

Research Article

Security Enrichment in Intrusion Detection System Using Classifier Ensemble

Uma R. Salunkhe¹ and Suresh N. Mali²

¹Smt. Kashibai Navale College of Engineering, Savitribai Phule Pune University, Pune, India

²Sinhgad Institute of Technology and Science, Savitribai Phule Pune University, Narhe, Pune, India

Correspondence should be addressed to Uma R. Salunkhe; umasalunkhe@yahoo.com

Received 6 January 2017; Accepted 20 February 2017; Published 12 March 2017

Academic Editor: Arun K. Sangaiah

Copyright © 2017 Uma R. Salunkhe and Suresh N. Mali. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In the era of Internet and with increasing number of people as its end users, a large number of attack categories are introduced daily. Hence, effective detection of various attacks with the help of Intrusion Detection Systems is an emerging trend in research these days. Existing studies show effectiveness of machine learning approaches in handling Intrusion Detection Systems. In this work, we aim to enhance detection rate of Intrusion Detection System by using machine learning technique. We propose a novel classifier ensemble based IDS that is constructed using hybrid approach which combines data level and feature level approach. Classifier ensembles combine the opinions of different experts and improve the intrusion detection rate. Experimental results show the improved detection rates of our system compared to reference technique.

1. Introduction

With the wide usage of Internet, Information Security is an important domain for research. Intrusion Detection System (IDS) is a major concern of security. IDS is designed to monitor the network traffic and identify the suspicious patterns representing network intrusion that may compromise the system. That is, it continuously inspects network traffic for potential vulnerabilities [1]. Whenever IDS finds security breach or any kind of compromise to the system, it generates an alert to indicate the existence of intrusion. IDS play a crucial role in enhancing security of networking environment. Based on the approaches that are used to detect the intrusions, IDS can be categorized into following groups [2].

(1) *Signature Based IDS*. IDS monitor the network and compare actual behavior with known suspicious patterns that are maintained in a database of attack signatures. Matching behavior indicates the existence of attack and generates an alert. The database does not cover any unknown or newly introduced threat whose signature is not available. If any unknown attack occurs, IDS cannot detect it as its signature does not match with those in the database. This indicates that

success of intrusion detection is limited by the availability of the recent attack signatures in the database. These systems have proved efficient for known attacks.

(2) *Anomaly Based IDS*. Signature based IDS effectively detect known attacks but are ineffective for unknown attacks. In order to overcome this limitation, anomaly based IDS compare actual behavior with the baseline that defines the normal state of the system, that is, parameters such as protocols, traffic load, and typical packet size [3]. Deviation from the baseline indicates the anomalous behavior and generates an alert. Sometimes normal behavior can be misclassified as attack due to incomplete description of normal behavior.

(3) *Hybrid IDS*. Hybrid IDS makes combined use of signature based and anomaly based ones in order to gain advantages of both [4]. That is, they try to increase detection rates of known attacks and decrease false positive rates of novel attacks.

The rest of this paper is organized as follows. Section 2 presents a review of related work. Section 3 describes the proposed Intrusion Detection System and its algorithm is discussed in Section 4. Section 5 presents the experimental setup used. Section 6 focuses on obtained results and discussions. Finally, conclusions are given in Section 7.

2. Related Work

Buczak and Guven [4] reviewed machine learning methods for intrusion detection with respect to parameters like complexity of algorithm, challenges in security enhancement, and so forth. Authors suggested different criteria such as accuracy, algorithm complexity, and time complexity to select the effective technique for intrusion detection.

Khor et al. [5] proposed a cascaded classifier approach for IDS that enhances the detection rates of the attacks which belong to the rare category. The proposed technique first separates out the rare intrusions from nonrare intrusion category so that each expert can focus on fewer categories. The method helps to diminish the effects of dominant intrusion category which has shown increased detection rates for rare intrusions. Also double filtering of network traffic improves detection rates and computational cost of the approach is less.

Abuomman and Ibne Reaz [6] presented a novel classifier ensemble approach for Intrusion Detection System in order to improve the accuracy. Authors have constructed an ensemble by using proposed PSO generated weights scheme and compared the results with that of the Weighted Majority Algorithm (WMA) approach. LUS metaoptimization of the set of generated weights has resulted in the performance improvements of IDS.

Qassim et al. [7] reviewed the set of features that is more suitable for detecting wide range of anomalies from the network traffic. Authors introduced A-IDS, an alarm classifier that can automatically analyze and categorize the anomalies monitored by a packet header based anomaly detection system. Proposed method monitors the network traffic flow, selects appropriate features, and compares traffic flows representing attack to existing data.

Govindarajan [8] introduced a new hybrid Intrusion Detection System by combining radial basis function and support vector machine. Experimentation carried out on various data sets of intrusion detection proves effectiveness of heterogeneous models compared with homogeneous models. Liu et al. [9] presented a hybrid approach SmoteAdaNL that applies resampling in order to increase number of flows in minority class and then diversified ensemble technique to improve the generalization of classifier. Weight assignment to the misclassified flows helps to improve the classification performance.

Al-Jarrah et al. [1] introduced a traffic based IDS (T-IDS) for botnet, which includes number of compromised machines known as bots, remotely controlled by a machine known as botmaster. The proposed approach makes use of a novel randomized data partitioned learning method (RDPLM) and analyzes packet header rather than packet payload to identify intrusion. Authors developed a novel feature selection technique to create a subset of features which will be helpful for correct detection of intrusions. Approach has proved to improve detection accuracy with lower computational cost and is scalable to large networks.

Hu et al. [10] proposed a distributed intrusion detection framework in which each node constructs a global detection model that combines local parametric models created using a small set of samples. Hence a node can detect attack

signatures present in other nodes, though it does not have representative samples of that attack. Li et al. [11] proposed nonnegative matrix factorization (NMF) based method for classification of networked text. Proposed algorithm puNet initially identifies clusters with the help of NMF method and then learning algorithm is trained with available labeled data.

Hu et al. [12] proposed a novel intrusion detection algorithm that has low computational complexity and high detection rate. If any false detection of attack is made, next iteration of AdaBoost focuses on it and improves the detection rate. The proposed approach also handles overfitting issue where detection of attack is not very specific and new attacks will be also detected effectively.

Yu et al. [13] presented an automatically tuning IDS (ATIDS) that can automatically tune the detection model based on the feedback about the false predictions. Whenever deployed detection model encounters novel data, it adapts to that data so that model performance is improved. Experimental results on KDDCup'99 dataset have shown 35% improvements in detecting the anomalous behavior.

Alrajeh et al. [14] discussed few existing IDS and research issues relevant to Wireless Network Security (WSN). Authors briefed different categories of IDS and choosing appropriate type of IDS for specified WSN. They suggested use of anomaly based IDS for small sized WSN due to their lightweight nature. Relatively larger WSN should prefer signature based IDS while very large WSN should choose hybrid type of IDS. Authors suggest not to prefer cross layer IDS for WSN with limited resources.

Machine learning techniques have helped in correctly identifying the intrusions in IDS which in turn helps to improve the security of IDS. Although there is much work on IDS, still some issues in this area need further attention of researchers. Skewed nature of training datasets of IDS is such an important issue that may have significant impact on the performance of IDS. The number of instances belonging to positive class is very low compared to that of negative class. The classifier that is trained on skewed data may be biased towards negative class in decision making. This has motivated us to address the imbalance between the classes in order to avoid this issue. The first concern in the proposed system is to reduce the imbalance between the classes by resampling the dataset and then apply classifier ensemble technique to improve the classification performance.

3. Proposed System

Basically, Intrusion Detection System involves analysis of network traffic collected and comparison with the baseline defined for the system that indicates the normal behavior of the system. If a mismatch is found, it indicates that someone has intruded the system.

Intrusion Detection System comprises the following elements.

(1) *Monitoring of Network Traffic.* This involves monitoring the user and system activity in order to collect network traffic data.

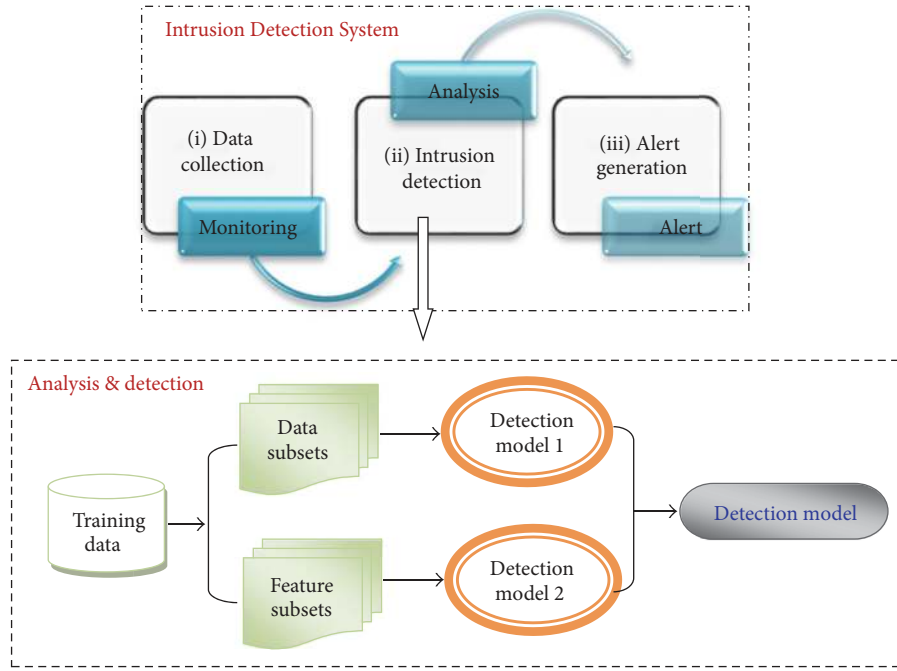


FIGURE 1: Proposed system.

(2) *Analysis and Detection.* Figure 1 represents the analysis and detection process of the proposed system.

This element incorporates generation of a prediction model for intrusion detection that can correctly detect the intrusion.

In this paper, we propose a classification-based framework for the analysis and detection of intrusions. First concern of this work is to focus on intrusions of rare category. Such category has few representative instances and hence detection model trained on such data may not be efficient in detecting the intrusions of that category. In order to avoid this, initially resampling of minority category is done. Synthetic data is introduced to such attack category. Also samples of category having relatively high number of instances are reduced. Such preprocessed data is provided as input for learning of detection models. Preprocessing also involves identification of noisy data or data with missing values.

Existing studies have shown improved rates of detection with the usage of classifier ensemble approach. Hence proposed system creates a novel classifier ensemble that combines opinions of individual experts. Two level ensembles are constructed by using two different approaches of creating the ensemble. That is, data level and feature level method is used to generate two detection models.

Detection Model 1. Data subsets D_1, D_2, \dots, D_n are created by extracting subset of original training data and are provided as input to the individual base classifier. Results of those classifiers are combined to get predicted output of ensemble named Detection Model 1.

Detection Model 2. Feature subsets S_1, S_2, \dots, S_n are created by extracting subsets of features from the original training

dataset and individual classifiers are trained with those subsets. Their results are combined to get Detection Model 2.

Outputs of Detection Model 1 and Detection Model 2 are combined to get the final prediction of whether intrusion exists or not.

(3) *Alert Generation.* If any malicious activity is detected, an alert will be generated to inform the administrator about the existence of intrusion.

The detailed algorithm is explained in Section 4.

4. Algorithm

Algorithm 1 (GenerateClassifier)

T : Original Training data set

T_1, T_2, T_3 : Training Subsets by using different datasets

S_1, S_2, S_3 : Training Subsets by using different feature sets

T' : Modified data set after Pre-processing

F : Final classifier Ensemble model

CE: Classifier Ensemble

Steps

(1) Apply pre-processing to original training data set T

$S' = \text{Over_sample}(T)$

$B' = \text{under_sample}(T)$

(2) For $i = 1$ to K do //create k models

(3) Create a new training dataset T_i by extracting different data subsets $T_i = S' \cup B'$

(4) Train and learn a base classifier using T_i

$$B_i = \text{BuildClassifier}(T_i)$$

(5) Create a new training dataset S_i by extracting different feature subsets

$$S_i = \text{Feature subset}(T')$$

(6) Train and learn a base classifier J48 using S_i

$$M_i = \text{BuildClassifier}(S_i)$$

(7) Construct first level classifier ensembles

$$E_1 = \text{CE}(B_1, B_2, B_3)$$

(8) Construct first level classifier ensembles

$$E_2 = \text{CE}(M_1, M_2, M_3)$$

(9) Final classifier is

$$F = \text{CE}(E_1, E_2)$$

5. Experimental Investigation

For experimentation, we have chosen KDDCup'99 dataset that is publicly available in UCI repository [13]. Many existing works in the area of IDS have been evaluated by using KDDCup'99 data as standard dataset. Dataset includes various intrusions simulated in a military network environment for several weeks. The dataset consists of a training dataset with 494,021 records and a test dataset with 311,029 records [6] described with 41 attributes.

Attacks in the KDDCup'99 dataset can be categorized into four main categories [4]: Remote to Local (R2L), User to Root (U2R), Probing, and Denial of Service (DOS). R2L is a type of attack in which attacker tries to gain access to network or machine [6]. In U2R attack, attacker has access to victim machine but aims to get superuser privileges. Probing is an attack in which attacker executes scanning in order to identify possible vulnerabilities in the victim system. Identified weaknesses can be used to harm the system. DOS is a kind of attack that aims to make the resources unavailable to authorized users. Usually this is achieved by flooding systems or networks with excess traffic, disrupting the connection or services. This will result in delayed or inefficient services.

In this work, we have selected subset of attacks from KDDCup'99 dataset including attacks such as the following.

(a) *Teardrop*. It involves sending fragmented IP packets that are overlapping with each other to the target machine. After receiving, target machine tries to reassemble them but cannot succeed. Windows 95 and Windows NT contain one bug related to overlapping due to which system cannot handle

TABLE 1: Datasets used in the experiment.

Attack name	Number of records
Normal	3987
Phf	3
Teardrop	50
Loadmodule	7
Smurf	43
Total	4090

overlapping packets in an effective way. As a result, system may crash or reboot.

(b) *Smurf*. It is a kind of Distributed DOS attack in which attacker spoofs the target system and broadcasts Internet Control Message Protocol (ICMP) packets with target system's IP. Most of the networked devices reply to the source IP which generates a huge traffic and floods the target system. Hence its services will not be available to authorized users.

For our experimentation, we have chosen subset of the KDDCup'99 dataset. The details of the dataset used in our experimentation are shown in Table 1.

Evaluation of the system performance is done by using detection rate as an evaluation measure. Accuracy is a measure that represents fraction of intrusions that are correctly identified.

6. Results and Discussion

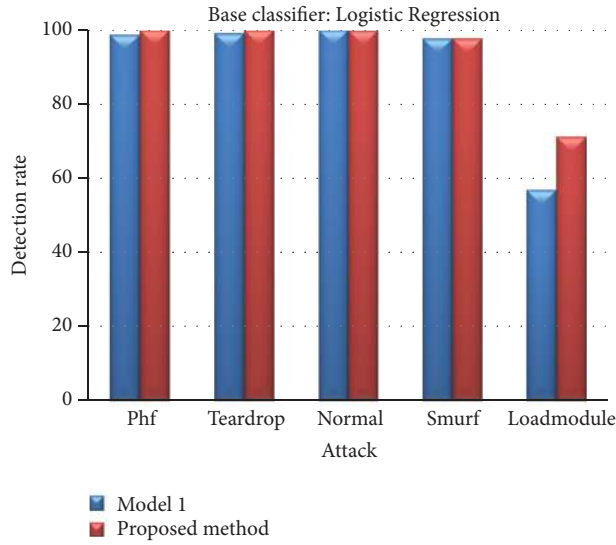
Performance of proposed system is compared with existing multiclass classifier ensemble. Experimentation is carried out for different individual classifiers, namely, Logistic Regression, J48, and Naive Bayes. Table 2 summarizes the detection rates of proposed and other reference techniques.

Figure 2 depicts performance evaluation of proposed method in terms of detection rate. Though the performance improvement seems smaller, correct identification of intrusion is extremely important and proves beneficial.

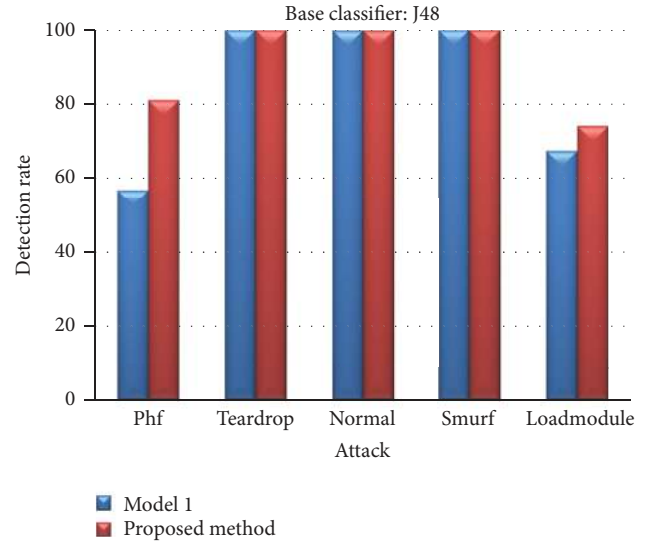
Analysis of the graphs presented in Figure 2 clearly shows improved accuracy of detecting intrusions with the use of proposed method. The major aim of the experimentation was to investigate the effect on detection rates of the proposed IDS by selecting different individual classifiers as base classifiers of ensemble. This has helped to derive some conclusions about the suitable classifiers for IDS. Analysis of the results leads to some findings that can help in choosing the appropriate base classifier to be used for ensemble designed for Intrusion Detection System. Three classifiers, namely, J48, Logistic Regression, and Naive Bayes, were tested as base classifiers of proposed ensemble technique. Logistic Regression has proved more beneficial as a base classifier in detecting the intrusions. Usage of preprocessing helps to detect the attacks of rare category correctly and improves the performance of classifier. But it has overhead as it requires more time for the learning phase of model. Overall, the proposed method improves performance of IDS by using a simpler design and easier approach.

TABLE 2: Performance evaluation using detection rate (%).

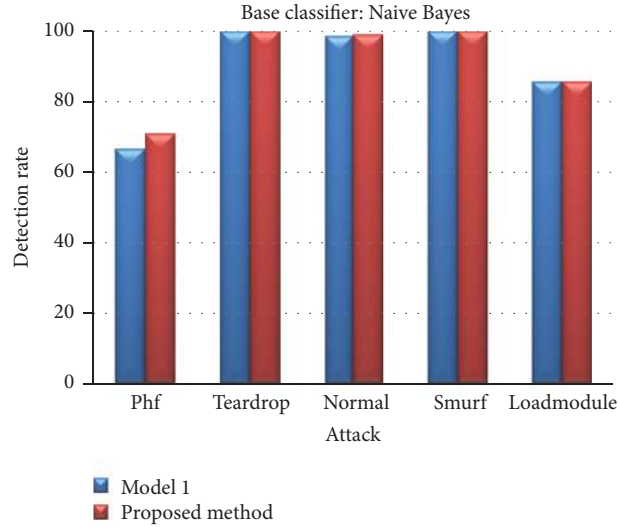
Base classifier	Logistic Regression		J48		Naive Bayes	
Attack	Model 1	Proposed method	Model 1	Proposed method	Model 1	Proposed method
Phf	98.73	100	57	81.3	66.7	71
Teardrop	99.11	100	100	100	100	100
Normal	100	99.9	99.9	99.9	98.6	99
Smurf	97.7	97.7	100	100	100	100
Loadmodule	57.1	71.4	67.4	74.2	85.7	85.7



(a) Detection rate with Logistic Regression as base classifier



(b) Detection rate with J48 as base classifier



(c) Detection rate with Naive Bayes as base classifier

FIGURE 2: Performance evaluation.

7. Conclusion

In this work, we proposed a novel classifier ensemble method for intrusion detection that is diversified by using two different approaches. That is, it uses different feature sets and training sets both. The methodology also makes use of resampling technique that emphasizes the attack of rare category. The

comparison of proposed approach with reference techniques shows significant improvement in detecting the intrusions correctly. The procedure can be further extended to adjust the ensemble size dynamically according to the size of dataset. That is, decision of number of base classifiers to be used for constructing ensemble should be done dynamically. If the size is decided statistically, it may not prove effective for

different dataset sizes with varying imbalance ratios. Hence adaptively changing the size by analyzing these factors will help to improve performance with relatively less overhead. Also performance of the approach can be tested for more number of attack categories.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

- [1] O. Y. Al-Jarrah, O. Alhussein, P. D. Yoo, S. Muhaidat, K. Taha, and K. Kim, "Data randomization and cluster-based partitioning for botnet intrusion detection," *IEEE Transactions on Cybernetics*, vol. 46, no. 8, pp. 1796–1806, 2016.
- [2] K. Kumar and S. Singh, "Intrusion Detection Using Soft Computing Techniques," 2016.
- [3] S. Rajasegarar, C. Leckie, J. C. Bezdek, and M. Palaniswami, "Centered hyperspherical and hyperellipsoidal one-class support vector machines for anomaly detection in sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 518–533, 2010.
- [4] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.
- [5] K.-C. Khor, C.-Y. Ting, and S. Phon-Amnuaisuk, "A cascaded classifier approach for improving detection rates on rare attack categories in network intrusion detection," *Applied Intelligence*, vol. 36, no. 2, pp. 320–329, 2012.
- [6] A. A. Aburomman and M. B. Ibne Reaz, "A novel SVM-kNN-PSO ensemble method for intrusion detection system," *Applied Soft Computing Journal*, vol. 38, pp. 360–372, 2016.
- [7] Q. S. Qassim, A. M. Zin, and M. J. Ab Aziz, "Anomalies classification approach for network—based intrusion detection system," *International Journal of Network Security*, pp. 1159–1171, 2016.
- [8] M. Govindarajan, "Evaluation of ensemble classifiers for intrusion detection," *World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering*, vol. 10, no. 6, pp. 876–884, 2016.
- [9] Z. Liu, R. Wang, and M. Tao, "SmoteAdaNL: a learning method for network traffic classification," *Journal of Ambient Intelligence and Humanized Computing*, vol. 7, no. 1, pp. 121–130, 2016.
- [10] W. Hu, J. Gao, Y. Wang, O. Wu, and S. Maybank, "Online adaboost-based parameterized methods for dynamic distributed network intrusion detection," *IEEE Transactions on Cybernetics*, vol. 44, no. 1, pp. 66–82, 2014.
- [11] M. Li, S. Pan, Y. Zhang, and X. Cai, "Classifying networked text data with positive and unlabeled examples," *Pattern Recognition Letters*, vol. 77, pp. 1–7, 2016.
- [12] W. Hu, W. Hu, and S. Maybank, "AdaBoost-based algorithm for network intrusion detection," *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, vol. 38, no. 2, pp. 577–583, 2008.
- [13] Z. Yu, J. J. P. Tsai, and T. Weigert, "An automatically tuning intrusion detection system," *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, vol. 37, no. 2, pp. 373–384, 2007.
- [14] N. A. Alrajeh, S. Khan, and B. Shams, "Intrusion detection systems in wireless sensor networks: a review," *International Journal of Distributed Sensor Networks*, vol. 9, no. 5, Article ID 167575, 2013.

