Introduction

An Intrusion Detection System (IDS) monitors the network bustle through incoming and outgoing data to access the conduct of data usage thereby identifying any apprehensive activity and alerting with a sign of intrusion. There are two types of intrusion detection techniques known as misuse and anomaly detection. Misuse detection is possible only for those attacks whose prior knowledge is present in the dataset used for training the model. The challenge is to develop an efficient model for real-time intrusion detection which can be modeled for online data. Anomaly detection also called profile-based detection approach is one such technique that adapts to the normal behavior of the user/network and applies statistical measures to events or activities to decide whether the encountered event is normal or not. Though there are a number of measures available to analyze the performance of IDS but the focus of this study is only on two key performance metrics known as the Detection rate (DR) and False Alarm Rate (FAR). The efficiency of IDS can be talked about in terms of these two metrics which can be depicted in the form of Receiver Operating Characteristics (ROC) curve. Though this measure does not provide exactly the best operating point for IDS but does help in deciding comparatively, a better operating point.

The ultimate aim in the development of IDS is to achieve best accuracy. The two basic techniques used in intrusion detection have their own advantages and disadvantages. The misuse detection can very well detect known attacks with lower FAR but fail to identify novel attacks whereas the strength of anomaly detection technique is...
the ability to detect unknown attacks but suffers from the drawback of high FAR\(^7,8\).

The dataset popularly used for the study of IDS is KDD’99\(^9\) dataset which was earlier released by DARPA\(^10\). Though this dataset is quite old but still provides a benchmark for the research in the area of IDS. It was observed through research that the DARPA and KDD’99 data had redundancy which resulted in biased outcomes of the classifiers used for intrusion detection\(^11,12\). The NSL-KDD\(^13\) dataset overcomes the inherent problem\(^14\) of KDD’99 dataset producing reasonable results, even though the overall accuracy of the system has gone down. In this research paper, NSL-KDD dataset is used for study which is a new version of KDD’99 dataset although it still suffers from some of the problems due to the characteristics of synthetic data\(^15\).

Machine learning algorithms are quite suitable for IDS\(^16\) because they develop a model based on the input data through learning and then this model is used for prediction on test data\(^17\). In other words, machine learning algorithms develop intelligence and use it for prediction rather than being programmed. The machine learning algorithms can be put in various categories based on the inherent methodology employed like rule based, tree based, instance based, neural network based, bayesian network based, and the support vector machines\(^18\). There are many variants of tree based algorithms available like random tree, random forest and J48 algorithm\(^19,20\) outperforming support vector machines and neural network approaches to intrusion detection\(^21\).

In this practical study, NSL-KDD\(^13\) dataset is used. Subset of NSL KDD Cup dataset is used with hybrid classifiers thereby proposing a new Intrusion Detection System\(^22\).

This dataset has 42 attributes out of which 41 are classified under one of the following labels: Basic, Content, Traffic, or Host\(^12,23\). The details of categorization of 41 attributes with four labels are specified in Table 1. The selected dataset has many possible arrangements such that the records may be classified in binary classes as normal/anomalous or in five classes as normal, Denial of Service (DoS) attack, User to Root (U2R) attack, Remote to Local (R2L) attack and Probe attack\(^12\).

The objective of this research is to study and interpret the role of 41 attributes of KDD dataset with respect to four specified labels as in Table 1 on DR and FAR for IDS. The focus is not to analyze the contribution of each of the 41 attributes individually for feature selection purpose but study the cumulative effect as per the four labels. Though, the results of this study can be used for better feature selection at a later stage. The goal of any efficient IDS is to achieve maximum DR with minimum FAR\(^24\). This paper aspires to deduce which categories of the four labeled attributes contribute significantly in achieving high DR and low FAR. The conclusions drawn from this empirical study can help overcome the limitation of training data which in the case of anomaly tries to over protect the network from intrusions thereby increasing the FAR. Hence the audit data used in anomaly detection to detect novel attacks can be enhanced so that FAR is negligible.

### 2. Experimental Setup

The experimental setup presents the dataset employed for the study, the tool used for simulation and the research methodology applied to conduct the test thus generating the results. This section is divided into four subsections.

Weka 3.7.11\(^17,25\) is used for preprocessing and simulation of KDD dataset on the chosen classification algorithms. The KDD data files for training and testing are preprocessed in Weka.

#### 2.1 Data Base

The KDD dataset\(^13\) is selected for this empirical study whose attributes are labeled in four classes as discussed in the introduction section. This study considers the binary classification dataset whose details are listed in Table 2. Table 3 presents the class wise detail of all 42 attributes of KDD dataset.

#### 2.2 Proposed Work

A systematic approach is used to make fifteen possible configurations of KDD dataset based on the four labels given to attributes. The total number of attribute labels is four (N=4) hence sixteen different combinations are possible (2\(^N\)). The NULL combination comprising of nil label

| Attribute Class | Abbreviation | Attributes |
|-----------------|--------------|------------|
| Basic           | B            | 1-9        |
| Content         | C            | 10-22      |
| Traffic         | T            | 23-31      |
| Host            | H            | 32-41      |

| Attribute Class | Abbreviation | Attributes |
|-----------------|--------------|------------|
| Basic           | B            | 1-9        |
| Content         | C            | 10-22      |
| Traffic         | T            | 23-31      |
| Host            | H            | 32-41      |
Table 2. Data instances of NSL-KDD dataset

| Dataset                          | Normal Class Instances | Anomalous Class Instances | Total  |
|---------------------------------|------------------------|---------------------------|--------|
| KDDTrain+20Percent (Training Data) | 13449                  | 11743                     | 25192  |
| KDDTest+ (Test Data)            | 9711                   | 12833                     | 22544  |

with zero attributes is excluded. Hence, there are fifteen combinations possible to form different configurations of dataset \(2^N-1\).

The dataset which includes training as well as the test files is preprocessed individually to develop fifteen configurations as per Table 4. Out of the total 41 attributes (excluding class attribute), the attributes not required for one of the fifteen selected configuration are removed from training and test data file. The last attribute ‘Class’ which remains integral in all the fifteen configurations describes whether the instance is a normal record or an anomalous one. The preprocessing and simulation of data on the selected classifiers is done in Weka tool\(^{17}\). These fifteen dataset configurations are simulated for three classification algorithms, Random Forest, OneR and Naïve Bayes.

2.3 Classifiers used

Three classifiers are selected for this empirical study from three different classes of algorithms to validate that the results are not biased towards one particular class of algorithms. Random Forest is a tree based ensemble algorithm\(^{17}\) which constructs random forests by bagging ensembles of random trees whereas the tree generated using random tree test all the random features at each node without pruning. Rule based algorithm OneR generates a one-level decision tree expressed in the form of a set of rules that all test one particular attribute which is considered for its decision and selects the one that works best\(^{17}\). Naïve Bayes is a standard probabilistic classifier which assumes that the attributes are independent and works well when combined with some attribute selection measures\(^{17}\).

![Table 3. Classwise detail of KDD dataset attributes](image)
Table 4. Combinations of attributes with maximum four labels for KDD dataset

| Sr. No. | Attribute class Combinations | # Attributes | B | C | T | H |
|---------|-----------------------------|--------------|---|---|---|---|
| 1       | BCTH                        | 41           | √ | √ | √ | √ |
| 2       | BCT                         | 31           | √ | √ | x |   |
| 3       | BCH                         | 32           | √ | x |   | √ |
| 4       | BTH                         | 28           | x |   | √ | √ |
| 5       | CTH                         | 32           | x | √ | √ |   |
| 6       | BC                          | 22           | x |   | x | x |
| 7       | BT                          | 18           | √ | x | x |   |
| 8       | BH                          | 19           | x |   | x | x |
| 9       | CT                          | 22           | x |   | √ | x |
| 10      | CH                          | 23           | x |   | x | √ |
| 11      | TH                          | 19           | x | x | x |   |
| 12      | B                           | 9            | √ | x | X | X |
| 13      | C                           | 13           | x |   | X | X |
| 14      | T                           | 9            | x | x | x |   |
| 15      | H                           | 10           | x | x | X |   |

Table 5. Confusion matrix for IDS

| Confusion Matrix | Predicted Instances |
|------------------|---------------------|
|                  | Normal | Anomalous |
| Actual Instances | TN    | FP        |
|                  | FN    | TP        |

2.4 Evaluation Metrics

The evaluation metrics help assess the performance of an IDS. Some of the evaluation metrics majorly used in measuring the efficiency of IDS are accuracy, DR, FAR, precision and F-score\(^24\). All these metrics are derived from the four basic result elements of any classification algorithm presented in the form of confusion matrix which illustrates the actual instance classes versus predicted classification result. As shown in Table 5, the elements are True Negative (TN), False Negative (FN), False Positive (FP) and True Positive (TP).

Accuracy is defined as the ratio of total true predicted instances to the total number of instances in the dataset. DR is the ratio of correctly predicted attacks to the total number of actual attacks. FAR for intrusions is the rate at which normal instances are classified as anomalous. Precision is defined as the ratio of correctly predicted attacks to the total number of predicted attacks. The F-score can be defined as the harmonic mean of DR and the precision value. A good IDS tries to achieve maximum possible accuracy, F-score and DR with minimum FAR.

3. Simulation Result and Analysis

The simulation results from the confusion matrix for fifteen configurations of dataset are shown in Table 6 for Naive Bayes, Random Tree and OneR algorithms. The result comprises of the TP, TN, FP and FN values for each of the fifteen combinations with respect to the three selected classifiers.

The summary of results is presented in Table 7 which is generated from Table 6. The key metrics used in the study are DR and FAR. The classification results in the form of DR and FAR for all the fifteen cases of attribute class’s combinations are presented for Random Forest, OneR and Naïve Bayes classifiers in Table 7.

In this paper, the results are analyzed with respect to DR and FAR individually, which emphasizes on one attribute, two attribute and three attribute class combinations of attributes for all the three classification algorithms under study. The conclusions are drawn only for those highlighted points on the plots where each of the three classification algorithm shows significant conduct. Hence, algorithms from different class of machine learning are considered to ensure that there is no biasing in the results.

Figures 1 to Figure 3 presents the plot of three classification algorithms for one, two and three labeled attribute combinations respectively. Considering the analysis of DR, Figure 1 depicts the plot of DR with respect to single class of attributes. The green marked arrow highlights the high DR for all the three classifiers for content labeled attributes and red marked arrow highlights the low DR for traffic labeled attributes. Hence it can be concluded from Figure 1 that the content class attributes have significant contribution towards achieving high DR whereas the traffic class attributes deteriorate the same.

In Figure 2, red arrow highlights the combination of basic and host (BH) labeled attributes which reflects lower DR as compared to BT label for all the three classifiers. Hence, attributes of host label show poor performance for DR as compared to traffic labeled attributes.

Similarly, Figure 3 shows the plot of all three labeled classes in comparison to the original set of four labeled attributes. The green arrow highlights the BCT label showing DR nearly equal to the BCTH labeled attributes. The
Table 6. Result set for Naive Bayes, Random Forest and OneR algorithms

| Sr. No. | Attribute Class Combination | Naïve Bayes | Random Forest | OneR |
|---------|---------------------------|-------------|---------------|------|
|         |                           | TN  | FN  | FP  | TP  | TN  | FN  | FP  | TP  | TN  | FN  | FP  | TP  |
| 1       | BCTH                      |     |     |     |     | 9446| 4067| 265 | 8766| 9300| 3652| 411 | 9181|
| 2       | BCT                       |     |     |     |     | 8975| 3616| 736 | 9217| 9300| 3652| 411 | 9181|
| 3       | BCH                       |     |     |     |     | 9218| 4039| 493 | 8794| 9300| 3652| 411 | 9181|
| 4       | BTH                       |     |     |     |     | 9168| 4297| 543 | 8536| 9300| 3652| 411 | 9181|
| 5       | CTH                       | 8997| 4546| 714 | 282 | 9043| 5267| 668 | 7566| 9544| 7187| 167 | 5646|
| 6       | BC                        | 9563| 6250| 148 | 86  | 8890| 3588| 821 | 9245| 9300| 3652| 411 | 9181|
| 7       | BT                        | 9020| 4502| 691 | 833 | 8890| 3588| 821 | 9245| 9300| 3652| 411 | 9181|
| 8       | BH                        | 9375| 4929| 336 | 790 | 9434| 4079| 277 | 8754| 9300| 3652| 411 | 9181|
| 9       | CT                        | 8915| 4386| 796 | 844 | 8973| 5125| 738 | 7708| 9544| 7187| 167 | 5646|
| 10      | CH                        | 9325| 4683| 386 | 815 | 9001| 5569| 710 | 7264| 9083| 5878| 628 | 6955|
| 11      | TH                        | 9008| 4574| 703 | 825 | 9026| 5342| 685 | 7491| 9544| 7187| 167 | 5646|
| 12      | B                         | 9625| 9365| 86  | 346 | 8848| 2608| 863 | 10225| 9300| 3652| 411 | 9181|
| 13      | C                         | 7350| 2619| 236 | 10214| 7349| 2743| 236 | 10090| 7350| 2619| 2361| 10214|
| 14      | T                         | 8962| 4111| 749 | 842 | 9081| 5627| 630 | 7206| 9544| 7187| 167 | 5646|
| 15      | H                         | 9340| 4738| 371 | 809 | 8982| 5475| 729 | 7358| 9083| 628 | 5878| 6955|

Table 7. Summary of results for Random Forest, OneR and Naive Bayes algorithm

| Sr. No. | Attribute Class Combination | Detection Rate (%) | False Alarm Rate (%) | False Alarm Rate (%) |
|---------|-----------------------------|--------------------|----------------------|----------------------|
|         |                             | Random Forest      | OneR                 | Naive Bayes          |
|         |                             |                    |                      |                      |
| 1       | BCTH                        | 68.31              | 71.54                | 64.30                |
| 2       | BCT                         | 71.82              | 71.54                | 66.07                |
| 3       | BCH                         | 68.53              | 71.54                | 62.12                |
| 4       | BTH                         | 66.52              | 71.54                | 63.98                |
| 5       | CTH                         | 58.96              | 44.00                | 64.58                |
| 6       | BC                          | 75.28              | 71.54                | 51.30                |
| 7       | BT                          | 72.04              | 71.54                | 64.92                |
| 8       | BH                          | 68.21              | 71.54                | 61.59                |
| 9       | CT                          | 60.66              | 44.00                | 65.82                |
| 10      | CH                          | 56.60              | 54.20                | 63.51                |
| 11      | TH                          | 58.37              | 44.00                | 64.36                |
| 12      | B                           | 79.68              | 71.54                | 27.02                |
| 13      | C                           | 78.63              | 79.59                | 79.59                |
| 14      | T                           | 56.15              | 44.00                | 65.63                |
| 15      | H                           | 57.34              | 91.72                | 63.08                |
Contribution of Four Class Labeled Attributes of KDD Dataset on Detection and False Alarm Rate for Intrusion Detection System

Considering FAR for the three classifiers, Figure 4 to Figure 6 are plotted with respect to one, two and three class attributes respectively. Figure 4 shows FAR for the three classifiers with respect to single class of attributes. The green arrow highlights that the FAR is minimum for basic attributes for all the three classifiers whereas the red arrow highlights the contribution of content labeled attributes towards higher FAR. Also, it can be observed that FAR is on the lower side for traffic labeled attributes as compared to content labeled attributes.

The arrow in Figure 5 highlights the BH labeled attributes presenting better FAR as compared to BT class of attributes for two of the three classifiers whereas the third classifier OneR shows constant value. Similarly, arrow in Figure 6 emphasizes on BCT labeled attributes which indicates absence of host attributes showing comparatively high FAR for the three classifiers hence it

**Figure 1.** Detection rate distribution considering single attribute class for Random Forest, OneR and Naïve Bayes.

**Figure 2.** Detection rate distribution considering two attribute classes for Random Forest, OneR and Naïve Bayes.

**Figure 3.** Detection rate distribution considering three attribute classes for Random Forest, OneR and Naïve Bayes.

red arrow highlights the CTH label depicting the absence of basic attributes and it can be observed that DR significantly falls for all the three classification algorithms.

**Figure 4.** False alarm rate distribution considering single attribute class for Random Forest, OneR and Naïve Bayes.

**Figure 5.** False alarm rate distribution considering two attribute classes for Random Forest, OneR and Naïve Bayes.

**Figure 6.** False alarm rate distribution considering three attribute classes for Random Forest, OneR and Naïve Bayes.
can be concluded that the host attributes have positive contribution in trimming down FAR.

4. Discussion

In this section, the results are discussed highlighting the key observations. The three classification algorithms under study are intentionally selected from different class of machine learning algorithms to make sure that the outcome of simulation is independent of a particular classifier.

It is observed from the analysis of results that the outcome of BC (22 attributes) labeled dataset is on the moderate side whereas BTH and CTH configurations show poor result in comparison to BCTH data configuration. Another observation of prime concern is the contribution of BH (19 attributes) labeled attributes is almost equivalent to the contribution of BCTH (41 attributes) labeled dataset configuration. Hence, it can be deduced that the BH labeled attributes give computationally similar results as compared to BCTH label with low cost as the number of attributes has reduced significantly.

Table 8 concludes the studied behavior of DR and FAR with respect to the class-wise distribution of attributes for KDD dataset. It is observed that the Basic label attributes contribute maximum in achieving highest DR whereas the contribution of Host attributes is least. Similarly, the contribution of Basic label attributes is highest in achieving minimum FAR whereas the content label attributes has the least significant role in reducing FAR. Therefore, the four classes of attributes are ranked for high DR and low FAR separately with rank ‘1’ depicting the maximum dominance. Hence, Table 8 summarizes the class wise contribution of 41 attributes in accomplishing high DR and low FAR which can help recognize significant attributes with respect to these four labels. The results of this study can be further used for feature selection purpose indicating that instead of trying all $2^{41}$ combinations, feature selection can be applied on selective labels. It can be inferred from Table 8 that the base labeled attributes need minimum feature reduction whereas traffic class attributes need maximum feature reduction followed by content and host classes.

5. Conclusion

In this pragmatic study KDD dataset was used to examine the behavior of detection rate and false alarm rate metrics for an Intrusion Detection System (IDS). The 41 attributes of the KDD dataset were classified under Basic, Content, Traffic and Host labels. This paper explored the contribution of KDD dataset attributes with respect to these four labels in improving the value of detection and false alarm rate. The study was done on Random Forest, OneR and Naïve Bayes classification algorithms. A significant contribution of basic class attributes was observed for IDS with remarkable observations with respect to attributes of other labels. Finally the four attribute labels were ranked for their dominance in enhancing the detection and reducing the false alarm rate. This study can help improve the dataset by reducing the predisposition of results towards attributes of a particular label resulting in high false alarm rate and hence enhance the dataset to attain efficient IDS for anomaly detection. The results of this study can be used for selective feature selection on particular labeled attributes rather than on all the individual attributes.
6. References

1. Han J, Kamber M. Data Mining: Concepts and Techniques. Morgan Kaufmann: San Francisco, 2006.
2. Zhang Z, Shen H. Application of online-training SVMs for real-time intrusion detection with different considerations. Computer Communications. 2005; 28(12):1428–42.
3. Shyu ML, Chen S, Sarinnapakorn K, Chang L. A novel anomaly detection scheme based on principal component classifier. Proceedings of the IEEE Foundations and New Directions of Data Mining Workshop, in conjunction with the Third IEEE International Conference on Data Mining (ICDM03), 2003. p. 172–79.
4. Denning DE. An Intrusion-Detection Model', IEEE Transactions on Software Engineering. 2006; SE-13(2):222–32.
5. Lee W, Stolfo SJ. A framework for constructing features and models for intrusion detection systems. ACM Transactions on Information and System Security. 2000; 3(4):227–61.
6. Landgrebe TCW, Pavel P, Duin RPW, Bradley AP. Precision-Recall Operating characteristic (PROC) curves in imprecise environments. Proceedings of 18th International Conference on Pattern Recognition, ICPR2006, Hong Kong. 2006; 4. p.123–27.
7. Wang W, Guan XH, Zhong X. Processing of massive audit data streams for real time anomaly intrusion detection. Computer communications. 2008; 31(1):58–72.
8. Garcia-Teodoro P, Diaz-Verdejo J, Macia-Fernandez G, Vazquez E. Anomaly-based network intrusion detection: techniques, systems and challenges. Computer Security. 2009; 28(1-2):18–28.
9. KDD Cup 1999. [Online]. 2014 Nov. Available from: http://kdd.ics.uci.edu/databases/kddcup99/
10. MIT Lincoln Labs. DARPA intrusion detection evaluation [Online]. 2014 Nov. Available from: http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/index.html
11. Lippmann RP, Fried DJ, Graf I, Haines JW. Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation. Proceedings of the 2000 DARPA Information Survivability Conference and Exposition (DISCEX’00), Hilton Head, SC. 2000; 2. p. 12–26.
12. Tavallae M, Bagheri E, Lu W, Ghorbani AA. A Detailed analysis of the KDD CUP 99 Dataset. Proceedings of the IEEE Symposium on Computational Intelligence in Security and Defense Applications. 2009; 1–6.
13. Nsl-kdd dataset for network-based intrusion detection systems. 2014 Nov. Available from: http://nsl.cs.unb.ca/NSL-KDD/
14. Revathi S, Malathi A. A detailed analysis of KDD cup99 Dataset for IDS. International Journal of Engineering Research and Technology (IJERT). 2013; 2(12):1848–53.
15. McHugh J. Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory. ACM Transactions on Information and System Security. 2000; 3(4):262–94.
16. Tsai C-F, Hsu Y-F, Lin C-Y, Lin W-Y. Intrusion detection by machine learning: A Review. Expert Systems with Applications. 2009; 36(10):1994–2000.
17. Witten IH, Frank E, Hall MA. Data Mining- Practical Machine Learning Tools and Techniques. Morgan Kaufmann: San Francisco, CA, 2011.
18. Wu X, Kumar V, Quinlan JR, Ghosh J, Yang Q, Motoda H, McLachlan GJ, Ng A, Liu B, Yu PS, Zhou Z, Steinbach M, Hand DJ, Steinberg D. Top Ten Data Mining Algorithms. Knowledge and Information Systems Journal, Springer-Verlag London. 2007; 14(1):1–37.
19. Gaffney JE, Ulvila JW. Evaluation of intrusion detectors: A decision theory approach. Proceedings of the IEEE symposium on Security and Privacy, S&P’01, Oakland, CA, USA. 2001; 50–61.
20. Apte C, Weiss S. Data mining with decision trees and decision rules. Future Generation Computer Systems. 1997; 13(2-3):197–210.
21. AbdJalil K, Kamarudin MH, Masrek MN. Comparison of Machine Learning algorithms performance in detecting network intrusion. 2010 International Conference on Networking and Information Technology (ICNIT), Manila, IEEE. 2010. p. 221–26.
22. Azad C, Jha VK. Data Mining Based Hybrid Intrusion Detection System. Indian Journal of Science and Technology. 2014 Jun; 7(6).
23. Elkan C. Results of the KDD’99 classifier learning. SIGKDD Explorating. 2000; 63–4.
24. Gu G, Fogla P, Dagon D, Lee W. An Information-Theoretic Measure of Intrusion Detection Capability. Proceedings of the ACM Symposium on Information, Computer and Communications Security. 2006; 90–101.
25. Waikato environment for knowledge analysis (weka) version 3.7.11. 2014 November. Available from: http://www.cs.waikato.ac.nz/ml/weka/