A Review of Cyber Attack Classification Technique Based on Data Mining and Neural Network Approach

Bhavna Dharamkar[1], Rajni Ranjan Singh[2]
M.Tech Scholar[1], Department of Computer Science & Engg, VNS, Bhopal, INDIA
Astt. Professor[2], Department of Computer Science & Engg, VNS, Bhopal, INDIA

Abstract

Cyber attack detection and classification is major challenge for web and network security. The increasing data traffic in network and web invites multiple cyber attack. The dynamic nature and large number of attribute of cyber data faced a problem of detection and prevention. In current research trend various method and framework are proposed by different authors. These framework and proposed method is based on data mining and neural network approach. Data mining offers various techniques such as clustering, classification, rule generation and temporal event mining; these techniques are very efficient for detection process of cyber attack. The application of neural network in cyber attack classification use as feature reduction technique. Feature reduction is very important task in cyber attack classification; because the cyber attack data consists of huge amount of features. This paper presents various method of cyber attack detection and classification technique based on data mining and neural network approach along with IDS evaluation criteria and dataset used for validated of IDS is also discussed here.

Keywords: - cyber attack, data mining, neural network and KDDCUP99

I. INTRODUCTION

The efficiency and data integrity of cyber data are major area of research in network security and cyber security. The integrity of data compromised with current cyber attack. The current cyber attack creates illegal authorization and traffic for denial of service. Cyber security is defined as the protection of cyber components against threats to discretion, reliability, and Accessibility[1]. Privacy means that data is disclosed only according to rule, reliability means that data is not cracked or tainted and that the network performs properly, availability means that network services are available when they are needed. Cyber attack detection system inspects all inside and outside network movement and identifies mistrustful patterns that may point to a network or system attack from someone attempting to break into or compromise a network[4]. In cyber attack detection, we generally deal with a large amount of data collected from cyber agent to make a decision on the current situation of the network. Different types of attacks may have different effects on the operations of a cyber network. As a result, the data that need to be collected from cyber agent vary from one kind of attacks to the other. For example, denial of service attacks aim at flooding the computing or memory resources of target systems and preventing them from providing services to legitimate users.

The most complex and advanced attacks are beleaguered attacks which are specifically aimed at companies or governments to reach a predetermined aim.The Aurora trojan was aimed at obtaining intellectual property of large corporations. The Stuxnet worm was aimed at disruption of industrial systems in Iran[7]. The Diginotar hack was aimed at generating rogue signed certificates with the goal of spying on traffic to websites. Data mining algorithms that classify the attacks must do it accurately. It must reduce unclassified attack to improve accuracy. Classification errors can be reduced by various algorithms like ADA-boost, bagging and wagging.[4] proposes multi-boosting technique, which is a combination of ADA-boost and wagging techniques, to reduce classification errors. When compared with other techniques multi-boosting performs better in reducing classification errors in classification algorithms. Classification and clustering techniques in data mining are useful for a wide variety of real time applications dealing with large amount of data. They detect attacks using the data mining techniques classification and clustering algorithms. Classification techniques analyze and categorize the data into known classes. Each data sample is labeled with a known class label. Clustering is a process of grouping objects resulting into set of clusters such that similar objects are members of the same cluster and dissimilar objects belong to different clusters. Classification techniques are examples of supervised learning and clustering techniques are examples of unsupervised learning. An artificial neural network consists of connected set of processing units. The connections have weights that determine how one unit will affect other. Subset of such units act as input nodes, output nodes and remaining nodes constitute the hidden layer. By assigning activation to each of the input node and allowing them to propagate through the hidden layer nodes to the output nodes, neural network performs a functional mapping from input values to output values. The mapping is stored in terms of weight over connection. This paper is divided into five sections. Section-I gives the introduction of cyber attack and data mining. Section-II gives the related of cyber attack. Data mining and

neural network in III. In section-IV evaluation and performance analysis and finally discuss conclusion and future work in section V.

II. RELATED WORK

In this section described the related work of cyber attack classification with data mining and neural network approach. The detection and classification of cyber attack faced a problem of false detection of cyber attack data. The data mining and neural network play an important role in cyber attack classification. The process improved the rate of classification. Some work in the field of attack classification discuss here.

Clustering: The process of grouping a set of physical or abstract objects into classes of similar objects is called clustering. A cluster is a collection of data objects that are similar to one another within the same cluster and are dissimilar to the objects in other clusters. A cluster of data objects can be treated collectively as one group and so may be considered as a form of data compression.

a) **X.Li et al. [2] :** authors proposed a work in level of hardware in from of Data storage devices may additionally be included in the network to support networked storage, local fault diagnosis, and distributed decision making. There is a communication gateway in each community network. It manages the communication among the network elements, performs data aggregation, and bridges the bottom and top layers to allow data exchange.

b) Vineet Richhariya, Dr J.L.Rana,Dr R.C.Jain, Dr. R.K.Pandey [14] : authors Proposed a model in which first dimension reduction technique is applied. Secondly on reduced data set fuzzification of feature values is done to get simpler range. Thirdly combination of clustering and naïve based approach, on the large test dataset applied. Obtained results are analyzed on detection rate, false positive rate and precision rate. Fuzzy logic based discretization of the dataset has helped to improve the training data representation, and performs well in terms of detecting attacks faster and with reasonable reduction in false alarm rate.

c) **S. Staniford-Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, C. Wee, R. Yip, and D. Zerkle [15] :** authors proposed a AFID is a framework for a distributed intrusion detection system that employs autonomous agents at the lowest level for data collection and analysis and transceivers and monitors
at the higher levels of the hierarchy for controlling the agents and obtaining a global view of activities

Classification: classification is an effective means for distinguishing groups or classes of objects; it requires the often costly collection and labelling of a large set of training tuples or patterns which the classifier uses to model each group. It is often more desirable to proceed in the reverse direction Typical classify models have the linear regression model, the decision tree model, the model based on rule and the neural network model

d) Shailendra Singh, Sanjay Silakari [1] : authors proposed a model of Cyber Attack Detection System and its generic framework, which has been found to perform well for all the classes of attack. In this framework authors used four tiers architecture to enhance the adaptability of the cyber attack detection system. The first tier is dedicated to data collection and preprocessing of the data. The Second tier is meant for the feature extraction technique, third tier is dedicated to classification of cyber attacks and fourth tier is dedicated to user interface for reporting the events.

e) **Hoa Dinh Nguyen, Qi Cheng [4]** : authors proposed a new feature selection algorithm for distributed cyber attack detection and classification. Different types of attacks together with the normal condition of the network are modeled as different classes of the network data. Binary classifiers are used at local sensors to distinguish each class from the rest. The proposed algorithm outputs for each local binary classifier a set of pair wise feature subsets which are selected for discriminating that particular class from each of the rest classes. This is different from conventional feature selection algorithms, which select a unique feature subset for each local binary classifier. The new feature selection method is shown to be more capable of selecting all relevant features, thus to improve the detection and classification accuracy.

f) **Bimal Kumar Mishra, Hemraj Saini [5] :** authors used classification approach of cyber attack which uses characteristics metrics and game theoretic approach to classify the attacks to their closest category. The standard weights of the metrics are used as the base line to classify the cyber attacks in the proper category. The approach is simple and extendible; as new characters of the newly identified attacks can be added to the attack characteristic metrics and the corresponding unique weight to the character are assigned by the proposed formula. Besides this, the proposed approach clearly represents the cause effect relationship for all possible attacks which helps us to find the appropriate solution to restrict them in the Internet.

g**) Haitao Du, Christopher Murphy, Jordan Bean , Shanchieh Jay Yang [7] :** In this paper authors used a statically theory of Mean that the track length and the time interval between two observations can be very different, potentially by orders of magnitude. These differences, along with the various other uncharted features of cyber attack tracks present an exciting and critical new challenge. This paper will first illustrate the non-uniformity and cyber track features, as well as the pros and cons of the traditional K-means clustering algorithm.

h) **Dewan Md.Farid ,Nouria Harbi,Emna Bahri,Mohammad Zahidur Rahman,Chowdhury Mfizur Rahman [9] :** In this paper authors proposed a new learning algorithm for anomaly based network intrusion detection system using decision tree algorithm that

distinguishes attacks from normal behaviors and identifies different types of intrusions.

i) **Shailendra Singh, Sanjay Agarwal [12]** : In this paper authors proposed an improved Support Vector Machine (iSVM) algorithm for classification of cyber attack dataset. Result shows that iSVM gives 100% detection accuracy for Normal and Denial of Service (DOS) classes and comparable to false alarm rate, training, and testing times. The performance of traditional SVM is enhanced in this work by modifying Gaussian kernel to enlarge the spatial resolution around the margin by a conformal mapping, so that the separability between attack classes is increased. It is based on the Riemannian geometrical structure induced by the kernel function.

III DATA MINING AND NEURAL NETWORK

Data mining and neural network play an important role in cyber attack classification. Data mining offer various technique for classification such as KNN, decision tree, SVM and rule based classification; all these classification promise the result of classification. The result of classification suffered a problem of false detection. The false detection of data mining technique is big issues in research trend. Now the minimization of false detection rate in cyber attack classification required reduction of attribute in cyber data and valid pattern of data. The artificial neural network plays an important role in feature reduction and valid pattern generation. Over the complicated structure of neural network the neural networks approach can be applied to a wide range of pattern recognition problems intrusion detection included[18]. The idea behind the application of soft computing techniques and particularly ANN in implementing cyber attack is to include an intelligent agent in the system that is capable of disclosing the latent patterns in abnormal and normal connection audit records and to generalize the patterns to new connection records of the same class[14]. And the beauty of neural networks in intrusion detection is that no signatures or even rules are needed. To simply start feeding input data concerning network or host based events to a neural network and it does the rest. Neural networks are therefore well suited to picking up new patterns of attacks readily although some learning time is required [15]. The neural networks approach has been around for a long time and if anything it is likely to become more widely used and relied on in intrusion detection in the future as reliance on signatures diminishes. Different types of Artificial Neural Network exist for various purposes such as classification, prediction, clustering, association, etc. A feed-forward ANN was the first and arguably simplest type of artificial neural network devised. In this network the information moves in only one direction forward from the input nodes through the hidden nodes (if any) and to the output nodes[16]. There are no cycles or loops in the network) with the back propagation learning algorithm is commonly used for classification problems. Cyber attack detection can be considered a classification problem in that computer and network data is classified into attack or normal use. One advantage of a feed-forward ANN for classification problems lies in its ability to learn a sophisticated nonlinear input-output function. The ANN learns signature patterns of cyber attacks and normal use activities from the training data and uses those signature patterns to classify activities in the testing data into attack or normal use[17]. Now a day's support vector machine is widely used a classification technique in cyber attack detection. The prediction of result of support vector machine is 90%. The process of grouping a set of physical or abstract objects into classes of similar objects is called clustering. A cluster is a collection of data objects that are similar to one another within the same cluster and are dissimilar to the objects in other clusters. A cluster of data objects can be treated collectively as one group and so may be considered as a form of data compression. Classification is an effective means for distinguishing groups or classes of objects; it requires the often costly collection and labeling of a large set of training tuples or patterns which the classifier uses to model each group. It is often more desirable to proceed in the reverse direction Typical classify models have the linear regression model, the decision tree model, the model based on rule and the neural network model.

Table 1 gives the description of classification and clustering technique for data mining with advantage and disadvantage.

Types	Method	Disadvantage	Advantages	Concept
Classification methods	Simple rules	Complex situation are hard to define in simple rules	Simple to use	If…then … like rules
	Neural Networks	Black box	Can handle complex relations	Mathematical model calculating output based on inputs
	Support Vector Machines	Slow on large sample sizes	Small chance at over fitting and possible to use dynamically	Classes are separated by a hyperplane by calculating support vectors to the closest points from each class
	Bayesian Networks	Cannot handle missing data well	Efficient with causal relations	Probability of events
	Decision Trees	Very hard to find optimal	Can handle numeric and text	Classification by If..then..

		solution	data types	like tree structure
	k-Nearest Neighbor	Storage intensive and susceptible to noise	Simple to implement	Distance/ density calculation between case and classes
	Hidden Markov Models	Events must be independent. (The events may not provide a probability of a following event.)	Can analyze sequences of events in which the events are not independent	The probability of a sequence of observed events is used to calculate the probability of a sequence of non-visible events.
Clustering methods	k-Means	Initial choice of parameter values Hard to find optimal solution and sensitive to cluster shape	Insensitive to noise and cluster shape Pre-classification not necessary	Clustering based on equality Clusters data into a given number of k clusters by minimizing the mean distance to a cluster center
	Self-organizing maps	Resulting model is a black box and creating a model is computational intensive	Good reduction of data feature dimensionality while maintaining relationships between the features	Neural network where output neurons are pixels of a density map and similar cases are mapped close to each other

IV EVALUATION AND PERFORMANSE ANALYSIS

In this section discuss DARPA 1999 and KDD'99 dataset Evaluation of performance of data mining and neural network algorithm for cyber attack classification; we can evaluate it practically using DARPA DATA SET AND KDD'99 cyber attack datasets [18].

In the DARPA IDS evaluation dataset, all the network traffic including the entire payload of each packet
was recorded in tcpdump format and provided for evaluation. In these evaluations, the data was in the form of sniffed network traffic, Solaris BSM audit data, Windows NT audit data (in the case of DARPA 1999) and file system snapshots and tried to identify the intrusions that had been carried out against a test network during the data-collection period. The test network consisted of a mix of real and simulated machines; background traffic was artificially generated by the real and simulated machines while the attacks were carried out against the real machines. Taking the DARPA 1999 dataset for further discussion, the dataset consists of weeks one, two and three of training data and weeks four and five of test data. In training data, the weeks one and three consist of normal traffic and week two consists of labeled attacks.

In 1998, DARPA in concert with Lincoln Laboratory at MIT launched the DARPA 1998 dataset for evaluating IDS
[16]. The DARPA 1998 dataset contains seven weeks of training and also two weeks of testing data. In total, there are 38 attacks in training data as well as in testing data. The refined version of DARPA dataset which contains only
network data (i.e. Tcpdump data) is termed as KDD dataset [17]. The Third International Knowledge Discovery and Data Mining Tools Competition were held in colligation with KDD-99, the Fifth International Conference on Knowledge Discovery and Data Mining. KDD dataset is a dataset employed for this Third International Knowledge Discovery and Data Mining Tools Competition. KDD training dataset consists of relatively 4,900,000 single connection vectors where each single connection vectors consists of 41 features and is marked as either normal or an attack, with exactly one particular attack type [18]. These features had all forms of continuous and symbolic with extensively varying ranges falling in four categories:

1. In a connection, the first category consists of the intrinsic features which comprises of the fundamental features of each individual TCP connections. Some of the features for each individual TCP connections are duration of the connection, the type of the protocol (TCP, UDP, etc.) and network service (http, telnet, etc.).

2. The content features suggested by domain knowledge are used to assess the payload of the original TCP packets, such as the number of failed login attempts.

3. Within a connection, the same host features observe the recognized connections that have the same destination host as present connection in past two seconds and the statistics related to the protocol behavior, service, etc are estimated.
4. The similar same service features scrutinize the connections that have the same service as the current connection in past two seconds.

A variety of attacks incorporated in the dataset fall into following four major categories:

a. **Denial of Service Attacks**: A denial of service attack is an attack where the attacker constructs some computing or memory resource fully occupied or unavailable to manage legitimate requirements, or reject legitimate users right to use a machine.
b. **User to Root Attacks:** User to Root exploits are a category of exploits where the attacker initiate by accessing a normal user account on the system (possibly achieved by tracking down the passwords, a dictionary attack, or social engineering) and take advantage of some susceptibility to achieve root access to the system.
c. **Remote to User Attacks:** A Remote to User attack takes place when an attacker who has the capability to send packets to a machine over a network but does not have an account on that machine, makes use of some vulnerability to achieve local access as a user of that machine.
d. **Probes:** Probing is a category of attacks where an attacker examines a network to collect information or discover well-known vulnerabilities. These network investigations are reasonably valuable for an attacker who is staging an attack in future. An attacker who has a record, of which machines and services are accessible on a given network, can make use of this information to look for fragile points.

DATASET:

MIT-DARPA dataset (IDEVAL 1999)[1] was used to train and test the performance of Intrusion Detection Sys-tems. The network traffic including the entire payload of each packet was recorded in tcpdump format and provided for evaluation. The data for the weeks one and three were used for thetraining of the anomaly detectors PHAD and ALAD and the weeks four and ¯ve were used as the test data. The DARPA 1999 test data consisted of 190 instances of 57 attacks which included 37 Probes, 63 DoS attacks, 53 R2L attacks, 37U2R/Data attacks with details on attack types given in Table 1.

Attacks present in DARPA 1999 dataset

Attack Classes	**Attack type**
Probe	portsweep, ipsweep, queso, satan, msscan, ntinfoscan, lsdomain, illegal-sni®er
DoS	apache2, smurf, neptune, dosnuke, land, pod, back, teardrop, tcpreset, syslogd, crashiis, arppoison, mailbomb, selfping, processtable, udpstorm, warezclient
R2L	dict, netcat, sendmail, imap, ncftp, xlock, xsnoop, sshtrojan, framespoof, ppmacro, guest, netbus, snmpget, ftpwrite, httptunnel, phf, named
U2R	sechole, xterm, eject, ps, nukepw, secret, perl, yaga, fdformat, ffbconfig, casesen, ntfsdos, ppmacro, loadmodule, sqlattack

Table2. Different types of attacks in DARPA 1999 dataset

In KDD99 dataset these four attack classes (DoS, U2R, R2L, and probe) are divided into 22 different attack classes that tabulated in Table I. The 1999 KDD datasets are divided into two parts: the training dataset and the testing dataset. The testing dataset contains not only known attacks from the training data but also unknown attacks. Since 1999, KDD'99 has been the most wildly used data set for the evaluation of anomaly detection methods.DARPA'98 is about 4 gigabytes of compressed raw (binary) tcp-dump data of 7 weeks of network traffic, which can be processed into about 5 million connection records, each with about 100 bytes. For each TCP/IP connection, 41 various quantitative (continuous data type) and qualitative (discrete data type) features were extracted among the 41 features, 34 features (numeric) and 7 features.

4 Main Attack Classes	22 Attack Classes
Denial of Service (DoS)	back, land, neptune, pod, smurt, teardrop
Remote to User (R2L)	ftp_write, guess_passwd, imap, multihop, phf,spy, warezclient, warezmaster
User to Root (U2R)	buffer_overflow, perl, loadmodule, rootkit
Probing(Information Gathering)	ipsweep, nmap, portsweep, satan

Table1. Different types of attacks in kdd99 dataset

To analysis the different results using some standard parameter such as Precision- Precision measures the proportion of predicted positives/negatives which are actually positive/negative. Recall -It is the proportion of actual positives/negatives which are predicted positive/negative. Accuracy-It is the proportion of the total number of prediction that were correct or it is the percentage of correctly classified instances.True positive (TP) is the attacks that are detected which are actually true attacks ,True False (TF) is the normal data and is a ctually the normal data False-negative rate (FN) is the percentage that attacks are misclassified from total number of attack records. False-positive (FP) is the percentage that normal data records are classified as attacks from total number of normal data records. Below we are showing how to calculate these parameters by the suitable formulas.

$$\text{Precision} = \frac{TP}{TP+FP}$$

$$\text{Recall} = \frac{TP}{TP+FN}$$

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

$$FPR=\frac{FP}{FP+TN} \quad , FNR=\frac{FN}{FN+TP}$$

V CONCLUSION AND FUTURE WORK

In this paper present current method of data mining and neural network of cyber attack classification, in meticulous, this paper reviews recent papers which are between 2010 and 2013. In addition, we consider a large number of data mining techniques used in the cyber attack domain for the review including clustering, classification, and ensemble technique. Regarding the comparative results of related work, found that the improvement in process of cyber attack classification still needs to be researched. The applied process of neural network approach such as RBF are more effective than other method but still suffered from problem of false classification.

REFERENCES:

[1] Shailendra Singh, Sanjay Silakari "An Ensemble Approach for Cyber Attack Detection System: A Generic Framework" 14th ACIS, IEEE 2013. Pp 79-85.

[2] X. Li et al., "Smart Community: An Internet of Things Application," IEEE Commun. Mag., vol. 49, no. 11, 2011, pp. 68–75.

[3] V. Bapuji, R. Naveen Kumar2,Dr. A. Govardhan, S.S.V.N. Sarma "Soft Computing and Artificial Intelligence Techniques for Intrusion Detection System" Vol 2, No.4, 2012, pp 24-33.

[4] Hoa Dinh Nguyen , Qi Cheng "An Efficient Feature Selection Method For Distributed Cyber Attack Detection and Classification" IEEE 2013. pp 1-6.

[5] Bimal Kumar Mishra,Hemraj Saini "Cyber Attack Classification using Game Theoretic Weighted Metrics Approach" World Applied Sciences Journal 7, 2009. Pp 206-215.

[6] Xu Li, Inria Lille, Xiaohui Liang, Xiaodong Lin, Haojin Zhu "Securing Smart Grid: Cyber Attacks,Countermeasures, and Challenges" IEEE Communications Magazine IEEE 2012. Pp 38-46.

[7] Haitao Du, Christopher Murphy, Jordan Bean, Shanchieh Jay Yang "Toward Unsupervised Classification of Non-uniform Cyber Attack Tracks" International Conference on Information Fusion 2009. Pp 1919-1925.

[8] Abhishek Jain And Ashwani Kumar Singh "Distributed Denial Of Service (Ddos) Attacks - Classification And Implications"journal of Information and Operations Management vol-3 2012. Pp 136– 140.

[9] Dewan Md. Farid, Nouria Harbi, Emna Bahri, Mohammad Zahidur Rahman, Chowdhury Mofizur Rahman "Attacks Classification in Adaptive Intrusion Detection using Decision Tree" World Academy of Science, Engineering and Technology, 2009. Pp 86-91.

[10] Chee-Wooi Ten, Govindarasu Manimaran "Cybersecurity for Critical Infrastructures:Attack and Defense Modeling "IEEE TRANSACTIONS ON SYSTEMS, vol-40 IEEE 2010. Pp 853-865.

[11] Mohammad A. Faysel , and Syed S. Haque "Towards Cyber Defense: Research in Intrusion Detection and Intrusion Prevention Systems" IJCSNS, vol-7 2010. Pp 316-325.

[12] Shailendra Singh, Sanjay Agrawal, Murtaza,A. Rizvi and Ramjeevan Singh Thakur " Improved Support Vector Machine for Cyber Attack Detection" WCECS IEEE 2011. Pp 1-6.

[13] Real-time Misuse Detection Systems, Proceedings of the IEEE on Information, 2004.

[14 Vineet Richhariya , Dr. J.L.Rana ,Dr. R.C.Jain ,Dr. R.K.Pandey" Design of Trust Model For Efficient Cyber Attack Detection on Fuzzified Large Data using Data Mining techniques" IJRCCT Vol 2, Issue 3, 2013. Pp 126-132.

[15] S. Staniford-Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, C. Wee, R. Yip, and D. Zerkle. GrIDS-a graph based intrusion detection system for large networks. In Proceedings of the 19th National Information Systems Security Conference, September 1996.

[16] Howard, J.D. "An Analysis of Security Incidents on the Internet" Doctoral Thesis. UMI
UMI Order No. GAX98-02539, Carnegie Mellon University.1998.

[17] James P. Anderson, "Computer security threat monitoring and surveillance," IEEE 2007. pp 255-261.

[18] Deepak Rathore and Anurag Jain "Design Hybrid method for intrusion detection using Ensemble cluster classification and SOM network" in International Journal of Advanced Computer Research Volume-2 Number-3 Issue-5 September-2012.