is 0.0323, and the area under ROC curve is 0.9970. Results also show traditional naïve Bayes based model's accuracy is 0.9618, error rate is 0.0382, and the area under ROC curve is 0.9760. Figure 4 also illustrate that AODE based model always closer to top left corner and occupy a larger area under the curve than the naïve Bayes based model. These findings indicate that AODE based intrusion detection model performed better than naïve Bayes based model in terms of all there measures.

4. Conclusion

In this article, we explained briefly the importance of intrusion detection systems for digital forensic efforts to detect malicious attacks including the DOS attacks. We summarized the use of data mining, specifically classifier methods including the Bayesian network classifiers in intrusion detection systems. We reviewed the naïve Bayes model which relies on the independence of attributes assumption and naïve Bayes' extended models to relax this assumption including the AODE model. We introduced our intrusion detection model based on AODE multiclass classifier along with the EMD discretization and consistency based feature selection filter. We applied and tested our model using classic KDD'99 intrusion detection dataset. Our experiment results indicate that our AODE classifier based intrusion detection model performed better than the traditional naïve Bayes classifier based model in terms of detection of DOS attacks in accuracy, error rate and area under ROC curve measures.
For future work, using a similar research model, we aim to explore the effects of the discretization and feature selection methods for the application of naïve Bayes models in the intrusion detection domain.

References

[1] E. Casey, *Handbook of digital forensics and investigation*: Academic Press, 2009.

[2] P. Kabiri and A. A. Ghorbani, "Research on intrusion detection and response: A survey," *International Journal of Network Security*, vol. 1, pp. 84-102, 2005.

[3] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response," *NIST Special Publication*, pp. 800-86, 2006.

[4] G. I. Webb, Boughton, J. R., Wang, Z., "Not so naive Bayes: aggregating one-dependence estimators," *Machine Learning*, vol. 58, pp. 5-24, 2005.

[5] Langley, Iba, and Thompson, "An analysis of Bayesian classifiers," in *Proceedings of the tenth national conference on artificial intelligence*, San Jose, California, 1992, pp. 223-228.

[6] KDD-Cup. (1999). *KDD Cup 1999 Data*. Available: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[7] M. Tavallaee, Bagheri, E., Lu, W., Ghorbani, A.A., "A detailed analysis of the kdd cup 99 data set," in *IEEE Symposium on Computational Intelligence in Security and*

Defense Applications (CISDA 2009), Ottawa, Canada, 2009, pp. 53-58.

[8] C. Tsai, Hsu, Y., Lin, C., Lin, W., "Intrusion detection by machine learning: A review," *Expert Systems with Applications,* vol. 36, pp. 11994-12000, 2009.

[9] J. Cannady, "The application of artificial neural networks to misuse detection: initial results," in *Proceedings of the Recent Advances in Intrusion Detection ’98 Conference,* Louvain-la-Neuve, Belgium, 1998, pp. 31-47.

[10] T. F. Lunt, "Real-time intrusion detection," in *COMPCON Spring '89. Thirty-Fourth IEEE Computer Society International Conference: Intellectual Leverage, Digest of Papers.*, 1989, pp. 348-353.

[11] W. Lee, Stolfo, S. J., Mok, K. W., "A data mining framework for building intrusion detection models," in *Proceedings of the 1999 IEEE Symposium on Security and Privacy*, Oakland, California, 1999, pp. 120-132.

[12] S. Benferhat, Boudjelida, A., Drias, H., "On the use of TAN in intrusion detection systems," in *Second International Conference on Information Processing (ICIP)*, 2008, pp. 1-13.

[13] Z. A. Baig, Shaheen, A. S., AbdelAal, R., "An AODE-based intrusion detection system for computer networks," in *World Congress on Internet Security (WorldCIS), 2011*, London, United Kingdom, 2011, pp. 28-35.

[14] L. Breiman, "Bagging predictors," *Machine Learning,* vol. 24, pp. 123-140, 1996.

[15] Y. Yang and G. I. Webb, "A comparative study of discretization methods for Naive-Bayes classifiers," in *Proceedings of PKAW 2002: The 2002 Pacific Rim Knowledge Acquisition Workshop*, Tokyo, Japan, 2002, pp. 159-173.

[16] S. L. Win, Z. Z. Htike, F. Yusof, and I. A. Noorbatcha, "Gene expression mining for predicting survivability of patients in early stages of lung cancer," *International Journal on Bioinformatics & Biosciences,* vol. 4, 2014.

[17] C. Chen, Y. Tian, and C. Zhang, "Spam filtering with several novel bayesian classifiers," in *Pattern Recognition, 2008. ICPR 2008. 19th International Conference on*, 2008, pp. 1-4.

[18] D. Barbara, Wu, N., Jajodia, S., "Detecting novel network intrusions using bayes estimators," in *First SIAM Conference on Data Mining*, Chicago, IL, 2001.

[19] U. Fayyad and K. Irani, "Multi-interval discretization of continuous-valued attributes for classification learning," in *Proceedings of the 13th International Joint Conference on Artifical Itelligence, IJCAI'93*, Chambéry, France, 1993, pp. 1022-1029.

[20] L. Huan and R. Setiono, "Feature selection via discretization," *Knowledge and Data Engineering, IEEE Transactions on,* vol. 9, pp. 642-645, 1997.

[21] Hall, "Correlation-based feature selection for machine learning," Doctoral Dissertation, Department of Computer Science, The University of Waikato, Hamilton, New Zealand, 1999.

[22] I. H. Witten, Frank, E., Hall, M. A., *Data mining : practical machine learning tools and techniques*, 3rd ed. Burlington, MA: Morgan Kaufmann, 2011.

[23] N. Japkowicz, Shah, M., *Evaluating Learning Algorithms : a classification perspective*. New York: Cambridge University Press, 2011.

[24] T. Fawcett, "An introduction to ROC analysis," *Pattern Recognition Letters,* vol. 27, pp. 861-874, 2006.

Levent Koc is Cybersecurity Postdoctoral Fellow in Center for Security Studies at the University of Maryland University College, in Adelphi, Maryland. He holds a BSc. in Computer Science from Bilkent University, MSc. and PhD in Systems Engineering from The George Washington University. His research interests include information security, data science, knowledge management, software engineering and cloud computing.

Alan D. Carswell is a Collegiate Professor, Vice Dean, Cybersecurity and Information Assurance Department and Director of Center for Security Studies at the University of Maryland University College, in Adelphi, Maryland. He holds a Bachelor of Science in Civil Engineering from Northwestern University, an MBA from Harvard Business School and received his Ph.D. from the University of Maryland, College Park in 2001. His research interests include knowledge management and systems development. His dissertation research focused on facilitating student learning in an asynchronous learning environment.