Efficient Technique for Boosting Attack Detection Rate over a Host or Network System

Shashikant Sharma
M.Tech Scholor,
Deptt. of CSE
RIET, Jaipur,Rajasthan, India

Vineeta Soni
Asst. Prof.,
Dept. of CSE
RIET, Jaipur,Rajasthan, India

Nitesh Pradhan
Asst. Prof.
,Dept. of CSE
RIET, Jaipur,Rajasthan, India

ABSTRACT
In recent years, with the growth of network technologies and its sizes the ratio of attacks has also increases. An attack is an event which has been designed with the aim to bypass the security parameters such as confidentiality, integrity, and/or availability of a standalone computer system or a network. Sometime attacks may cause of heavy loss for an individual, or an organization. To reduce an effect of attacks, it is good to detects at an early stage as it entered in a system or network. However, since the age of computer network number of researchers and industry communities has proposed a variety of exclusive attack detection algorithms in order to prevent information from such threats but each approach has its own problem in their performance. On the other hand most of the accessible techniques use signature base algorithm, detect only previously identified attack types, fails to detect the new attacks and produce huge false alarms so not be suitable for high pace networks. These issues severely restrict the utility of deterrence system. This paper has considered such issues and proposed a novel attack detection technique which generates low false alarms with enhancing the attack detection rate of known as well as anomaly attacks over the network.

Keywords
Intrusion Detection System, Security, Data Mining, Feature Extraction.

1. INTRODUCTION
Nowadays, with the growth of communication techniques the security fears have also augmented. The attackers come rapidly with the naïve techniques of attacks. On the other hand the vulnerabilities of a system/network and secrete information always attract the consideration of an attackers. Thus safe and sound communication has become a fundamental issue in a network based system. Broadly the whole attacks can be categories in one of the following four categories as depicted in figure 1.

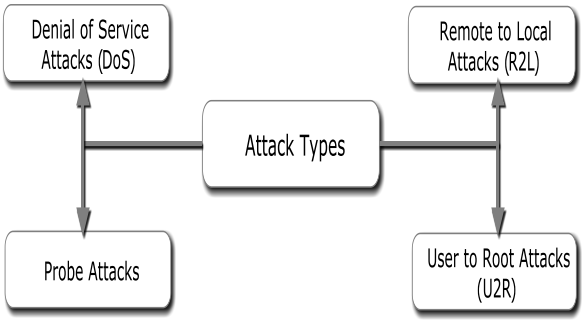

Fig.1 Types of Attacks over a host or Network System

- **Denial of Service Attacks (Dos):** These types of attacks targeted the computer's network bandwidth or connectivity by flooding a tall amount of traffic or connection requests to prevent authorized users from the right to use of requested service. SYN, Ping of Death, Eavesdropping, Spoofing, Smurf, Teardrop are some example of DoS types attacks [1-2].
- **Probe Attacks:** With the aim to prevent legitimate users from accessing information or services these type of attack automatically scans a computer network for open ports and Attackers tries to gain information about the target host.
- **Remote to Local Attacks (R2L):** The attacker use wide-rang in g procedure transversely on a diverse network or surrounded by a sole host for services to probe the targeted network or single machine for open ports. This process is referred to as Probe Attacks [3].Ipsweep, Portsweep, Nmap, Satan is probe type of attacks.
- **User to Remote Attacks (U2R):** These types of attacks are designed with the aim to gain the root privileges at single host or a network system by unauthorized way.The attacker get permission to access the special files exfiltrates them via common applicationssuch as mail or FTP [4]. Loadmodule, Perl, Buffer Overflow are a types of U2R attacks.

2. CLASSICAL ATTACK DETECTION MECHANISMS
In order to detect signs of security problems at an alone or a network mechanism the applied course of actions is known as an attack detection system. These systems monitor and analyze the occurring events in an alone or network machine for detecting an attack types of activities. There are a number of unrelated systems provide sole functions and mechanisms for attack detection with the aim to detect, filter, or prevent system from attack to provide data security and ensure continuity of services provided by a network. On the base of attack detection system component, monitoring activity, detection technique and their response activity the detection system can be broadly categories as presented in fig 2.

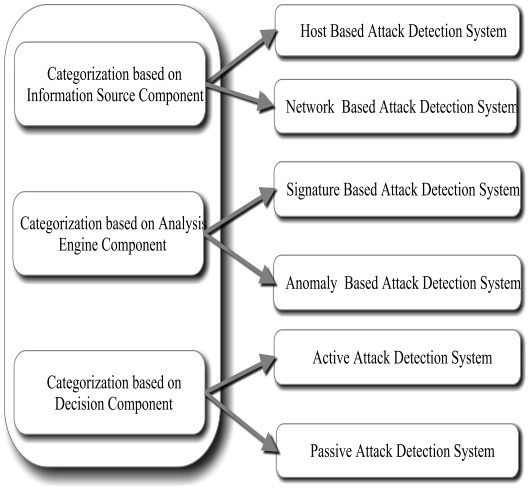

Fig. 2 Categorization of Attack Detection System

2.1 Host Based System

Typically the Host-based attacks attempt to achieve privileged services or resources of the system. Usually Host-based detection mechanism uses routines that obtain system call data from an audit process, which tracks all system calls made on behalf of each user. In comparison of Network-based attack detection system the Host-based attack detection systems relies on events gathered by the hosts and present much more relevant information.

- **Advantages of Host based Systems**
  - Detects attacks with high accuracy that cannot be detected by Network based attack detection system.
  - The data sources are normally generated on a plaintext so it can efficiently operate in encrypted environment.
  - A change in topology does not change its performance.
  - Does not require additional hardware.
  - Lower entry cost
- **Disadvantages of Host based Systems**
  - Provide poor real-time response and cannot effectively protect against one-time catastrophic events.
  - Are not well suited by detecting network scans or other such surveillance that targets an entire network.

2.2 Network Based System

As like its name these types of detection systems monitor network traffic instead of a single host for finding unauthorized activities. A network attack tries to prevent the users to access the network services or resources by sending large amounts of network traffic, exploiting well-known faults in networking services, and overloading network hosts. Sometime scanning process of OS trails or system logs are not efficient to detecting such types of attacks. On the other hand huge and rapid increases size make problem in detection of network attack. Typically a network attack detection systems desires enthusiastic hardware which can verify network packets in order to find out any malicious or abnormal activity

- **Advantages of Network based Systems**
  - Useful to monitor flexible network in place of single host.
  - Useful to speedy real rime detection and reaction.
  - Can work with classical security mechanisms such as firewalls, encryption, and other authentication methods.
  - Easy to install with low cost and small number of sensors at hubs, routers etc.
  - Uses packet sniffing.
- **Disadvantages of Network based Systems**
  - It may have difficult processing, all packets in a large or busy network and therefore, may fail to recognize an attack launched during periods of high traffic.
  - The encrypted information cannot be analyzed by this system.
  - Modern switch-based networks make it more difficult: Switches subdivide networks into many small segments and provide dedicated links between hosts serviced by the same switch. Most switches do not provide universal monitoring ports.

2.3 Signature Based System

This technique detects attacks repeatedly and more accurately in terms of the characteristics of known attacks or system vulnerabilities in same way as any anti-virus software operates. Depending on the robustness and seriousness of a signature that is activated within the system, some alarm response or notification should be sent to the right authorities. There are two techniques used in signature based attack detection mechanisms (i) Expression matching and (ii) State transition analysis. Expression matching is a trouble-free type technique which monitor events like log entries for the occurrence of accurate pattern. Where state transition analysis model analysis the transitions in the network. Every event in the network is applied to finite state machine instances which finally results in transition. An attack will be occurred when the machine reaches its final state. Regular updating of signatures database is a key part for this type of attack detection mechanisms because of in case of non-updating the mechanism will face trouble to detect the new threats.

- **Advantages of Signature Based System**
  - Detect huge amount of attacks efficiently.
  - Produce low false alarms.
  - Can apply on a single host or network based system.
- **Disadvantages of Signature Based System**
  - Require huge storage space to store signatures.
  - Require regular updating of signature database to identify novel intrusion profiles.
  - Requires lots of domain knowledge and huge time for execution process.

2.4 Anomaly Based System

The anomaly based attack detection systems are able to detect the novel attacks with the functionality of signature based

mechanism. To build the attack detection model anomaly based systems use regular statistics which make it dissimilar from signature based attack detection mechanism. It typically involves the creation of knowledge bases that contain the profiles of the monitored activities. The mechanism further classifies in two categories i.e. static and dynamic detectors.

The constant part of the observing scheme assumed as a static anomaly detector. In a system a binary bit may be an example of static segment. The mechanism is possessed into two parts i.e. system code and system data. If any discrepancy from its inventive form is take place then fault has been designate or the intruder has redesigned the piece of the system. Dynamic detector incorporated the system behavior i.e. an order of different events. If uncertain behavior is considered as anomalous, then the system administrators may be alerted by false alarms.

- **Advantages of Anomaly System**
  - Can detect novel attacks without specific knowledge of details.
  - Doesn‘t require frequently updating of signature database.
- **Disadvantages of Anomaly System**
  - Produce false alarm at high rates due to the unpredictable behaviors of users and networks.

2.5 Active System

These types of systems not required human intervention for configuring process. System build up automatically and providing real-time remedial action in response to an attack. However system block the attack at real time event occurrence but for the system it is must that it placed as in-line along a network boundary; thus, the IPS itself is susceptible to attack.

2.6 Passive System

The system not provides any action automatically whenever it found any suspicious events. It only aware the administrator for taking an receptive action on the base of information. This type of attack detection system is not capable of performing any protective or corrective functions on its own. The major advantages of these types of systems are that the systems can be easily and rapidly deployed and are not normally susceptible to attack themselves.

3. RELATED WORK

In the era of information and system security first approach was introduced in 1980. The approach monitors the user actions for detecting an attack. However proposed approach detects an attack in a system but its examination process was slow that make system inefficiency.

To improve an attack detection system performance a novel rule based approach has been proposed in [5]. The approach has increased the attack detection ratio by takes out features from a variety of audit streams and examines the network packets with matching the values to a set of attack signatures provided by human experts. However approach significantly presents its efficiency over the previous approach for attack detection but required regular updating process of new attack signature in database. The regular updating process of an signature database may be possible with a small network but with the growing size of an network the regular updating process is not possible for human analysts which produce inefficiency of such approach. On the other hand the process of encoding rules is exclusive and time-consuming. To enhance the performance of rule based attack detection mechanism a number of researchers have proposed their unique and effective ideas, presented in [6-8].

In same context to enhance attack detection accuracy over a system a number of authors have combined different techniques such as combining the decision tree and support vector machine (DT-SVM)[9] and Fuzzy logic and Genetic Algorithms [10-12]. These techniques have been used to mine normal patterns from audit data and concentrate on analyzing the properties of the audit patterns rather than identifying the process which generated them.

Several of techniques introduced on the base of node monitoring concepts to examine distinctive division of a network i.e., either communication links or WMN nodes [13,14] . However techniques improve the performance of attack detection systems but generate huge amount of false alarms due to inadequate resources e.g., memory and processing power. To trim down the ratio of false alarms a Lightweight detection engine for WMN has been presented in [15]. The approach requires a smaller amount of computational load than off-the-shelf ADS. However approach still suffers from high false negative rates production problem. For improving the QOS of accessible attack detection systems number of researchers used different techniques such as classification, clustering, association rule, and outlier detection [16]. However approach pick up some quality of ADS but suffers from their own limitations such as clustering technique has limitation that it cannot be easily used with symbol features, the observation must be numeric. It considers the features independently and unable to capture the relationship between different features of a single record, which degrades attack detection accuracy.

A novel detection mechanism named ADWICE proposed in [17]. The technique was based on the algorithm named BIRCH. However approach produces improved incremental learning function but suffer with the noise data. In same direction an author has proposed an approach to improve the mechanism of ADWICE [18].

Same as previous approach the proposed mechanism was depends on the training data and consequently the set of independent variables (attributes) that enters the analysis is also an issue. A new feature selection based approach for reducing the delay proposed by author in [19]. The approach use expectation maximization to calculate the attribute value of the missing data.

To handle detection accuracy ratio over the huge and speedy networks a flow and packet examination based multi-layered approach has proposed in [20]. The flow-based detection mechanism suggest numerous compensation in terms of processing requirements the aggregation of packets into flows obviously entails a loss of information. Apart from this the amount of information is not forced when packet-based intrusion detection is act upon, but due to strict processing necessities its application is habitually impracticable. The proposed approach fills this gap by makes a pre-selection of suspicious traffic at it very first level than examine the packet for a normal or attack event.

In same way a layered approach by using anomalyand signature based technique proposed in [21]. The proposed approach use Hidden Markov Model and have four layer mechanisms which has been designed and trained to detect separate type of attack. An analysis work for a random deployment of sensor nodes on the surveillance WSN

applications has done in [22]. The author addresses the problem of network coverage and enhances the deployment quality.

A sequence-aware attack detection system present in [23]. The proposed approach trained with the real ICS traffic samples captured from a water treatment and purification facility and demonstrate how a precise sequence of acceptable process can escape standard attack detection systems and motionless damage an infrastructure.

In direction to improve the detection rate of minority attack class a hybrid approach by combining SVM and genetic algorithm proposed in[24]. The approach use reduced feature set and hierarchical clustering algorithm to provide a high detection rate of an attack events. A new outlier detection mechanism proposed in [25]. The mechanism deliberate anomaly dataset by the Neighborhood Outlier Factor (NOF). The proposed approach consists of huge datasets with dispersed storage setting for improving the recital of attack detection system. In another approach author has proposed a Neuro-Fuzzy-Genetic attack detection system [26].

The approach identified a new research direction in the related field. A distributed attack detection system over the network has proposed in [27]. The approach use naïve bayes classifier in a level form for detecting anomaly events and to avoid the single point of failure issue. However approach enhances the accuracy of attack detection system but provide more focus on DDoS attacks.

4. MODERN STATUS, CHALLENGES AND RESTRICTIONS OF ACCESSIBLE IDS

In the last two decades, different approaches have been designed and implemented to accomplish the desirable elements of an efficient attack detection system but on daily basis naïve attackers have introduces the advance and powerful techniques for breaking the security system of a host or a network. On the other hand the regular increases size of a network system makes it more prone to vulnerabilities. The idea of attack detection system was introduce with the paper [28]. Since then several of researchers use different unique approaches for improving the excellence of this system [29-32].However, the accessible approaches augmented the attack detection mechanism but still have some following major challenges [33-36].

- In the era of higher bandwidths and ease of connectivity of wireless and mobile devices the conventional detection systems takes more time for analysis process and often computationally exhaustive.
- Majority of conventional systems are tuned to detect only known major service level attacks.
- Unable to detect anomaly attacks over the system or network.
- Major of attack detection systems demonstrate better accuracy in detecting certain class of attacks while performing inadequately for the other classes.
- Always required updating process by human.
- Produce low accuracy.
- Generate huge false alarms.

These challenges has produce an opportunity and motivation in direction to design an novel approach for enhancing the recital of accessible attacks detection mechanism by using a variety of advanced techniques.

5. ADVANCED ATTACK DETECTION SYSTEM: PROPOSED APPROACH

As discussed in literature, nearly all accessible attack detection systems are designed and trained with the signature based technique thus can detect only previously known attacks and be unsuccessful with the sense of novel event of an attack. On the other hand most of system use full feature set for attack detection process thus generate high false alarm with expensive operation cost. In order to trim down such issues of accessible detection mechanism the proposed approach has incorporated a new feature reduction technique. Apart from inclusion of feature reduction mechanism proposed approach has sense the data in layered format, as packet entered in system or network it check at four stages in sequential manner. If a packet found as an attack at any stage of proposed system it will be block else passes to the next stage for same process, at the end stage if packet is not block than it will be allowed for the system as normal data. Typically framework of proposed approach consists with the three different parts.

5.1 Gathering Data for Training & Testing of Proposed Approach

Gathering truthful and well-organized data is an important dilemma for design and development of an efficient attack detection system. A widespread dataset named NSL-KDD dataset [37] has been used to train and test of proposed approach. The selected data set incorporated 125973 instances, 58630 attack type and 67343 normal data instances. Broadly attack types are fall under the four categories [38], tabulated in Table 1.

Table 1 Attacks Associated With NSL KDD Dataset

Attack Type	Attack Name
DOS	Smurf, Neptune, Back, Teardrop, Pod, land, syslogd, ftp_write, guess_passwd, imap, phf, spy, warezclient, warezmaster
PROBE	Satan, Ipsweep, Portsweep, Nmap, Mscan
R2L	Warezclient, Guess_passwd Warezmaster, Imap, ftp_write, Guest, Netbus, Multihop, Phf, Spy
U2R	Buffer, Overflow, Rootkit, Load Module, Perl, Multihop

The DoS and Probe attacks belong to majority class whereas U2R and R2L belongs to minority class also called as rare class of attacks. The selected dataset contain 45927 DoS, 11656 Probes, 995 R2L, 52 U2Rattack instances. The following Figure3 illustrates the percentages of attacks.

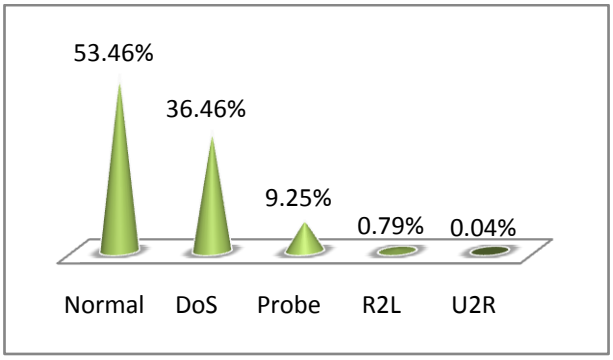

Fig. 3 Percentage of attack Instances Associates with Selected Dataset

5.2 Pre-processing of Selected Dataset

To improve the efficiency and ease of data QOS the preprocessing is one of the most critical process which deals with the preparation and transformation of the initial dataset. The step of preprocessing divided into two categories i.e. (i) Discretization & Feature selection. Typically, Discretization is the process of converting numerical attributes into nominal ones. The feature selection/reduction is a central issue in the era of attack detection field. The performance of a classifier is heavily influenced by the features chosen for entity representation. Fundamentally feature selection is a technique which trims down the calculation time and model complication by selecting only relevant/important features from the complete feature set. The table 2 presents the complete feature set of NSL KDD dataset.

Table 2 Complete List Of Features Given In Nsl Kdd Cup 99 Dataset

Feature Index	Feature name	Description
1.	duration	length (number of seconds) of the connection
2.	protocol_type	type of the protocol, e.g. tcp, udp, etc.
3.	Service	network service on the destination, e.g.,http, telnet,etc.
4.	Flag	normal or error status of the connection
5.	src_bytes	number of data bytes from source to destination
6.	dst_bytes	number of data bytes from destination to source
7.	Land	1 if connection is from/to the same host/port; 0 Otherwise
8.	wrong_fragment	number of ``wrong'' fragments
9.	Urgent	number of urgent packets
10.	Hot	number of ``hot'' indicators
11.	num_failed_logins	number of failed login attempts
12.	logged_in	1 if successfully logged in; 0 otherwise
13.	num_compromised	number of ``compromised'' conditions
14.	root_shell	1 if root shell is obtained; 0 otherwise
15.	su_attempted	1 if ``su root'' command attempted; 0 otherwise
16.	num_root	number of ``root'' accesses
17.	num_file_creations	number of file creation operations
18.	num_shells	number of shell prompts
19.	num_access_files	number of operations on access control files
20.	num_outbound_cmds	number of outbound commands in an ftp session
21.	is_hot_login	1 if the login belongs to the ``hot'' list; 0 otherwise
22.	is_guest_login	1 if the login is a ``guest'' login; 0 otherwise
23.	Count	number of connections to the same host as the currentconnection in the past two seconds
24.	srv_count	number of connections to the same service as the current connection in the past two seconds
25.	serror_rate	% of connections that have ``SYN'' errors
26.	srv_serror_rate	% of connections that have ``SYN'' errors
27.	rerror_rate	% of connections that have ``REJ'' errors
28.	srv_rerror_rate	% of connections that have ``REJ'' errors
29.	same_srv_rate	% of connections to the same service
30.	diff_srv_rate	% of connections to different services
31.	srv_diff_host_rate	% of connections to

		different services
32.	dst_host_count	count for destination host
33.	dst_host_srv_count	srv_count for destination host
34.	dst_host_same_srv_rate	same_srv_rate for destination host
35.	dst_host_diff_srv_rate	diff_srv_rate for destination host
36.	dst_host_same_src_port_rate	same_src_port_rate for destination host
37.	dst_host_srv_diff_host_rate	diff_host_rate for destination host
38.	dst_host_serror_rate	serror_rate for destination host
39.	dst_host_srv_serror_rate	srv_serror_rate for destination host
40.	dst_host_rerror_rate	rerror_rate for destination host
41.	dst_host_srv_rerror_rate	srv_serror_rate for destination host

However, the entire feature set may apply for the solving of classification issues but it is not must and efficient way at each and every time. Some time use of entire feature set may degrades the performance of the detection system. Therefore, a manual effort has been done in proposed approach for the process of feature selection. The table 3 present the selected features set which used in the proposed approach for enhance the power the attack detection mechanism.

Table 3 List of Selected Feature Set Used In Proposed Approach

S.No.	Feature name
1.	duration
2.	Service
3.	src_bytes
4.	dst_bytes
5.	Hot
6.	num_compromised
7.	num_root
8.	num_file_creations
9.	rerror_rate
10.	diff_srv_rate
11.	dst_host_count
12.	dst_host_srv_count
13.	dst_host_same_src_port_rate

The figure 4 presents the feature selection mechanism of proposed approach.

X: The original feature vector

D: Training data used for classification.

TPDR: True Positive and Detection Rate

NTPDR: New True Positive and Detection Rate

Input: X={X1, X2,…,Xm}, D

1. Compute TPDR with X
2. IR← 0
3. For i is from 1 to m do
4. For j is from 1 to m do
5. Delete j^{th} feature from X and execute classifier
6. Compute NTPDR
7. If NTPDR ≤ TPDR
   Added the deleted j^{th} feature in X
   Else
   TPDR← NTPDR
   IR← 1
   Endif
   Endfor
8. If IR = = 0
   Endfor

Fig. 4 Feature Selection/ Reduction Method

5.3 Classification

Typically, classification procedure is a methodical approach to build classification models from an input data set. Each and every classification technique take up a unique learning algorithm to recognize a model that best fits the connection between the attribute set and class label of the input data. Over the past several years, a rising number of researchers have applied different classification methods such as decision trees, artificial neural networks and a probabilistic classifier to solve a classification problem. They present their classification results in terms of attack detection rates and generation of false alarms and have demonstrate that these classification techniques still suffer from generating of high false positives and irrelevant alerts in detection of novel attacks with requirement of more time to build the detection model. On the other hand a number of researchers have demonstrated the efficiency of Naïve Bayes classification algorithm over the other in terms of model building time and other parameters. The proposed technique incorporated the Naïve Bayes mechanism for the process of classification.

Naive Bayes classification algorithms are a set of supervised learning as well as a statistical method. Typically it is based on Bayesian theorem with the "naive" assumption of independence between every pair of features. This classification algorithm is mainly suited in the situation of high inputs dimensionality and provides a practical perspective for considerate and assess various learning algorithms.

Figure 5 presents the complete mechanism of proposed approach.

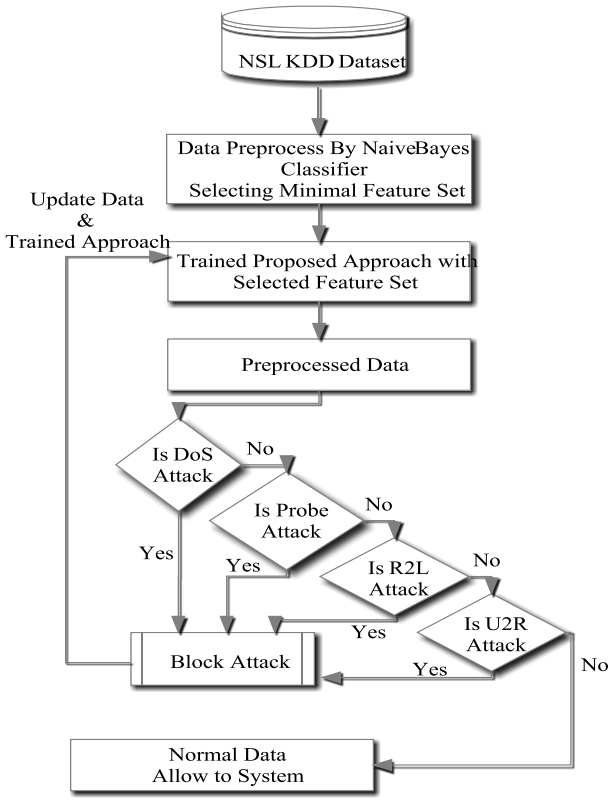

Fig. 5 Flow Chart of Method Used to Attack Detection

6. EXPERIMENTAL SETUP & RESULT ANALYSIS

Evaluations of an attack detection mechanism in real world applications may be an expensive way in terms of construct a human resources, network or server client architecture. On the other hand evaluation of an algorithm in a simulated environment is a cheap and efficient way to know the performance of proposed approach in nearer to real or real world environment. To evaluate recital of proposed work simulation tool Weka[39] is used in this investigation.

The word WEKA stand for Waikato Environment for Knowledge Analysis is anadmired simulation tool in the era of machine learning. The tool is implemented in a popular robust language JAVA so it can be used at any platform without affecting the evaluation performance which enhance it acceptability and efficiency. Anyone can access the version of WEKA simulation tool without any cost from an internet [39] which provides a simple and effective GUI for users to use without any troublefor completing the tasks, more specifically related to data pre-processing, classification, regression, clustering, association rules, visualization, and feature selection. The tool incorporated a number of machine learning techniques which may use by user by applying datadirectlyor may call from their own designed code.This interface is flexible enough and users need only concern themselves with the selection of features in the data for analysis and what the output means, rather than how to use a machine learning scheme. It has a number of advantages over the other accessible simulation tools which make it more effective.

6.1 Evaluation Matrices

To evaluate the performance of proposed algorithm against accessible approaches differentperformance matriceshas been used, which can be explained as

- **True Positive (TP):** Attack event detect correctly related to its class type.
- **True Negative (TN):** True Negative corresponds to a state of affairs when no attack has taken positionand no alarm is raised.
- **Detection rate (DR):** It define the rate of correctly attack detection rate and calculate as

$$\text{Detection Rate (DR)} = \frac{\text{TP}}{\text{TOTAL NO OF INTRUSION INSTANCE IN DATASET}}$$

- **False Positive (FP):** System raised alarm while there is no attackknown as FP.
- **False Negative (FN):** Situation when genuine attack event detected as normal event.
- **False Alarm Rate (FAR):**Represent the percentage of FP calculated as

$$\text{False Alarm Rate (FAR)} = \frac{FP}{FP+TN}$$

Accuracy is measured by the following formula:

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN}$$

6.2 Result Analysis

To present the effectiveness of selected feature set and proposed attack detection method the performance is compared with the classification results based on other existing automatic feature selection algorithms such as CFS with the Best First Search method, Gain Ratio and Info Gain with the Ranker method. The figure 6 & 7 has present the comparative classification result based on the detection accuracy and detection rates of attack types.

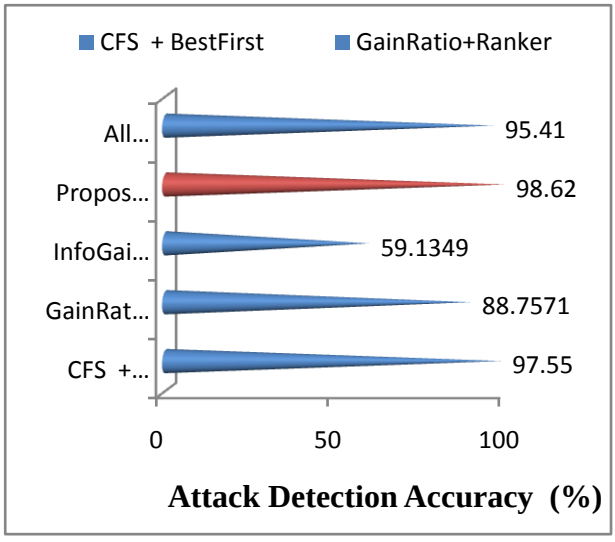

Fig 6 Efficiency of Selected Feature Set over the Existing Feature Selection Technique

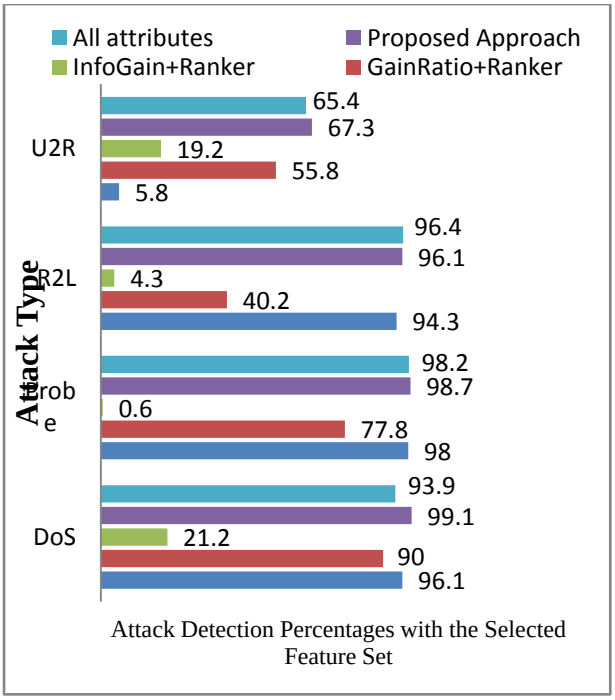

Fig. 7 Class wise Accuracy

However the above figure shows that proposed feature set produced efficient result in comparison of the features set which provided by the other existing automatic feature selection/reduction based algorithm. To check efficiency of proposed approach in more depth it compared also with the results of other accessible detection approaches on the base of same evaluation metrics. The values presents in following table 4 present the significant comparative results of proposed approach over the other accessible attack detection algorithm.

Table 4 Detection Accuracy Rate Of Proposed Approach Over The Other Offered Algorithms

Approaches	Correctly Classified Instances (%)	False Alarms Rate
Proposed Approach	98.62	1.38
Hierarchical Clustering, SVM and GA based techanique [89], January 2015	98.45	1.55
Hybrid layered intrusion detection system [91], Feb. 2015	92.13	7.87
improved PSO-BP neural network algorithm[92], 2015	96.73	3.27
K-medoids method and clustering based approach [74], March 2014	96.38	3.2
DTNB Based Approach [93], June 2014	97.14	2.86

The above table values clear present the significance of proposed approach over the other offered approaches which are accessible since 2010 to the current time. The results of the proposed approach compares in two ways i.e. on the base of attack detection accuracy and false alarms generating rate. In both ways the proposed approach has produced comparative and significant improved results over the other accessible approaches. However the approach which has been proposed in this paper has produced false alarms but in comparison of other on hand algorithms it is low with the high detection rate of attack events that shows the significance of proposed technique.

7. CONCLUSION

This paper presents a novel layered mechanism for attack detection system. The proposed technique incorporates a new feature set selection mechanism to improve the performance of classification. The presented table and figures in results section clearly shows the significance of proposed approach over the other accessible feature selection or detection mechanism. However proposed approach enhances the accuracy but still generate false alarms. Therefore future work can in done in direction to trim down such issues with increasing the efficiency and accuracy of proposed approach.

8. REFERENCES

[1] Frank Kargl, Jörn Maier, Stefan Schlott, Michael Weber ―Protecting Web Servers from Distributed Denial of Service Attacks‖ ACM 1-58113-348-0/01/0005. May 1-5, 2001,

[2] Anita K. Jones and Robert S. Sielken –"Computer System Intrusion Detection A Survey "International Journal of Computer Theory and Engineering, Vol.2, No.6, December, 2010.

[3] Khaled Labib, V. Rao Vemuri ―Detecting and Visualizing Denial-of-Service and Network Probe Attacks Using Principal Component Analysis‖, 2006.

[4] K. Kendall, A database of computer attacks for the evaluation of intrusion detection sytsems, Thesis, MIT, 1999.

[5] Dorothy E. Denning, and P.G. Neumann "Requirement and model for IDES- A real-time intrusion detection system," Computer Science Laboratory, SRI International, Menlo Park, CA 94025-3493, Technical Report # 83F83-01-00, 1985.

[6] Barbarà, D., Couto, J., Jajodia, S., Popyack, L., and Wu, N., ADAM: A Testbed for Exploring the Use of Data Mining in Intrusion Detection, ACM SIGMOD Record, 30(4), 2001,pp. 15-24.

[7] Wenke Lee and Salvatore J. Stolfo, ―A Framework for Constructing Features and Models for Intrusion Detection Systems‖, ACM Transactions on Information and System Security (TISSEC), Volume 3, Issue 4, November 2000.

[8] Hamdan.O.Alanazi, Rafidah Md Noor, B.B Zaidan, A.A Zaidan "Intrusion Detection System: Overview" Journal Of Computing, Volume 2, Issue 2, February 2010, Issn 2151-9617

[9] S. Peddabachigaria, A. Abrahamb, C. Grosanc and J. Thomas, "Modelling intrusion detection system using hybrid intelligent systems," Computer Applications, vol.30, 2007, pp.

[10] Chi Ho Tsang, Sam Kwong, and Hanli Wang, "Genetic-fuzzy rule mining approach and evaluation of feature selection techniques for anomaly intrusion detection." Pattern Recognition, 40(9), 2007, pp. 2373–2391.

[11] M. Saniee Abadeh, J. Habibi, and C. Lucas, "Intrusion detection using a fuzzy genetics-based learning algorithm." Journal of Network and Computer Applications, 30(1), 2007, pp. 414–428.

[12] Animesh Patcha and Jung-Min Park. An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends. Computer Networks, 51(12):3448– 3470, 2007.

[13] D.-H. Shin and S. Bagchi, "Optimal monitoring in multi-channel multi-radio wireless mesh networks," in Proceedings of the Tenth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), 2009.

[14] A. Hassanzadeh, R. Stoleru, and B. Shihada, "Energy efficient monitoring for intrusion detection in battery-powered wireless mesh networks," in Proceedings of the 10th International Conference on Ad Hoc Networks and Wireless (ADHOC- NOW), 2011.

[15] F. Hugelshofer, P. Smith, D. Hutchison, and N. J. Race, "OpenLIDS: a lightweight intrusion detection system for wireless mesh networks," in Proceedings of the 15th Annual International Conference on Mobile Computing and Networking (MobiCom), 2009.

[16] L. Portnoy, E. Eskin, and S. Stolfo, ―Intrusion Detection with Unlabeled Data Using Clustering,‖ Proc. ACM Workshop Data Mining Applied to Security (DMSA), 2001.

[17] K. Burbeck & N.Y. Simmin, "Adaptive Real-Time Anomaly Detection with Incremental Clustering", Information Security Technical Report, Vol. 12, No. 1, Pp. 56–67. 2007.

[18] R. Fei, L. Hu & H. Liang, "Using Density-based Incremental Clustering for Anomaly Detection", Proceedings of the 2008 International Conference on Computer Science and Software Engineering, Vol. 3, Pp. 986–989. 2008

[19] J.H. Lee, S.G. Sohn, B.H. Chang & T.M. Chung, "PKG-VUL: Security Vulnerability Evaluation and Patch Framework for Package-based Systems", ETRI Journal, Vol. 31, No. 5, Pp. 554–564. 2009.

[20] Mario Golling, Robert Koch, Rick Hofstede "Towards Multi-layered Intrusion Detection in High-Speed Networks" 2014 6th International Conference on Cyber Confl ict P.Brangetto, M.Maybaum, J.Stinissen (Eds.) 2014 © NATO CCD COE Publications, Tallinn

[21] Archana I. Patil, Girish Kumar Patnaik, Ashish T. Bhole" Network Intrusion Detection using Layered Approach and Hidden Markov Model" International Journal of Computer Applications (0975 – 8887) Volume 93 – No.13, May 2014

[22] Noureddine Assad, Brahim Elbhiri, Moulay Ahmed Faqihi, Mohamed Ouadou, and Driss Aboutajdine "Analysis of the Deployment Quality for Intrusion Detection in Wireless Sensor Networks" Hindawi Publishing Corporation Journal of Computer Networks and Communications Volume 2015.

[23] Marco Caselli, Emmanuele Zambon, Frank Kargl "Sequence-aware Intrusion Detection in Industrial Control Systems" CPSS'15, April 14, 2015, Singapore. ACM 978-1-4503-3448-8/15/04.

[24] Minakshi Bisen & Amit Dubey "An Intrusion Detection System based on Support Vector Machine using Hierarchical Clustering and Genetic Algorithm" The SIJ Transactions on Computer Science Engineering & its Applications (CSEA), Vol. 3, No. 1, January 2015.

[25] Jabez J, Dr.B.Muthukumar "Intrusion Detection System (IDS): Anomaly Detection using Outlier Detection Approach" International Conference on Intelligent Computing, Communication & Convergence, Procedia Computer Science 48 (2015) 338 – 346, ELSEVIER

[26] Ibrahim Goni, Ahmed Lawal "A Propose Neuro-Fuzzy-Genetic Intrusion Detection System" International Journal of Computer Applications (0975 – 8887) Volume 115 – No. 8, April 2015

[27] Michel Toulouse, B`ui Quang Minh, Philip Curtis "A consensus based network intrusion detection System" arXiv:1505.05288v1 [cs.CR] 20 May 2015

[28] James P.Anderson. ComputerSecurity Threat Monitoring and Surveillance,1980.Lastaccessed:Novmeber30,2008. http://csrc.nist.gov/publications/history/ande80.pdf

[29] Prabhjeet Kaur, Amit Kumar Sharma, Sudesh Kumar Prajapat " Madam ID for intrusion detection using data mining" IJRIM volume 2, issue 2, February 2012

[30] Yogendra Kumar Jain and Upendra "An Efficient Intrusion Detection Based on Decision Tree Classifier Using Feature Reduction" International Journal of Scientific and Research Publications, Volume 2, Issue 1, January 2012.

[31] G.V. Nadiammai, S.Krishnaveni, M. Hemalatha " A Comprehensive Analysis and study in Intrusion Detection System using Data Mining Techniques" International Journal of Computer Applications (0975 – 8887) Volume 35– No.8, December 2011

[32] R.Shanmugavadivu, Dr.N.Nagarajan "Learning of Intrusion Detector in Conceptual Approach of Fuzzy Towards Intrusion Methodology" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 5, May 2012

[33] Amin Hassanzadeh, Radu Stoleru, Michalis Polychronakisy , Geoffrey Xie "RAPID: A Traffic-Agnostic Intrusion Detection for Resource-Constrained Wireless Mesh Networks" Technical Report 2014, Texas A& M University Copyright 2014 LENSS.

[34] Dr. S.Vijayarani and Ms. Maria Sylviaa.S "Intrusion Detection System – A Study" International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, February 2015

[35] Ashish Negi, Himanshu Saini" An Overview of Intrusion Detection System in Computer Networks" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-4 Issue-7, December 2014

[36] Uma Vishwakarma, Prof. Anurag Jain "Reduces Unwanted Attribute in Intruder File Based on Feature Selection and Feature Reduction Using ID3 Algorithm"

Uma Vishwakarma et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (1) , 2014, 896-900

[37] Available from: http://nsl.cs.unb.ca/NSL-KDD/

[38] Long-Sheng Chen, Jhih-Siang Syu "Feature Extraction Based Approach for Improving the Performance of Intrusion Detection System" Proceedings of the International MultiConference of Engineers and Computer Scientists 2015 Vol I, IMECS 2015, March 18 - 20, 2015, Hong Kong

[39] http://www.cs.waikato.ac.nz/ml/weka/arff.html