2010 Second International Conference on Computer Engineering and Applications

Comparing Single and Multiple Bayesian Classifiers Approaches for Network Intrusion Detection

Kok-Chin Khor, Choo-Yee Ting, Somnuk-Phon Amnuaisuk
Faculty of Information Technology
Multimedia University
Jalan Multimedia, 63100, Cyberjaya, Selangor, Malaysia
{kckhor, cyting, somnuk.amnuaisuk}@mmu.edu.my

***Abstract*—A general strategy for improving the performance of classifiers is to consider multiple classifiers approach. Previous research works have shown that combination of different types of classifiers provided a good classification results. We noticed a raising interest to incorporate single Bayesian classifier into the multiple classifiers framework. In this light, this research work explored the possibility of employing multiple classifiers approach, but limited to variations of Bayesian technique, namely Naïve Bayes Classifier, Bayesian Networks, and Expert-elicited Bayesian Network. Empirical evaluations were conducted based on a standard network intrusion dataset and the results showed that the multiple Bayesian classifiers approach gave insignificant increase of performance in detecting network intrusions as compared to a single Bayesian classifier. Naives Bayes Classifier should be considered in detecting network intrusions due to its comparable performance with multiple Bayesian classifiers approach. Moreover, time spent for building a NBC was less compared to others.**

Multiple Classifiers, Intrusion Detection, Bayesian Classifiers

I. INTRODUCTION

Intrusion Detection System (IDS) is one of the important measures to mitigate the problem of computer network intrusions. IDSs focus not only on the detection of abnormal activities in computer networks, but also determining whether such activities are malicious or benign. As such, IDSs must be capable of inferring the intent of the activities but also its consequences or impacts to the computer networks [1].

There are basically two types of IDS, namely, *host-based IDS* (HIDS) and *network-based IDS* (NIDS). HIDS concentrate on the activities in a host without considering the activities in the computer networks. On the other hand, NIDS put its focus on computer networks without examining the hosts' activities.

Both *inline* and *passive* technologies can be implemented for HIDS and NIDS. An *inline* IDS is able to prevent further damages on computer network if network intrusions are detected. Conversely, a *passive* IDS only records the intrusive activities without taking any further action to reduce the damages done by intruders.

There are two fundamental approaches for detecting intrusions in computer networks. IDS that utilize *misuse detection* approach detects only known intrusions. Whenever there is a novel type of intrusion, the signatures of the IDS has to be updated. To detect novel intrusions, IDS that utilize the *anomaly detection* approach will build a profile for computer networks. Any activities that are deviated from the built profile will be considered as intrusions [2].

Researchers in network intrusion detection domain put herculean efforts utilizing data mining and Artificial Intelligence (AI) techniques in building efficient IDSs. A single classifier will normally be used in detecting intrusions. However, in order to increase the classification accuracies, a general strategy that combines various types of classifiers is normally implemented. A multiple classifiers framework generally gives better performance in many research domains. Such strategy is commonly seen in the network intrusion detection domain where different types of classifiers are used in building a multiple classifiers framework.

Implementing Bayesian classifiers in a single classifier or multiple classifiers environment has also become an increasing interest in the network intrusion detection domain. However, little attention has been given in evaluating Bayesian classifiers in a multiple classifiers framework based on the fact that there are different types of Bayesian classifiers. *Naïve Bayesian Classifier* (NBC) and *Bayesian Network* (BN), and *Expert-elicited Bayesian Network* (EE) are the variations of Bayesian classifiers.

In this research work, we constructed a multiple classifiers framework that consisted of NBC, BN, and EE. An empirical evaluation was then conducted on standard intrusion detection datasets. Classification results obtained from the empirical evaluation were compared with the results of single Bayesian classifiers. Comments on the classifiers were made based on the comparison of the results.

II. RELATED WORK

A. Multiple Classifers Approach for IDS

Utilizing different types of classifiers in building efficient IDS is common in the IDS research domain [3-8]. Incorporating a Bayesian classifier in an IDS framework of multiple classifiers is also noticed in the research domain.

A novel IDS with multiple-level hybrid classifiers was proposed to detect network intrusions [6]. In this research works, researchers combined the supervised tree classifiers and unsupervised Bayesian clustering to build efficient IDS.

A study by [7] constructed an ensemble classifier by combining both BNs and Classification and Regression Trees (CART) in order to increase the robustness and

978-0-7695-3982-9/10 $26.00 © 2010 IEEE
DOI 10.1109/ICCEA.2010.214

accuracy of the IDS. The features of the intrusion data were selected based on Markov Blanket of the target variables.

In the research conducted by [8], a hybrid intelligent IDS was developed by incorporating BN and Self-Organizing Map (SOM). The SOM theory was slightly modified in this research in order to be used with the standard network intrusion dataset that contains labels. The experimental results showed that the performance of the hybrid intelligent IDS was better compared to the non-hybrid Bayesian learning approach.

B. Bayesian Classifiers

There are two basic types of Bayesian classifiers namely, NBC and BN. Bayesian classifiers are statistical classifiers that are able to perform probabilistic reasoning under uncertainty using Bayes theorem.

Consider X as a data sample consisting *n* features and C_i denotes a class to be predicted (suppose there are *i* classes). Classification is determined by obtaining $P(C_i|X)$, probability for a class conditioned upon an observed data sample X, is equal to its likelihood $P(X|C_i)$ times it probability prior to any observed data sample $P(C_i)$, normalized by dividing P(X).

$$P(C_i|\mathbf{X}) = \frac{P(\mathbf{X}|C_i)P(C_i)}{P(\mathbf{X})} \quad (1)$$

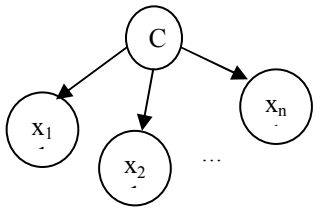

Figure 1. A NBC where features are conditionally independent from each other.

Consider a NBC with n nodes, X_1 to X_n (Fig. 1). The features and classes are represented by nodes, labeled with X_n and C, respectively. An assumption is made in NBC where features are conditionally independent from each other. Such assumption enables fast computation with limited computing resources. Since P(X) is constant for all classes, only $P(X|C_i)$ need to be maximized. Hence,

$$P(\mathbf{X}|C_i) = \prod_{k=1}^{n} P(x_k|C_i) = P(x_1|C_i) \times P(x_2|C_i) \times .. \times P(x_n|C_i) \quad (2)$$

The assumption made in NBC may not reflect the actual domain problem where features related to certain classes have complex relationship with each other. BN is introduced to overcome the problem. Nevertheless, NBC remains a popular classifier looking at its competitive performance in many research domains and its simplicity in computation that allows researchers to save a lot of computational costs [9-10].

A BN uses a graphical model to represent the causal relationship of features. An assumption is made in BN where not every node is connected to each other (Fig. 2). The structure of the graphical model and also a Conditional Probability Table (CPT) of a BN classifier could be built based on a training dataset.

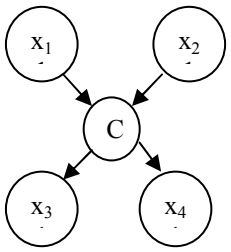

Figure 2. A BN with five nodes.

The graphical model specifies a factorization of the join probability distributions, where a value of a node is conditioned only on its parent node(s) [11]. Hence,

$$P(x_1,...,x_n) = \prod_{i=1}^{n} P(x_i | Parents(C_i)) \quad (3)$$

A BN can also be constructed manually by incorporating knowledge of a domain expert. The construction process is repetitive process which involves model verification and model revision.

Three types of variables, namely, *problem variables*, *information variables*, and *mediating variables* are needed to construct an EE. *Problem variables* are used for classification. On the other hand, *information variables* provide information relevant for solving the classification problem. The *mediating variables* are unobservable variables to counter the dependency of *information variables* for solving the problem. The *information variable* can be further sub-divided into *background information variables* and *symptom information variables*. *Background information variables* provide information available before the problem exists whereas *symptom variables* are consequences after the occurrence of the problem [12]. Fig. 3 shows the causal relationship of the variables in an EE.

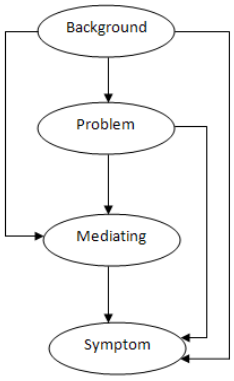

Figure 3. The causal relationship of variables in an EE.

C. Intrusion Detection Datasets

The empirical evaluation was conducted on standard network intrusion datasets derived from DARPA intrusion detection evaluation program [13]. The datasets itself consists of training and testing datasets with number of records 494,021 and 311,029, respectively. Besides the normal network traffics (categorized as Normal), there are 24 attack types in the training dataset. The testing dataset is not from the same distribution as the training data and an additional 14 types of attacks are included in the test dataset. All types of attacks can be categorized into four major categories, namely, *Denial of Service* (DoS), *Probing* (Probe), *Remote to Local* (R2L) and *User to Root* (U2R).

DoS attacks are considered as one of the most feared attacks by network administrator. It can be performed using simple tools or scripts with the purpose of using up resources of a particular host or network. Once a host or network is under the DoS attack, it will not be able to provide services to the users. *Smurf* is one of DoS attacks. *Smurf* attack can be performed by sending large amount of spoofed Internet Control Message Protocol (ICMP) messages to a computer network's broadcast address. Hosts that reside in the computer network are forced to reply the messages. Network traffics will therefore be multiplied and caused congestion in the computer network.

Probing can be performed without much difficulty as tools for such purpose can be found easily in the Internet. An example of such tool is *Nmap*. *Probing* normally comes before an actual intrusion or a DoS attack in order to collect information of a particular host or a computer network. *Probing* can be performed using several methods, namely, ping sweep, port scanning and etc. Information such as application type, version of the application or operating system type can be gathered. Intruders then figure out the vulnerabilities of a victim machine based on the information gathered.

In R2L attacks, packets can be sent by an intruder to a victim machine in a computer network in order to gain access rights. R2L attacks can be performed by taking the advantage of weakly configured victim machines, perform buffer overflow attacks and capture password of hosts in computer networks. On the other hand, U2R attacks can be performed by a local user by exploiting flaws in a poorly designed system to obtain root level privileges [14].

III. METHODOLOGICAL APPROACH

Table 1. The distribution of various attack categories in the network intrusion detection datasets.

Attack Category	No. of Records for Training Dataset	No. of Records for Testing Dataset
Normal	97,277	60,593
DoS	391,458	229,853
Probe	4,107	4,166
R2L	1,126	16,189
U2R	52	228
Total	494,020	311,029

An examination was performed on the datasets and we observed a low number of records for certain types of attacks. To facilitate the task of classification in the later stage, all attacks were categorized into five major categories as stated in Section II. As shown in Table 1, DoS and Normal are dominant categories in the training dataset and therefore easy to classify them. Conversely, it increases the difficulties in classifying the R2L and U2R attacks since their numbers are very much less as compared to the dominant categories.

Both training and testing datasets were first discretized to convert values of features in the datasets to interval type. Discretization was conducted so that the datasets can be used by Bayesian classifiers.

The training dataset was then underwent a feature selection stage. In our previous work [15], we considered only the existing feature selection approaches that are computationally feasible for processing huge datasets. There are basically two types of feature selection approaches: *filter* and *wrapper* approaches. The involved feature selection methods under *filter* approach were namely, *Consistency Subset Evaluator* (CSE) and *Correlation-based Feature Selection Subset Evaluator* (CFSE). On the other hand, Id3, J48, NBC, and BN were involved when employing the *wrapper* approach.

Table 2. Descriptions of the involved features in the optimal feature set.

Features	Description
duration	Length of a connection (in seconds)
service	Type of network service on the destination
flag	Status of a connection (normal or error)
src_bytes	Number of data bytes from source to destination
num_failed_logins	Number of failed login attempts
logged_in	Login successful or otherwise
root_shell	Root shell is obtained or otherwise
num_file_creations	Number of file creation operations
dst_host_diff_srv_rate	Rate of connections to different services
dst_host_rerror_rate	Rate of connections that have ``REJ'' errors

Feature sets were then formed by choosing the features based on the frequency they were selected by different feature selection methods. A feature that was selected by multiple feature selection methods implied its importance in detecting network intrusions. We then evaluated the generated feature sets. The feature set with optimal performance is as shown in Table 2.

Single Bayesian Classifiers, NBC, BN, and EE were built based on the optimal feature set. The classifiers were combined as well to form a multiple Bayesian classifiers. Schemes for combining the classifiers were namely, *product rule* (PROD), *majority vote rule* (MAJ), *average rule* (AVG), *min rule* (MIN), and *max rule* (MAX) [16].

Empirical evaluations were then conducted on the single Bayesian classifiers and the multiple Bayesian classifiers using the testing dataset. The classification accuracies were collected for performance evaluation.

IV. RESULTS AND DISCUSSION

Table 3. The classification accuracies (%) obtained using single Bayesian classifier approach based on the optimal feature sets. NBC performed relative well compared to others. Number in boldface indicates the highest average classification accuracy.

Attack Category	NBC	BN	EE
Normal	99.3	99.5	97.6
DoS	96.3	94	96.5
Probe	86	83.5	84.4
R2L	12	5.5	6.8
U2R	19.7	17.1	22.4
Average	**92.3**	90.3	91.8

Table 4. The classification accuracies (%) obtained using multiple Bayesian classifiers approach worked on five major schemes. The MAJ scheme performed relatively compared to others. Number in boldface indicates the highest average classification accuracy.

Attack Category	MAX	MIN	MAJ	PROD	AVG
Normal	99.5	99.5	99.5	99.5	99.5
DoS	96.7	96.6	97	96.9	97
Probe	82.4	85.8	83.3	85.7	83.4
R2L	8	8.1	8.6	7.9	8
U2R	16.7	18.4	17.5	18	16.7
Average	92.4	92.3	**92.7**	92.5	92.6

The evaluation results are as shown in Table 3-4. Note that the single Bayesian classifiers and multiple Bayesian classifiers performed equivalently well in the first two attack categories (Normal and DoS) due to their huge number of records in the training dataset.

The major challenge of the datasets is to classify R2L and U2R attack categories with low number of records in the training dataset. NBC performed relatively well compared to others in these categories (R2L-12% and U2R-19.7%). EE performed relatively well in U2R category by obtaining a classification accuracy of 22.4%. However, the average classification accuracy obtained by multiple Bayesian classifiers was only slightly better compared to single Bayesian classifier (MAJ-92.7% and NBC-92.3%).

Since NBC has comparable performance as multiple Bayesian classifiers, it should be considered for the building of IDS. Furthermore, the amount of time spent for building a NBC is definitely less compared to others due to its simplicity in computation.

Table 5. The classification accuracies (%) obtained is compared with the results of KDD Cup winner.

	NBC	MAJ	KDD Cup Winner
Normal	99.3	99.5	99.5
DoS	96.3	97	97.1
Probe	86.0	83.3	83.3
R2L	**12.0**	8.6	8.4
U2R	**19.7**	17.5	13.2

The obtained evaluation results were compared to the result of KDD Cup winner who won the data mining competition using the same network intrusion datasets (Table 5). Their performance were comparable but NBC performed relatively well in Probe, R2L and U2R categories.

V. CONCLUSIONS

The major challenge in dealing with the standard network intrusion detection datasets is to classify the attack categories with low number of records. Implementing a multiple classifiers framework is a general strategy to improve the overall performance of classification. We evaluated an approach, which combined only the Bayesian Classifiers for identifying network intrusions. However, the improvement in terms of classification is not significant as compared to a single Bayesian Classifier, NBC. Therefore, we suggested that NBC should be used for building IDS based on the fact that it has comparable performance with multiple Bayesian classifiers approach and the time spent for building NBC is certainly less compared to multiple Bayesian classifiers approach.

We will consider other multiple classifiers approaches to seek the possibility of improving the classification performance in our future work. We would also like to further improve the EE so that it can perform better in R2L and U2R categories in future.

ACKNOWLEDGMENT

The feature selection methods mentioned in this paper are based on WEKA application developed by the University of Waikato.

REFERENCES

[1] D.J. Marchette, Computer Intrusion Detection and Network Monitoring: A Statistical Viewpoint. Springer-Verlag New York, 2001.

[2] Wm. A. Conklin, G.B. White, C. Cothren, D. Williams and R. L. Davis, Principles of Computer Security: Security+ and Beyond, McGraw-Hill, 2005, pp. 309-332.

[3] Aki P.F. Chan, Wing W.Y. Ng, Daniel S. Yeung and Eric C.C. Tsang, "Multiple Classifiers System with Feature Grouping for Intrusion Detection: Mutual Information Approach," LNAI 3683, Springer-Verlag Berlin Heidelberg, 2005, pp: 141-148, doi: 10.1007/11553939.

[4] H.R. Deng and Y.H. Wang, "An Artificial-Neural-Network-Based Multiple Classifiers Intrusion Detection System," Proc. Of 2007 international Conference on Wavelet Analysis and Pattern Recognition, IEEE, Nov. 2007, pp. 683-686, doi: 10.1109/ICWAPR.2007.4420755.

[5] G. Giancinto, F. Roli and L. Didaci, "Fushion of Multiple Classifiers for Intrusion Detection in Computer Networks," Pattern Recognition Letters, vol. 24, 2003, pp. 1795-1803, doi: 10.1016/S0167-8655(03)00004-7.

[6] X. Cheng, Yong P.C., S.M. Lim, "Design of Multiple-level Hybrid Classifiers for Intrusion Detection System Using Bayesian Clustering and Decision Trees," Pattern Recognition, vol.29, 2008, pp. 918-924, doi: 10.1016/j.patrec.2008.01.008.

[7] S. Chebrolu, A. Abraham and J.P. Thomas, "Feature Deduction and Ensemble Design of Intrusion Detection System," Computer Security, vol. 24, 2005, pp. 295-307, doi: 10.1016/j.cose.2004.09.008.

[8] J.L Thames, R. Able and A. Saad, "Hybrid Intelligent Systems for Network Security," Proc. of the 44th Annual ACM Southeast Regional Conference, ACM, March 2006, pp. 286-289. doi: 10.1145/1185448.1185513.

[9] J.W. Han and M. Kamber, Data Mining: Concepts and Techniques, 2nd ed., Morgan Kaufmann, 2006, pp. 310-318.

[10] N. Friedman, D. Geiger and M. Goldszmidt, "Bayesian Network Classifiers," Machine Learning, vol.29, Nov. 1997, pp. 131-163, doi: dx.doi.org/10.1023/A:1007465528199.

[11] K. B. Korb and A. E. Nicholson, Bayesian Artificial Intelligence. Chapman and Hall/CRC, 2003, pp. 29-43.

[12] U.B Kjaerulff, and A.L. Madsen, Bayesian Networks and Influence Diagram: A Guide to Construction and Analysis, 1st ed., Springer, New York, 2008, pp. 140-172.

[13] Computer Network Intrusion Detection, ACM KDDCUP, http://www.sigkdd.org/kddcup/

[14] R.P. Lippmann, J.W. Haines, D.J. Fried, J. Korba and K. Das, "The 1999 DARPA off-line intrusion detection evaluation," Proc. of DARPA Information Survivability Conference and Exposition, 2002, pp. 12-26. doi: 10.1016/S1389-1286(00)00139-0.

[15] K.C. Khor, C.Y. Ting, Somnuk-Phon Amnuaisuk, "Forming an Optimal Feature Set for Classifying Network Intrusions Involving Multiple Feature Selection Methods," unpublished.

[16] J. Kittler, M. Hatef, Robert P.W. Duin, and J. Matas, "On Combining Classifiers", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 3, March 1998, pp. 226-239, doi: 10.1109/34.667881.