ORIGINAL RESEARCH PAPER
VOLUME-6 | ISSUE-7 | JULY-2017 | ISSN No 2277 - 8179 | IF : 4.176 | IC Value : 78.46
INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

IMPROVED THE INTRUSION DETECTION CLASSIFICATION RATE USING FEATURE REDUCTION TECHNIQUE BASED ON DCA AND PCNN NETWORK

Computer Science

Brajesh Kumar M.Tech. Scholar, CSE Department, IES college of Technology, RGPV Bhopal, India

Prof. Aishwarya Mishra Associate Professor, Department, IES college of Technology, RGPV Bhopal, India

ABSTRACT

Reduction and selection of intruder attribute in intrusion detection system play an important role in process of detection. The huge number of attribute in intruder induces a problem in detection process and increase more time in decision making process. In current research trend some authors used some standard technique for feature reduction such as PCA, PCNN and neural network, but these methods not consider all features for processing fixed some number of feature. In this dissertation proposed a feature selection and feature reduction method based on improved GSA algorithm. The proposed algorithm select multiple feature for reduction and the reduce feature set participant the process of detection. The reduce feature of network file classified by GSA classification algorithm. The DCA algorithm in the case of small data size, if sizes of data are increase the selection of attribute process raised some problem related to feature selection. For the improvement of this problem used PCNN function for increasing the biased value of feature and feature subset selection.

KEYWORDS:

Intrusion Detection System, Feature Reduction, Support Vector Machine, DCA algorithm, PCNN network.

1. INTRODUCTION

The performance of intrusion detection system depends on classification of unknown types of attacks. The detection of unknown types of attack is very difficult due to large number of attribute and huge amount of network data. For the improvement of unknown attack feature reduction is important area of research. The reduction process reduces the large number of attribute and improved the detection of intrusion detection system. In the process of feature reduction various algorithm are used such algorithm are principle of component analysis and neural network. The reduction process used PCA method this method is static reduction technique, reduces only fixed number of attribute. The fixed number of feature reduction process not justify the value of feature it directly reduces the feature. On the consideration of computational time feature reduction is also an important aspect, the reduced feature increase the processing of detection ratio. Many methods have been proposed in the last decades on the designs of IDSs based on feature reduction technique. With the tremendous growth of network-based services and sensitive information on networks, network security is becoming more and more importance than ever before. Intrusion detection techniques are the last line of defenses against computer attacks behind secure network architecture design, firewalls, and personal screening. Despite the plethora of intrusion prevention techniques available, attacks against computer systems are still successful. Thus, intrusion detection systems (IDSs) play a vital role in network security. Symantec in a recent report uncovered that the number of fishing attacks targeted at stealing confidential information such as credit card numbers, passwords, and other financial information are on the rise, going from 9 million attacks in June2013 to over 33 millions in less than a year. One solution to this is the use of network intrusion detection systems (NIDS) that detect attacks by observing various network activities. It is therefore crucial that such systems are accurate in identifying attacks, quick to train and generate as few false positives as possible. Internet has rapidly become one of the main communication methods in our society. Various types of internet application and usage are available more and more. Increasing usages of network applications also increase security risks to internet users, to prevent unwanted or dangerous threats.

1.1 INTRUSION DETECTION

An Intrusion Detection System (IDS) inspects the activities in a system for suspicious behavior or patterns that may indicate system attack or misuse. There are two main categories of intrusion detection techniques; Anomaly detection and Misuse detection. The former analyses the information gathered and compares it to a defined baseline of what is seen as "normal" service behavior, so it has the ability to learn how to detect network attacks that are currently unknown. Misuse Detection is based on signatures for known attacks, so it is only as good as the database of attack signatures that it uses for comparison. Misuse detection has low false positive rate, but cannot detect novel attacks. However, anomaly detection can detect unknown attacks, but has high false positive rate.

An intrusion detection system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches. In other words, intrusion detection is the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a system/network. Traditionally, intrusion detection systems have been classified as a signature detection system, an anomaly detection system or a hybrid/compound detection system. A signature detection system identifies patterns of traffic or application data presumed to be malicious while anomaly detection systems compare activities against a "normal" baseline. On the other hand, a hybrid intrusion detection system combines the techniques of the two approaches. Both signature detection and anomaly detection systems have their share of advantages and drawbacks. The primary advantage of signature detection is that known attacks can be detected fairly reliably with a low false positive rate. The major drawback of the signature detection approach is that such systems typically require a signature to be defined for all of the possible attacks that an attacker may launch against a network. Anomaly detection systems have two major advantages over signature based intrusion detection systems. The first advantage that differentiates anomaly detection systems from signature detection systems is their ability to detect unknown attacks as well as "zero days" attacks. This advantage is because of the ability of anomaly detection systems to model the normal operation of a system/network and detect deviations from them. A second advantage of anomaly detection systems is that the aforementioned profiles of normal activity are customized for every system, application and/or network, and therefore making it very difficult for an attacker to know with certainty what activities it can carry out without getting detected. However, the anomaly detection approach has its share of drawbacks as well.

Types of intrusion detection systems there are two types of intrusion detection systems that employ one or both of the intrusion detection methods outlined above. Host-based systems base their decisions on information obtained from a single host (usually audit trails), while network-based intrusion detection systems obtain data by monitoring the traffic in the network to which the hosts are connected. An intrusion detection system dynamically monitors the events taking place in a monitored system, and decides whether these events are symptomatic of an attack or constitute a legitimate use of the system. Figure depicts the organization of IDS where solid arrows indicate data/control flow while dotted arrows indicate a response to intrusive activities.

In general, IDSs fall into two categories according to the detection methods they employ, namely (i) misuse detection and (ii) anomaly detection. In addition to the detection method, there are other characteristics one can use to classify IDSs, as shown in

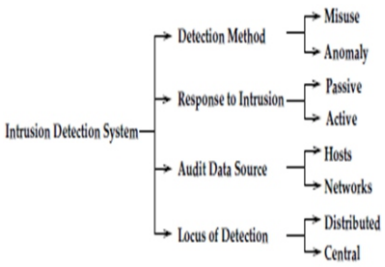

Figure 1.1.2 Characteristics of intrusion detection systems

1.2 NETWORK-BASED IDS

Network-based IDSs are the most common type of commercial product offering. These mechanisms detect attacks by capturing and analyzing network packets. Listening on a network backbone, single network-based IDS can monitor a large amount of information. Network-based IDSs usually consist of a set of single-purpose hosts that "sniff" or capture network traffic in various parts of a network and report attacks to a single management console. Because no other applications run on the hosts that are used by a network based IDS, they can be secured against attack. Many of them have "stealth" modes, which make it extremely difficult for an attacker to detect their presence and to locate them. With the proliferation of computer networks, more and more individual hosts are connected into local area networks and/or wide area networks. However, the hosts, as well as the networks, are exposed to intrusions due to the vulnerabilities of network devices and network protocols. The TCP/ IP protocol can be also exploited by network intrusions such as IP spoofing, port scanning, and so on. Therefore, network-based intrusion detection has become important and is designed to protect a computer network as well as all of its hosts. The installation of a network-based intrusion detection system can also decrease the burden of the intrusion detection task on every individual host.

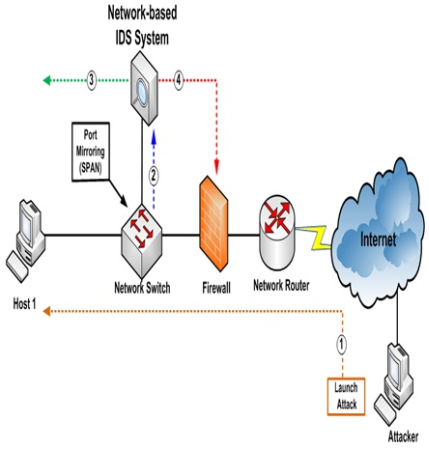

Figure 1.2.1 Network based IDS

Advantages- A few well-placed network-based IDSs can monitor a large network. The deployment of network based IDSs has little impact on the performance of an existing network. Network-based IDSs are typically passive devices that listen on a network wire without interfering with normal network operation. Thus, usually, it is easy to retrofit a network to include network-based IDSs with a minimal installation effort. Network-based IDSs can be made very secure against attack and can even be made invisible to many attackers.

Disadvantages- Network-based IDSs may have difficulty processing all packets in a large or busy network. Therefore, such mechanisms may fail to recognize an attack that is launched during periods of high traffic. IDSs that are completely implemented in hardware are much faster than those that have been totally realized in software. In addition, the need to analyze packets quickly forces vendors to try and detect attacks with as few computing resources as possible. This may reduce detection effectiveness.

1.3 HOST-BASED IDS

A generic intrusion detection model proposed by Denning is a rule-based pattern matching system in which the intrusion detection tasks are conducted by checking the similarity between the current audit record and the corresponding profiles. If the current audit record deviates from the normal patterns, it will be considered an anomaly. Several IDSs were developed using profile and rule based approaches to identify intrusive activity. Host-based IDSs analyze the activity on a particular computer Thus; they must collect information from the host they are monitoring. This allows IDS to analyze activities on the host at a very fine granularity and to determine exactly which processes and users are performing malicious activities on the operating system. Some host-based IDSs simplify the administration of a set of hosts by having the administration functions and attack reports centralized at a single IT security console. Others generate messages that are compatible with network administration systems.

Advantages- Host-based IDSs can detect attacks that are not detectable by a network based IDS because this type has a view of events that are local to a host. Host-based IDSs can operate in a network that is using encryption when the encrypted information is decrypted on (or before) reaching the host that is being monitored. Host based IDSs can operate in switched networks.

Disadvantages- The collection mechanisms must usually be installed and maintained on every host that is to be monitored. Because portions of these systems reside on the host that is being attacked, host-based IDSs may be attacked and disabled by a clever attacker. Host-based IDSs are not well-suited for detecting network scans of all the hosts in a network because the IDS at each host see only the network packets that the host receives. Host-based IDSs frequently have difficulty detecting and operating in the face of denial-of-service attacks. Host based IDSs use the computing resources of the hosts they are monitoring.

1.4 APPLICATION-BASED IDS

Application based IDSs monitor the events that are transpiring within an application. They often detect attacks by analyzing the application's log files. By interfacing with an application directly and having significant domain or application knowledge, application based IDSs are more likely to have a more discerning or fine-grained view of suspicious activity in the application.

Advantages- Application based IDSs can monitor activity at a very fine granularity, which allows them, often, to track unauthorized activity to individual users. Application based IDSs can work in encrypted environments, because they interface with the application that may be performing encryption.

Disadvantages- Application based IDSs may be more vulnerable than host based IDSs to being attacked and disabled because they run as an application on the host that they are monitoring.

1.5 NIDS

A network intrusion detection system (NIDS) is an IDS that aims to detect malicious activities such as denial of service (DoS) attacks and port scans. A DoS attack or distributed denial of service (DDoS) attack is an attempt to make a computer or network resource unavailable to its intended user. It is usually achieved by sending a huge number of requests from a single computer (DoS) or multiple computers (DDoS). The main targets of these types of attack are companies which heavily rely on online services provided through websites. What makes detection of DDoS attacks difficult is their use of actual source IP address and simulation of normal flows. They work by flooding traffic or using periodically low-rate attack flows on the victim's machine or network. Furthermore, at the beginning of an attack, since traffic fluctuations are kept low, it is difficult to recognize them.

1. RELATED WORK

In this dissertation proposed a feature selection and reduction based intrusion detection system. The process of feature reduction and selection improved the detection and classification ratio of intrusion detection system. The feature selection process used for find common feature for attacker participant and feature reduction process used for unwanted feature those who are not involved in attack and normal communication. For the reduction of feature used DCA function. In the process of feature reduction various algorithm are used such algorithm are principle of component analysis and neural network. The reduction process used PCA method this method is static reduction technique, reduces only fixed number of attribute. The fixed number of feature reduction process not justify the value of feature it directly

reduces the feature. On the consideration of computational time feature reduction is also an important aspects, the reduces feature increase the processing of detection ratio. Many methods have been proposed in the last decades on the designs of IDSs based on feature reduction technique. For example silakari and shaliendra [4] proposed a generic framework for intrusion detection based on feature reduction and ensemble based classifier. On the other hand genetic algorithm is directly applied for classification in the work of Li [5]. Jain and Upendra [6] applied information gain based feature reduction for intrusion detection. They used KDDCUP'99 dataset for comparing four machine learning algorithms and they found that J48 classifier outperforms over Bayes Net, OneR and NB classifiers. Muda et al. [7] also used KDDCUP'99 dataset for evaluating their K-Means and Naive Bayes based learning approach to carry out intrusion detection. Support Vector Machine (SVM) based IDS with Principal Component Analysis (PCA) dimension reduction is presented for intrusion detection in [8,9]. Z. Xue-qin et al. [10] proposed SVM IDS with Fisher score for feature selection. Some author proposed GS algorithm for feature selection. GS is attribute based classification technique in decision tree. The selection of attribute in GS algorithm is entropy of information and gain of information. The increasing the sample selection area used radial biases function in GS algorithm. The continuity of chapter further discusses feature selection feature reduction, DCA function and finally discuss proposed algorithm.

2. FEATURES EXTRACTION

Intrusion detection systems can either have single variable approach or a multi-variable approach to detect intrusions depending on the algorithm used. In the single variable approach a single variable of the system is analyzed. This can be, for example, port number, CPU usage of a local machine etc. In multi-variable approach a combination of several features and their inter-correlations are analyzed. [10] In addition based on the method the way in which features are chosen for the IDS can be divided into two groups; into feature selection and feature reduction.

3.1 FEATURE SELECTION

In the feature selection method the features are either picked manually from the data monitored or by using a specific feature selection tool. The most suitable features are selected by handpicking from the feature spectrum based on the prior knowledge about the environment that the IDS are monitoring. For example features that can distinguish certain type of traffic from the traffic flows are picked for the network traffic model training. The idea behind the feature selection tools is to reduce the amount of features into a feasible subset of features that do not correlate with each other. Examples of feature selection tools are Bayesian networks (BN) and classification and regression tree (CART). Bayesian network is a probabilistic graphical model that represents the probabilistic relationships between features. [36] CART is a technique that uses tree-building algorithms to construct a tree-like if-then prediction patterns that can be used to determine different classes from the dataset. Feature selection process is illustrated in Figure 4.1 On the left there are the features (F0…FN) that are available from the data monitored, which is, for example, from network traffic. On the right side is the output (F0...FM) of the selection tool. The number of features in the output varies based on the selection tool used and the inter-correlation of features in the input. Following the basic principles of feature analysis the number of features in the output (M in Figure4.1) is in most of the cases less than the number of features in the input (N in Figure 4.1). However, it is possible that the output is equal to the input.

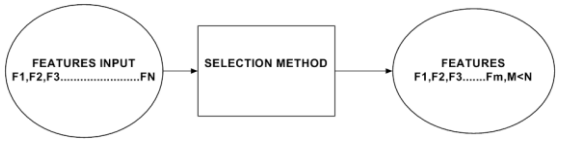

Figure 3.1.1: feature selection process in feature variable.

3.2 FEATURE REDUCTION

In the feature reduction method a new set of features is extracted based on the features available from the data monitored such as network traffic data. The basic idea behind feature reduction method is to reduce the total number of features used in the network traffic model training. In general feature reduction means that during a certain period of time a number of different features are monitored and a new set of features are then calculated from this monitored data. For example the feature reduction tool could monitor number of packets to a specific destination, within a certain period of time. Then, once the monitoring period is over, a new feature (number of packets to that destination) is available for the IDS. Another example of a feature reduction method is a principal component analysis (PCA). PCA is an algorithm that checks and converts the data set for all the correlated variables into a set of uncorrelated variables, also known as principal components. [13] Feature reduction process is illustrated in Figure 4.2. On the left there are the features (F0…FN) that are available from the monitored data, for example, from the network traffic. On the right is the output (V0…VN) of the reduction tool. The number of features in the output usually is less than in the input but it might as well be the same. The new features (V0…VN), can be calculated based on a single feature or a combination of multiple features (F0…FN).

Figure 3.2.1: process of feature reduction.

The method used to monitor network traffic is to use flow-based data. There are many advantages in using flow data instead of packet data. The major advantage comes from the reduced need of storage space for the data. Network flows requires a one tenth of the original packet-based data which is a huge difference. Another advantage is that the flow data does not contain payload data at all. So the user privacy is no longer a problem. Also the traffic volumes such as the number of packets and bytes between destinations are easily extractable from the flow data so extra calculation is not therefore needed. The disadvantage with this data is of course the loss of individual packet information such as the size of the packet, structure of the packets in order to detect malformed ones etc.

The network traffic generate huge amount of traffic data in every few seconds, the processing of these data for firewall and intrusion detection system is very complex. The complex raw data is not formatted and standard relation for the process of filtration and classification. These original raw data process through KDD data mining tools and converted into connection. A connection justifies the sequence of packet form source to distention. The process of conversion performs by Paxson algorithm. Finally get 41 features. These feature divided into four categories [3].

1. Basic Features: - These features are captured from packet headers only and without analyzing payload. Features 1 to 8 are in this category.
2. Content Features: - In this category original TCP packets analyzed with assistance of domain knowledge. An example of this category is number of "hot" indicators.
3. Time-based Traffic Features: - for capturing these types of features a window of 2 second interval is defined. In this interval, some properties of packets are measured. For example number of connections to the same service as the current connection in the past two seconds.
4. Host-based Traffic Features: - In this category instead of a time based window, a number of connections are used for building the window. This category is designed so that attacks longer than 2 second can be detected.

The processing of feature and description of feature discuss in table 1,2 and 3 according to their description and data types.

Feature selection is an important data processing step earlier to applying a detection algorithm. It is a process of determining whether a feature is relevant or not for a particular algorithm. Using effective features to propose algorithm not only can reduce the data size but also can improve the performance of the detection and enhanced the performance of intrusion detection system. One of the major problems in feature reduction is to select effective attributes that have the best discrimination ability between the groups. There are two common approaches for feature reduction: Wrapper and Filter. A Wrapper method selects feature subset based on the performance of the learning algorithm that is going to be used. Wrapper method is totally dependent on the learning algorithm. On the other hand Filter methods evaluate features according to statistical characteristics of the data only without

the involvement of any learning algorithm. The wrapper approach is generally considered to produce better feature subsets but runs much more slowly and requires more computing resource than a filter method.

3.3 DCAALGORITHM

The Dendrite Cell Algorithm (DCA) is not a classification algorithm, but shares properties with certain filtering techniques. It provides information representing how anomalous a group of antigen is, not simply if a data item is anomalous or not. This is achieved through the generation of an anomaly coefficient value, termed the MCAV – mature context antigen value [11]. The labeling of antigen data with a mature context antigen value coefficient is performed through correlating a time-series of input signals with a group of antigen. The signals used are pre- normalized and pre-categorized data sources, which reflect the behavior of the system being monitored. The signal categorization represents the degree of normal and abnormal data and categorized into mainly three categories:

PAMP: A measure that increases in value as the observation of anomalous behavior. It is a confident indicator of anomaly, which usually presented as signatures of the events that can definitely cause damage to the system.

Danger: A measure indicates a potential abnormality. The value increases as the confidence of the monitored system being in abnormal status increases accordingly.

Safe: A measure that increases value in conjunction with observed normal behavior. This is a confident indicator of normal, predictable or steady-state system behavior.

The algorithm steps given below
Input : S = set of data items to be labeled safe or dangerous
Output: D = set of data items labeled classes
DBF= dendrite belief function

Begin
Create an initial population of dendrite cells (Dcs), *D*
Create a set to contain migrated DCs, *M*
For all data items in *S* do
Create a set of DCs randomly selected from *D, P*
For all DCs in *P* do
Add data item to DCs collected list
Update danger, PAMP and safe signal concentrations
Update concentrations of output cytokines
Migrate the DC from *D* to *M* and create a new DC in *D* if concentration of co-stimulatory
Molecules is above a threshold
End
End
if entropy(bad && good)
Bad=high
Good=low
Pass DBF (bad)
For all DCs in *DBF* do
Set DC to be semi-mature if output concentration of semi-mature cytokines is greater than mature cytokines,
Otherwise set as mature
end
for all data items in *S* do
Calculate number of times data item is presented by a mature DC and a semi-mature DC
Label data item a safe if presented by more than semi-mature DCs than mature DC's,
otherwise label as dangerous
Add data item to labeled set *M*
end
end

3.4 SUPPORT VECTOR MACHINE

We begin by discussing a soft margin SVM learning algorithm written by Cortes, which is sometimes called c-SVM. This SVM classifier has a slack variable and penalty function for solving non-separable problems. First, given a set of points $x^i \in R^a$, i=1,……,l and each point x_i belongs to either of two classes with the label $yi \in \{+1,-1\}$.These two classes can be applied to anomaly attack detection with the positive class representing normal and negative class representing abnormal. Suppose there exists a hyper-plane $wTx_i + b = 0$ that separates the positive examples from the negative examples. That is, all the training examples satisfy:

$$W^T x_i + b \geq +1 \text{ for all } x_i \in P$$
$$W^T x_i + b \geq -1 \text{ for all } x_i \in P \quad (1)$$

w^T s an adjustable weight vector, x_i is the input vector and is the bias term.

Equivalently:

$$y_i \cdot (W^T . x_i - b) \geq 1 \forall i, = 1 \ldots N \quad (2)$$

In this case, we say the set is linearly separable[14].

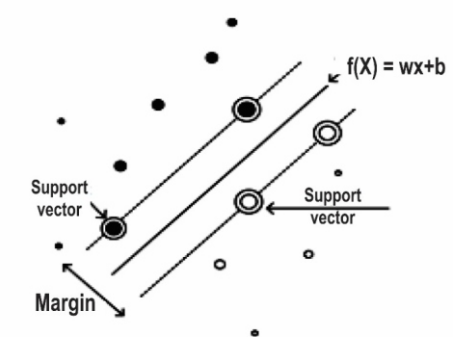

Figure 3.4.1: Separable hyper-plane between two datasets

3.5 PCNN NETWORK MODEL

In this section, we discuss model of pulse coupled neural network for intrusion detection. Pulse Coupled Neural Network (PCNN), also called the third-generation artificial neural network, is the neural network mathematic model deriving from synchronous pulses burst phenomenon in the visual cortex of mammals [23].It is based on Eckhorn's model, and derives from the phenomena of synchronous pulse bursts in mammals' (cats, monkeys, etc.) visual cortex When PCNN is used in intrusion data processing; it is a monolayer two dimensional array of laterally linked neurons. The number of neurons in the network is equal to that of data in the input network file. One-to-one correspondence exists between intrusion data and neurons. Each value is connected to a unique neuron and each neuron relates to its surrounding neurons.

Where Sij is external input stimulation, i.e. the intensity of the (i,j) value in the matrix formed by intrusion data values. Fij is feedback input, Lij, Uij, Yij and θij are linking input, internal activity, pulse output and dynamic threshold, respectively. w is synaptic weight matrix, Vθ is amplitude constant, αθ is the time decay constant of dynamic threshold, β is linking constant, and n is the iteration number of times.

The algorithm description
In order to give a more accurate description to the incomplete and uncertain problems which may appear in intrusion detection, and improve the effect of intrusion data processing, we come up with an intrusion detection algorithm based on PCNN time matrix and DCA indiscernibility relation in this dissertation.

There is certain correlation between each value's intensity and that of its neighborhood. Generally, if one value is polluted by intrusion , the correlation will be destroyed. Therefore, we can judge whether a value is noisy depending on PCNN time matrix. The method is: If the value of element in time matrix is different from its neighborhood, then the corresponding intrusion data value is noisy.

In this algorithm, we first adopt PCNN time matrix to detect intrusion, apply indiscernibility relation to partition original intrusion data's roughly, then intrusion using the intrusion reduction method based on PCNN, complete sub-intrusion data's, and finally enhance the intrusion data's. When enhancing the intrusion data, we adopt the following method: to the bright sub-intrusion data, histogram exponential transformation is used to make its histogram exponential distributing, dynamic range compressed, and the contrast of bright and dark areas be controllable; histogram-equalize the dark sub-intrusion data, and the result is that the histogram of object area becomes smooth, the intrusion data is much more clearer, more details are

preserved, and the processed intrusion data is convenient for subsequent processing. Simulation results indicate that the algorithm not can only enhance intrusion data commendably, but also can restrain intrusion efficiently. In many cases, for the gray intrusion data's, it is likely that their bright regions are background while dark regions are objects because of low illumination, low contrast between objects and background, and intrusion pollution. To the question, special detection algorithm is needed. The intrusion detection algorithm based on PCNN time matrix and Rough Set indiscernibility relation, a nonlinear intensity transformation, can enhance the detail information in dark areas efficiently, increase intrusion data's' contrast, and is very useful to the intrusion data's with plentiful information in low gray levels. Thereby, the algorithm proposed in this paper is of significant application value for the low contrast intrusion data's degraded by intrusion.

Step 1: Partition the original data to get sub data, i.e. apply the indiscernibility relation in DCA to partition the original intrusion data according to condition attribute C. And then determine which value sets need detection.

Secondly, partition the intrusion data according to intrusion attributes c2. Let y represent a noisy value detected by PCNN, then equivalence relation Rc1 can be defined as: all the noisy values are Rc2 indiscernible. Rc2(y) represents the set composed of those values and its supplementary represents the set composed of the values without intrusion.

Step 2: Intrusion data reduction.
Here we use our intrusion reduction algorithm based on PCNN proposed in reference. Slide a window matrix K (3×3, each element is one) on time matrix T, determine the firing time of the neurons inside the window, and choose proper subsequent operation to process the corresponding values. 1) If the element value in the center of the window is the maximum or minimum, then replace the corresponding value's intensity of the intrusion data by median filtering result; 2) the rest values' intensities remain unchanged

4. PROPOSED METHODOLOGY

In this section described a proposed method for improved DCA algorithm for feature reduction come classification technique. The huge amount of feature process through our sample selection process, the sample selection process used correlation factor for estimated feature value for reduction process. The radial biases function (PCNN) is Gaussian nature. The nature of mixture data correlation of attribute used in DCA algorithm. The combination of PCNN and DCA perform well feature reduction cum classification process over intrusion data. The PCNN [14] function incases the size of sample selection. The incasing size of sample selection incases the range of feature attribute of intruder data. PCNN function is creating for sample selection for reduces and unreduced categories data sample for dealing out of DCA classification. The input processing of training phase is data sampling technique for classifier. Single layer PCNN networks can potentially learn virtually any input output relationship; PCNN networks with single layers might learn complex relationships more quickly. The function ne DCA creates forward networks. The network-layer network also has connections from the input to all cascaded layers. The additional connections might improve the speed at which the network learns the desired relationship. PCNN artificial intelligence model is similar to feed-forward back-propagation neural network in using the back-propagation algorithm for weights updating, but the main indication of this network is that each layer of neurons related to all previous layer of neurons. The process of feature reduction and classification steps given below

1. input the dataset
2. estimate the feature correlation attribute as

$$Rel(a,b) = \frac{cov(a,b)}{\sqrt{var(a) \times var(b)}}$$

Here a and b the feature attribute of input data

3. the estimated correlation coefficient data passes through PCNN function as

$$x(t) = w0 + \sum_{j=1}^{\text{total data}} wj \exp\left(\frac{-(\text{total} - xj)}{\sigma^2}\right)$$

4. create the relative feature difference value

$$Rc = \sum_{k=1}^{r} \sum_{i=1}^{m} (hi - h)(eik - et)$$

5. After sampling of feature data get reduces set of feature attribute of feature matrix.
6. generate feature attribute of each matrix
7. compute the PAM of feature attribute for the similar data
8. $PAM(D) = -\sum_{i=1}^{N} pi \log pi \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1$
9. Compute reduces value

$$CR(v) = \sum_{j=1}^{N} Pj[pi \log pi] \ldots\ldots\ldots\ldots (2)$$

10. compute the reduces attribute

A(v) =PAM (D)-CR (v)

11. call PCNN netowk
12. data are classified
13. estimate the classification ratio
14. Exit

5. SIMULATION RESULT ANALYSIS

No. of attribute reduce	Method	PRECISION	RECALL	ACCURACY
2	SVM	97.958729	96.958729	99.958729
	DCA-PCNN	98.958731	97.958731	99.958731
5	SVM	78.265989	77.265989	80.265989
	DCA-PCNN	82.870988	83.870988	87.870988
7	SVM	80.870988	79.870988	82.870988
	DCA-PCNN	98.940127	97.940127	99.940127

Table 5.1: Comparative resultant with respect to number of reduce attribute(2, 5, 7) using SVM and DCA-PCNN method for precision, recall and accuracy.

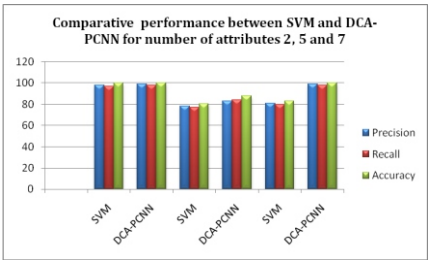

Figure 5.1: Comparative performance between SVM and DCA-PCNN method for precision, recall and accuracy.

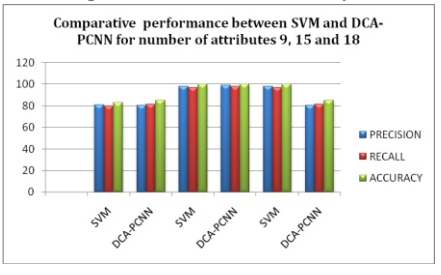

Figure 5.2: Comparative performance between SVM and DCA-PCNN method for precision, recall and accuracy.

6. CONCLUSIONS

A feature based intrusion data classification technique. The reduces feature improved the classification of intrusion data. The reduction process of feature attribute performs by PCNN function along with feature correlation factor. The proposed method work as feature reducers and classification technique, from the reduction of feature attribute also decrease the execution time of classification. The decrease time increase the performance of intrusion detection system. Our experimental process gets some standard attribute set of intrusion file such as pot_type, service, sa_srv_rate, dst_host_count, dst_host_sa_srv_rate. These feature attribute are most important attribute in domain of traffic area. The classification rate in these attribute achieved 98 %.

Reduction computational time of feature selection process is main objective. Because of this consumed time of each algorithm with different reject threshold measured. As evaluation result shows, although FFR cannot defeat other methodologies in accuracy of

classification and accuracy didn't changed very much, but in speed FFR outperformed all other feature selection method with great differences. We used DCA classifier for developing efficient and effective IDS. For improving the detection rate of the minority classes in imbalanced training dataset we used standard sampling and we picked up all of the important features of the minority class using the minority classes attack mode.

7. SUGGESTION FOR FUTURE WORK

The proposed algorithm is a combination of feature selection and feature reduction for intrusion detection system. The feature selection and reduction both improved the performance of classification algorithm, but it not achieved the classification ratio 100%. The process of data sampling improved the reduction process and improved the classification ratio up to 100%. The sampling process design as mixed sampler corresponding to the nature of network traffic data, the network traffic data is mixed data type some are continuous and discrete.

ACKNOWLEDGEMENT:

I take this opportunity to thanks Prof. AISHWARYA MISHRA, for accepting me to work under their valuable guidance, closely supervising this work over the past few months and offering many innovative idea and helpful suggestions, valuable advice and support, inspite of their busy schedule they have really been an inspirations and driving force for me. They have constantly enriched my raw ideas with their experience and knowledge.

REFERENCES:

[1] Shafigh Parsazad, Ehsan Saboori, Amin Allahyar "Fast Feature Reduction in Intrusion Detection Datasets" MIPRO 2012, Pp 1023-1029.

[2] Abebe Tesfahun, D. Lalitha Bhaskari "Intrusion Detection using Random Forests Classifier with SMOTE and Feature Reduction" International Conference on Cloud & Ubiquitous Computing & Emerging Technologies, 2013. Pp 127-132.

[3] Hachmi Fatma, Limam Mohamed "A two-stage technique to improve intrusion detection systems based on data mining algorithms" IEEE, 2013. Pp 1-6.

[4] Shailendra Singh, Sanjay Silakari "An Ensemble Approach for Cyber Attack Detection System: A Generic Framework" 14th ACIS, IEEE 2013.

[5] Li, "Using Genetic Algorithm for Network Intrusion Detection" Proc. the United States Department of Energy Cyber Security Group 2004 Training Conference, May 2004.

[6] Jain , Upendra "An Efficient intrusion detection based on Decision Tree Classifier using feature Reduction", International Journal of scientific and research Publications , Vol. 2, Jan. 2012.

[7] Dewan Md. Farid, Jerome Darmont, Nouria Harbi, Nguyen Huu Hoa, Mohammad Zahidur Rahman "Adaptive Network Intrusion Detection Learning: Attribute Selection and Classification" 2008. Pp 1-5.

[8] Gary Stein, Bing Chen, Annie S. Wu, Kien A. Hua "Decision Tree Classifier For Network Intrusion Detection With GA-based Feature Selection" 2556. Pp 1-6.

[9] Ritu Ranjani Singh a, Prof. Neetesh Gupta "To Reduce the False Alarm in Intrusion Detection System using self Organizing Map" in International journal of Computer Science and its Applications.

[10] Z. Xue-qin, G. Chun-hua, L. Jia-jin "Intrusion detection system based on feature selection and support vector machine" Proc. First International Conference on Communications and Networking in China (ChinaCom '06), Oct. 2006.