Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 3159-0040
Vol. 2 Issue 6, June - 2015

# Modeling Intrusion Detection Systems With Machine Learning And Selected Attributes

**Thaksen J. Parvat**
USET
G.G.S.Indratrastha University
Dwarka, New Delhi –78
pthaksen.sit@sinhgad.edu

**Pravin Chandra**
USICT
G.G.S.Indratrastha University
Dwarka, New Delhi –78
chandra.pravin@gmail.com

***Abstract*—Intrusion Detection System (IDS) has become a vital component in ensuring the safety of today's network. In this review, we does experimentation on NSL KDD Cup -20% dataset with selected attribute to improve the performance. The time complexity is improved by reducing false alarm rate with Machine Learning (ML) algorithms. This improve the detection rate for DoS, Probe, U2R and R2L attacks. In this paper, we use the Bayes Net, Naive Bayes, Random Tree, PART, C4.5, and Attribute Selected Classifier as a Machine Learning algorithm. By comparison with algorithms with all attribute and the proposed attributes performs higher predictive accuracy, faster result generalization. In the intrusion detection, the accuracy and the time complexity is important, and, in this paper we improved both. It results in significant precision and F-measure along with remarkable time complexity.**

***Keywords—Intrusion Detection, Machine Learning, KDD_99 dataset, Data Classification***

## I. INTRODUCTION

Today's computer systems need to be designed to prevent illegal access from the outdoors intruders. An unauthorized mechanism designed to access system resources and data is called intrusion and designers are called intruders. There are two types of Intruders or malicious activities. Internal Intruders attempt to elevate their limited privileges by abusing it. Outside Intruders attempt to gain unauthorized access to system resources from the public network [1].

The vital role of Intrusion Detection Systems (IDSs) is to detect anomalies or malicious activities and attacks in the network and for a single host only. Intrusion detection algorithms are classified into two methods: misuse detection and anomaly detection. Signature based algorithm attacks based on the known attack signatures database[13]. They are effective in detecting known attacks with low errors. However, they cannot detect unknown attacks that do not have similar properties to the known attacks. Anomaly detection classifiers analyze normal traffic and profile normal traffic patterns. The anomaly detection method was based on the hypothesis that the attacker behavior differs to that of a normal user. They classify traffic as a malicious if the characteristics of the traffic are far from those of normal attacks patterns. Anomaly detection classifiers can be useful for the new malicious code. They are not as effective as misuse detection models in the detection rate for known attacks and false positive (FP) rates, which is a ratio of misclassified normal traffic [2].

To resolve the disadvantages of these two intrusion detection methods, hybrid intrusion detection methods (HIDS) that combine the signature based detection method and the anomaly detection method have also been proposed [11]. Because none of the signature and anomaly detection methods was better than any other, an HIDS uses both the misuse detection system and anomaly detection system. The detection performance of the HIDS depends on the combination of these two different detection methods. Most hybrid IDS detection systems independently train a signature detection model and an anomaly detection model, and then simply aggregate all results of the detection models. In this case, the detection rate will be improved but the IDS will still have a high false positive(FP) rate. If the hybrid method regards an incoming traffic connection as an attack only if both models classify the incoming connection as an attack, false alarms will be reduced, but it may overlook many attack links [1][2].

Whenever an attack is detected, IDS raises an alarm to the system administrator. The alarm contains the information describing what malicious code is detected, who are the target and victims of the attack. The content associated with intrusion detection system alarms varies to a great extent depending on the nature of data and also on the type of intrusion detection system mechanism (signature or anomaly). Signature-based intrusion detection system generates rich information along with alarm whereas anomaly intrusion detection system may just identify the connection stream that detected as an attack. The major concern with these systems is that they attempt to detect suspected events that result in high false alarm rate. The maximum problem of false alarms by Snort even in the Defense Advanced Research Projects Agency (DARPA-99) dataset [11], which generated in a controlled environment. The reason attributed to this alarming number of wrong detection is because many intrusion detection system detect too many suspicious cases. In a sense, detected events are not necessarily intrusions to the system. An

intrusion detection system with improper ruleset may miss some genuine intrusions. In the IDS literature, these cases are termed as false alarms. False positives and false negatives indicate whether detection is spurious or a failure respectively [6].

**In this paper some standard terms are used as follows.**

- **Attacks:** Any malicious code that attempt to exploit a vulnerability, which may or may not be successful.
- **False Alarms**: Set of false positives.
- **False positive (FP):** False positive is produced when IDS raises an alarm for an unsuccessful attack attempt.

**There are various reasons for false alarm generation in IDS, and major of them listed below [6].**

- Intrusion activity does subtle deviation, close to normal, and in some cases is difficult to differentiate.
- Certain actions that are normal may be malicious under different prevailing circumstances. For example, network scan is normal if done by a security administrator otherwise it is abnormal.
- Many IDS detect not only attacks but also the number of attempts of attacks [11].
- An alarm may say that a stage in a multi-stage attack that may eventually fail due to various other reasons.

## II. Background and Literature Review

There are two types of classifiers/algorithms that can be applied to an Intrusion Detection System (IDS) [4]. First is Host-based Intrusion Detection System (HIDS) and second is Network-based Intrusion Detection System (NIDS). Host-based systems are used to protect a single host or single system, and to prevent them from malicious activates from threats and vulnerabilities. Network-based Intrusion Detection System (NIDS), this type of IDS provide protection by observing network traffic in an attempt to malicious activates [2].

IDS can be further differentiated into anomaly-based and signature-based. An Anomaly-based IDS detects the malicious activities in the host systems, and computer network. The deviation or the unauthorized access from the normal behavior is measured as an attack or disturb that particular system. In an anomaly based IDS detect attacks or malicious activities by comparing the new traffic with the already existing database. Signature based detection system matches the signatures of already known malicious activities that are stored in Database to detect the malicious activities in the host system [12].

The intrusion detection evaluation of any problem, and with its solution usually affects the choice of the suitable IDS for a particular environment depending on different factors. The false alarm rate (FAR), and the detection rate is considered from the four instances in the intrusion detection system i.e. False Positive (FP), False Negative (FN), True Positive (TP), and True Negative (TN). The tradeoff between these two factors (false alarm rate and the detection rate) analyzed with the help of the one curve i.e. Receiver Operating Characteristic (ROC) curve [3][14].

| | | Predicted | | Total |
|---|---|---|---|---|
| | | Normal | Attacks | |
| Actual | Normal | TN | FP | TN+FP |
| | Attacks | FN | TP | TP+FN |
| Total | | TN+FN | TP+FP | |

Table No. 1 IDS Confusion Matrix

There are four classes True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN) are count as predicted and actual classes. They are merged into in the 2x2 confusion matrix as shown in Table 1. Show that there are two columns of “Normal” and “Attack”. Here True Positive (TP) means a legitimate attack or malicious activities that trigger IDS to produce an alarm. True Negative (TN) An event when no attack detected. False Positive (FP) an IDS to produce an alarm when no attack has taken place. False Negative (FN) there is no alarm raised when an attack has occurred. In the machine learning algorithms, there is low false alarm rate as compared to the other IDS systems [5][11].

## III. KDD 99 Dataset Description

The KDD cup-99 dataset has many controversies, but it is the benchmark in this domain. It is widely used till 1999 for the detection of the abnormal behavioral in the network or a single host. In this experiment, we use the KDD 99 with 20% dataset in that there are approximately 25192 records in the 41 attributed dataset. For each connection, there are 41 attributes to specify the particular packet is normal or abnormal.

In this dataset, the simulated attacks fall in one of the following four types of categories:

**Denial of Service (DoS):** Using some services attacker tries to prevent ligaments users

**Remote to Local (R2L):** On the victim machine there is no attacker's account but tries to access that system.

**User to Root (U2R):** On the victim machine there is attackers account but tries to access that system with the super gain user or administrator privileges.

**Probe:** Attacker can access the gain information from the target host.

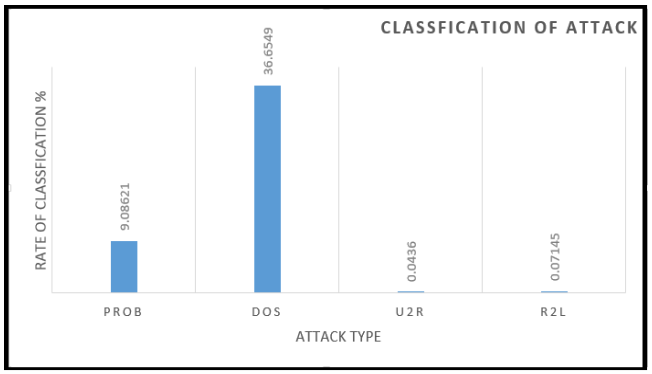



Fig.1. Classification of Attack

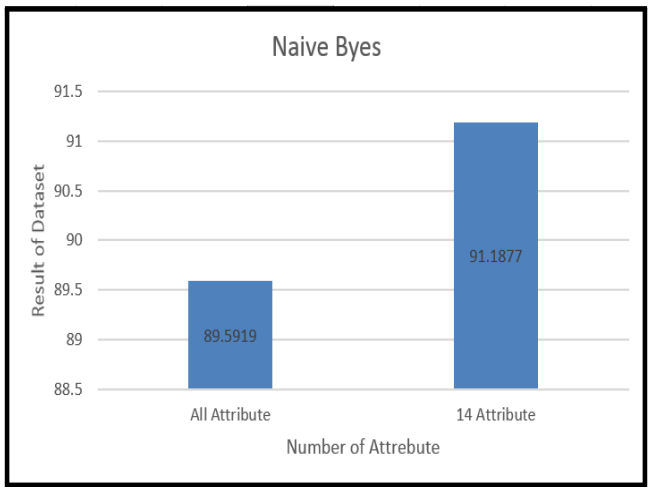
## IV. EXPERIMENT AND RESULT:

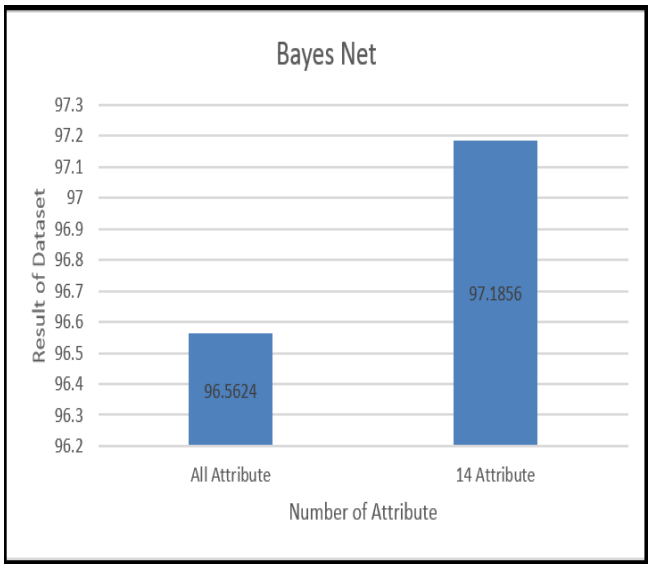
In this review, we experiment on to the Machine Learning algorithms. There are different types of classifiers are use for machine learning algorithms such as Byes Net, Naïve Byes, Decision Table, Trees J48 (C4.5), PART and Random Tree. These all are classifiers used for the analysis purpose with the KDD 99 20% dataset [9][10].

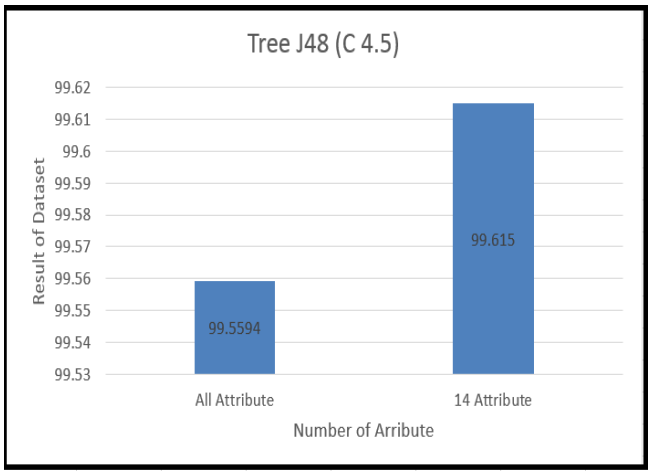
In the figure, 1 shows the all the result of all classifiers. In that, the result with all features will be compared with only 13 features. In this review, the time complexity and the accuracy will be increased by using the specified features. Time complexity is minimalized as compared to all attributes.

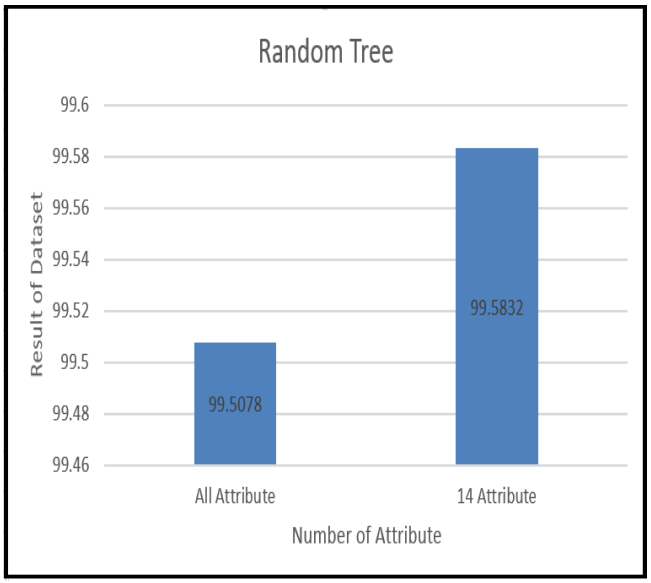
Using a machine learning algorithms with the selected attribute the accuracy, as well as the time complexity is improved as shown in figure 1. The accuracy will be increased, and the time complexity is less as compared to all attribute [8].

In this experiment, Weka tool is used to calculate the result by using the classifiers. In the machine learning algorithms such as Naïve Byes, the accuracy with all attribute is 89.5919%, and time complexity 0.2 seconds; but by using only 13 attribute result is 91.1877% and time complexity 0.09 seconds. In Bayes Net algorithm, the accuracy of all attribute 96.5624% and time complexity 0.63 seconds but by using the 13 attribute result is 97.1856% and time complexity 0.27 seconds. In the J48, the accuracy with all attribute is 99.5594% and time complexity 2.05 seconds but by using the 13 attribute result is 99.6115% and time complexity 0.09 seconds. In the Random Tree, the accuracy with all attribute is 99.5078% and time complexity 0.22 seconds but by using the 13, attribute result is 99.5832% and time complexity 0.13 seconds. Also in the rules PART algorithm the accuracy with all attribute is 99.0631%, and time complexity 2.72 seconds; but by using the 13 attribute result is 99.4482%, and time complexity 0.81 seconds [7][8][9].





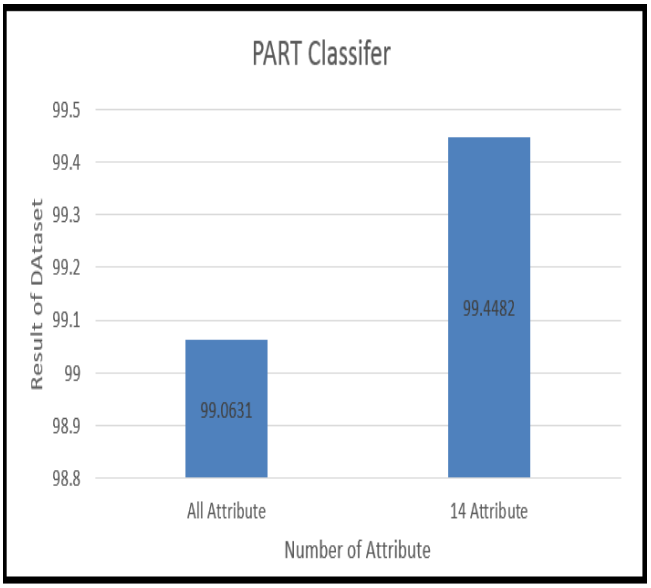




Fig.2. Result of all classifiers with time complexity

| Sr. No. | Classifier Name | Number of Attributes | |
|---|---|---|---|
| | | All | 14 |
| 1 | Naïve Byes | 0.2 | 0.09 |
| 2 | Byes Net | 0.63 | 0.27 |
| 3 | J48(C4.5) | 1.55 | 0.09 |
| 4 | Random Tree | 0.22 | 0.13 |
| 5 | PART | 2.72 | 0.81 |

Table I. Time Complexity of classifiers

| Sr. No | Attribute No. | Attribute Name | Description | Conditions for Malicious Activities |
|---|---|---|---|---|
| 1 | 2 | protocol type | Connection Protocol(e.g. TCP, UDP, ICMP) | icmp \| http \| tcp |
| 2 | 3 | service | Destination Service | eco_i \| ecr_i \| private \| ftp \| ftp_data \| other |
| 3 | 4 | flag | Status flag of connection | S0 \| REJ \| SF \| RSTR \|RST0 \| RSToS0 \|OTH \| SH |
| 4 | 5 | source byte | Bytes send from source to destination | 0 \| <30 \| >500 \| 54540 \| !=105 \| <10 \| ==334 \| >1000 \| 334 |
| 5 | 12 | logged in | 1 if successfully logged in; 0 otherwise | 0 |
| 6 | 14 | root shell | 1 if root shell is obtained; 0 otherwise | <2455 |
| 7 | 16 | #_root | Total number of root accesses | >0 |
| 8 | 18 | #shells | Number of shell prompts | >0 |
| 9 | 23 | count | Total number of connections to the destination host as the current connections in the past 2 seconds | >=1 |
| 10 | 34 | dst_host_sr_rate | %_of connections_the same destination host and using the same service [3]. | <=1 |
| 11 | 38 | dst_host_ serror_rate | %of connections to the current host that have an S0 error[3]. | <=1 |
| 12 | 39 | dst_host_srv_serr or_rate | % of connections to the current host and specified service that have S0 error [3]. | <=1 |
| 13 | 40 | dst_host_srv_rerr or_rate | % of connections to the current host that have an RST error[3]. | <=1 |

Table II. List of all attribute that are Malicious with their conditions

In Table No. 2 there is a list of all attribute that are malicious with their conditions. In this literature survey, we observe that all attribute in the KDD Cup-99 20% dataset is not giving the more accuracy as well as the having, the more time complexity to calculate the result. By using the selected attribute with also some conditions, we will improve the accuracy with a minimum time complexity.

## V. CONCLUSION

The paper, we use the Machine Learning algorithms by using the WEKA to calculate the accuracy and the time complexity by using the selected attribute with conditions. As compared to the existing algorithms or classifiers with all attribute, purpose work improves the more accuracy as well as the time complexity. In this review, we represent the minimum number of the attribute to vary the result of existing algorithms. For feature work, this review is more helping to the investigator to find the malicious or anomaly detection with minimum time and the maximum accuracy.

## REFERENCES

[1] Neminath Hubballi, Vinoth Suryanarayanan, "False alarm minimization techniques in signature-based intrusion detection systems: A survey" Computer Communications 49 (2014) 1–17.

[2] A. M. Riad, Ahmed Hassan and Nancy Awadallah, Visualize, "Network Anomaly Detection By Using K-Means Clustering Algorithm" IJCNC Vol.5, No.5, September 2013

[3] Dr.S.Siva Sathya, Dr. R..Geetha Ramani, K.Sivaselvi, "Discriminant Analysis_based Feature Selection in KDD_99 Intrusion Dataset" International Journal of Computer Applications (0975 – 8887)

[4] J. H. Güne Kayacýk, A, Malcolm I.H. "Selecting Features for Intrusion_Detection: A Feature Relevance Analysis on KDD-99 Intrusion Detection Datasets." International Journal of Computer Applications (0975 – 8887)

[5] Jianhua Sun, Hai Jin, Hao Chen, Zongfen Han, and Deqing Zou. 2003. "A Data Mining Based Intrusion Detection Model. Lecture Notes in Computer Science." Intelligent Data Engineering and Automated Learning. Springer publications. Volume 2690, 677-684.

[6] Knowledge discovery in databases Defense Advanced Research Projects Agency (DARPA) archive and Task Description. http://www.kdd.ics.uci.edu/databases/kddcup99/task.html.

[7] Phurivit Sangkatsanee, Naruemon Wattanapongsakorn, Chalermpol Charnsripinyo, "Practical real-time intrusion detection using machine learning approaches." Computer Communications 34 (2011) 2227–2235

[8] Weka 3.6.0 tools http://www.cs.waikato.ac.nz/ml/weka/.

[9] http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[10] http://nsl.cs.unb.ca/NSL-KDD/

[11] M. Hemalatha, G.V. Nadiammai,"Effective approach toward Intrusion Detection System using data mining techniques" Egyptian Informatics Journal (2014) 15, 37–50

[12] Robert Mitchell, Ing-Ray Chen, "survey of intrusion detection in wireless network applications" Computer Communications 42 (2014) 1–23

[13] Arjunwadkar Narayan M., Thaksen J. Parvat, "An Intrusion Detection System, (IDS) with Machine Learning (ML) Model Combining Hybrid Classifiers."

[14] Ibrahim Elhenawy, Ahmed Hassan, A. M. Riad and Nancy Awadallah, "Visualize Network Anomaly Detection By Using K-Means Clustering Algorithm" International Journal of Computer Networks & Communications (IJCNC)No.5, September 2013.