IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

An Implementation of Intrusion Detection System Based on Genetic Algorithm

Mr. Kamlesh Patel[1], Mr. Prabhakar Sharma[2]

Department of Computer Science and Engineering, Raipur Institute of Technology, Raipur (C.G.) [1, 2]

Abstract: The intrusion detection downside is turning into a difficult task attributable to the proliferation of heterogeneous networks since the raised property of systems provides larger access to outsiders and makes it easier for intruders to avoid identification. Intrusion observation systems are accustomed detect unauthorized access to a system. By This paper I am going to present a survey on intrusion detection techniques that use genetic rule approach. Currently Intrusion Detection System (IDS) that is outlined as an answer of system security is used to spot the abnormal activities during a system or network. To this point completely different approaches are utilized in intrusion detections, however regrettably any of the systems isn't entirely ideal. Hence, the hunt of improved technique goes on. During this progression, here I even have designed AN Intrusion Detection System (IDS), by applying genetic rule (GA) to expeditiously observe numerous styles of the intrusive activities among a network. The experiments and evaluations of the planned intrusion detection system are performed with the NSL KDD intrusion detection benchmark dataset. The experimental results clearly Show that the planned system achieved higher accuracy rate in distinctive whether or not the records are traditional or abnormal ones and obtained cheap detection rate.

Keywords: Intrusion Detection, Genetic Algorithm, NSL-KDD dataset.

I. INTRODUCTION

The intrusion is nothing but is an activity of intruding or the constraints of being intruded on. And this thesis includes that it is an undesirable addition. It is an illegal means not legally act of entering or taking possession of another's property or that an illegal act of entering into the system, seizing, or taking possession of another's property. The entry which is wrongful after the determination of a particular estate, made before the remainder man or reversionary has entered. An incident of unauthorized access that is taken place to data or an automatic information system .intrusion that is the mainly unauthorized act of spying, snooping, and stealing information through cyber space. Victims of cyber intrusion are those often unaware of their vulnerability.

Without security measures and controls in any place, the data may be subjected into an attack or in danger. Some of the attacks are passive; means can say that the information is already monitored. On the other hand some attacks are active, means the information is altering with intent and trying to corrupt or destroy the data or the network itself. Intrusion detection is changing into a progressively necessary technology that monitors network traffic and identifies network intrusions like abnormal network behaviours, unauthorized network access, and malicious attacks to pc systems [2]. There are a unit 2 general classes of intrusion detection systems (IDSs): misuse detection and anomaly detection Misuse sight ion systems detect intruders with legendary patterns, and anomaly detection systems establish deviations from traditional behaviours of networks and alert for dangerous unknown attacks. Some IDSs integrate each misuse and anomaly detection and kind hybrid detection systems. The IDSs also can be classified into 2 classes betting on wherever they appear for intrusions. A host-based IDS monitors activities related to a specific host, and a network-based IDS listens to network traffic. Variety of sentimental computing primarily based approaches are planned for detective work network intrusions. Soft computing refers to a gaggle of techniques that exploit the tolerance for inexactness, uncertainty, partial truth, and approximation to realize lustiness and low answer value. The principle constituents of sentimental computing area unit mathematical logic (FL), Artificial Neural Networks (ANNs), Probabilistic Reasoning (PR), and Genetic Algorithms .When we are going to use for intrusion detection, the soft computing techniques area unit typically utilized in conjunction with rule-based professional systems effort professional information , wherever the information is diagrammatical as a group of if-then rules. Despite completely different soft computing primarily based approaches having been planned, the probabilities of mistreatment the techniques for intrusion detection area unit still under-utilized. In this paper, we tend to give a Genetic algorithm based approach to network misuse detection. GA is chosen as a result of a number of its nice properties, e.g., sturdy to noise, no gradient info is needed to search out a worldwide optimum or sub-optimal answer, self-learning capabilities, etc. mistreatment GAs for network intrusion detection has tried to be a cheap approach. During this work, we tend to implement a software package supported the given approach. Now a day, security drawback becomes a serious issue thanks to great deal of use of web and ADP system. Any network attacks on a system violets integrity, confidentiality, and convenience. To decrease such AN

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

influence on a network we want intrusion detection system. There are a unit varied varieties of intrusion detection system like host primarily based IDS, Network primarily based IDS. The Host primarily based IDS run on singly on system. The Network primarily based IDS monitors' traffic on a network for any suspicious activity. Attacks types-Intrusion connected information is loosely classified in four different types of attacks [4] [6] as explained below:

1) Dos: (Denial of service): may be a category of attack wherever associate offender makes a computing code section or memory resources very busy or too full to handle legitimate request, so denying legitimate users access to a machine.
2) R2L (Unauthorized access from a distant machine): A remote to user attack may be a category wherever associate offender sends packet to a machine over a network, then exploits the machine's vulnerability to lawlessly gain native access as a user.
3) U2R (Unauthorized access to native super user (Root):U2R exploits area unit a category of attack wherever offender begin out with access to a traditional user account on the system and is in a position to use vulnerability to achieve root access to the system.
4) Inquisitor (Surveillance associated different probing):Is a category of attack wherever an offender scans a network to assemble info or realize better-known vulnerability .An offender with a map of machines and services that area unit out there on a network will use the knowledge to appear for exploits.

II. LITRATURE SURVEY

This section briefly summarizes some of the techniques for intrusion detection. However, a number of GA based IDSs are discussed in the later part of the paper in order to compare and contrast those work with our work. Different researchers have implemented GA in a different way for network intrusion detection.

Melani J Middlemiss et al. (2003) have used GA for weighted feature extraction with specific application to intrusion detection data. They have implemented a simple genetic algorithm which evolves weights for the features of data set. [18] A k-nearest neighbour classifier was used for the fitness function of GA as well as to evaluate the performance of the new weighted feature set. Performance was good and finds accuracy on fitness [18].
Wei Li (2004) presents a technique of applying GA to IDSs. After giving a brief introduction to IDS, GA and related detection techniques, he has discussed various implementation details. He has used GA to generate the classification rules which were used to classify normal network connections from anomalous connections. [21] These rules are in if {condition} then {act} form. He encoded chromosomes in integer form but IP addresses are encoded in hexadecimal form. Chromosome population is randomly selected. [21] Population is evolved using crossover and mutation. Effective fitness function is used to check the fitness of each rule. Fittest rules are then used for intrusion detection.
Ren Hui Gong et al. (2005) [20] have used a simple genetic algorithm to derive a set of classification rules from network audit data and the support confidence framework is utilized as fitness function to judge the quality of each rule. [20] The generated rules are then used to detect or classify network intrusions in a real time environment.
Jiu-Ling Zhao et al. (2005) have presented a novel approach of using clustering genetic algorithms to solve the computer network intrusion detection problem. They described a prototype intelligent intrusion detection system to demonstrate the effectiveness. This system combines two stages in to the process including clustering stage and genetic optimization stage. The algorithm can not only cluster the cases automatically, but also detect the unknown intruded action.
Tao Xia et al. (2005) present a hybrid method based on information theory and genetic algorithm to detect network attacks. Information theory is used to filter the traffic data and thus reduce the complexity. A linear structure rule is used to classify the network behavior in the normal and abnormal behaviors.
Chi Hoon Lee et al. (2006) presents the novel feature selection method that maximizes class separation between normal and attack patterns of computer network connections. They have focused on selecting a robust feature subset based on the genetic optimization procedure in order to improve a true positive intrusion detection rate.
Saqib Ashfaq et al. (2006) have used a genetic algorithm for generating efficient rules for cost sensitive misuse detection in intrusion detection systems. They have used five most weighted features identified by M.J.Middlemiss et al. They have designed a GA to identify these features. The algorithm generates if–then rules that identify an attack as well as its category so that appropriate action can be taken in response. This approach is cost sensitive that considers the cost of false alarms for each category of attack separately.
Nalini N. and Raghavendra Rao G. (2006) present a novel method of intrusion detection based on genetic algorithms and principal component analysis. [19] This technique can also be used to detect the class of intrusion. In this paper, they experiment with PCA to reduce the number of features of a TCP connection. This helps in reducing the number of bits required to represent a connection without loss of significant information. [19] They show how network connection information can be modelled as chromosomes and how the parameters in genetic algorithm can be defined in this respect. [19].
Hua Zhou et al. (2007) have used SVM and Genetic Algorithm to increase the classification accuracy. They used GA for feature selection and optimization and then used SVM model to detect intrusions.
Yong Wang et al. (2009) propose a fitness function, an efficient rule generator for denial of service attack. He used GA toolbox provided by MATLAB (R14) for his

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

implementation. He designed the genetic algorithm using 4 m-files. The rules generated are in if {condition} then {outcome} form. The rules generated are suitable for continuously changing misuse detection.

Chen Zhongmin et al. (2009) designed a training algorithm model based on abnormality detection. The proposed experimental model is based on a hypothesis that if variable x appears more times than the desired value, there is possibility of occurrence of abnormality.

Chris Sinclair et al. (2010) have proposed an approach to create rules for an intrusion detection expert system. They employ genetic algorithms and decision trees to automatically generate rules for classifying network connections. They have used genetic algorithms to evolve simple classification rule.

Blessy rajra and Dr. A.J.Deepa (2016) have proposed an approach "Enhanced Detection Guard System against malwares in Network" In this work, An Enhanced Detection Guard System (EDGS) is used to detect intrusions within the monitored networks. EDGS uses Heuristic algorithm to identify intrusions and it can identify the family of malwares. Detection Heuristic is capable of detecting many previously unknown malwares and new variants of current malwares. The Heuristic algorithm uses Entropy Measure and J-Measure. Entropy Measure is used to identify tuples. J-Measure combine's two metrics and compare with threshold to identify the intrusions within monitored networks finally performance evaluation is made to calculate the specificity, sensitivity, False Positive Rate, False Negative Rate, accuracy and precision.

III. PROBLEM IDENTIFICATION AND STATEMENT

There are many researchers who developed intelligent Intrusion Detection Systems. Some researcher used fuzzy based genetic algorithm but problem arises. A part from being fuzzy in nature the information could be very large requiring data mining techniques for extracting the data. The solution is the work can be extended further by using Dempster-Shafer theory. This Dempster-Shafer theory approach considers sets of propositions and assigns to each of them an interval. [Belief, Plausibility]. Another problem arised are for complex equation what is necessary. And solution for that is in near future will try to improve our intrusion detection system with the help of more statistical analysis and with better and may be more complex equations. Some limitations of the method are also observed.

First, the generated rules were biased to the training dataset. Second, while the support confidence framework is simple to implement and provides improved accuracy to final rules, it requires the whole training data to be loaded into memory before any computation. This issue may be resolved by carefully selecting either the number of generations in the training phase or the number of top best-fit rules in the intrusion detection phase. For large training datasets, it is neither efficient nor feasible. The use of some sorts of cache technologies may solve the problem.

IV. METHODOLOGY

The flowchart of methodology use is given below which includes:-

1. Initialization
2. Fitness calculation
3. Selection
4. Crossover
5. Mutation

V. GENETIC ALGORITHM

Genetic algorithm developed by Goldberg was inspired by Darwin's theory of evolution which states that the survival of an organism is affected by rule "the strongest species that survives". Darwin also stated that the survival of an organism can be maintained through the process of reproduction, crossover and mutation. Darwin's concept of evolution is then adapted to computational algorithm to find solution to a problem called objective function in natural fashion [24]. A solution generated by genetic algorithm is called a chromosome, while collection of chromosome is referred as a population. A chromosome is composed from genes and its value can be either numerical, binary, symbols or characters depending on the problem want to be solved. These chromosomes will undergo a process called fitness function to measure the suitability of solution generated by GA with problem [24]. Some chromosomes in population will mate through process called crossover thus producing new chromosomes named offspring which its genes composition are the combination of their parent. In a generation, a few chromosomes will also mutation in their gene. The number of chromosomes which will undergo crossover and mutation is controlled by crossover rate and mutation rate value. Chromosome in the population that will maintain for the next generation will be selected based on Darwinian evolution rule, the chromosome which has higher fitness value will have greater probability of being selected again in the next generation. After several generations, the chromosome value will converges to a certain value which is the best solution for the problem [24].

VI. ALGORITHM

1. Initialize the population
2. N = total number of records in the Dataset
3. For each chromosome in the population
4. A = 0, AB = 0
5. For each record in the set
6. If the record matches the chromosome
7. AB = AB + 1
8. End if
9. If the record matches only the "condition" part
10. A = A + 1

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

11. End if
12. End for
13. Fitness = 1 / (1+F_obj),
14. Where F_obj = f (x) = (a + 2b + 3c + 4d) - 41)

15. If Fitness of chromosome > among all Fitness values
16. Select the chromosome into new population
17. End if
18. End for
19. For each chromosome in the new population
20. Apply crossover operator to the chromosome
21. Apply mutation operator to the chromosome
22. End for
23. If number of generations is not reached, goto line no. 4 [24]

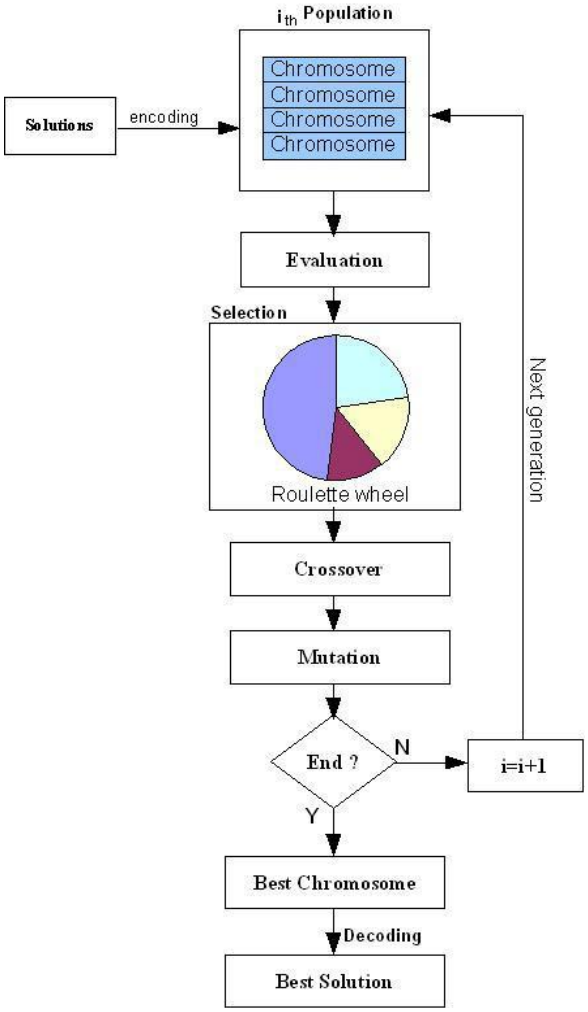

Fig.1 Genetic algorithm flowchart [24]

VII. PROCESSING STEPS

STEP-01

In the first step we will develop a zero matrix or we simply develop a matrix which containing "0" in all places initially means we can say that is under the stage of Initialization randomly. Now taking any one of the feature from NSL-KDD Dataset, means from out of 41 features we have to take any one feature column and we just have to fill out row by row or column by column of zero matrix .and here the initialize randomly step has been completed. But we have to know that we need to select the feature column randomly from our original NSL-KDD Dataset [means out of 41 features].

STEP-02 FITNESS CALCULATION OF EACH CHROMOSOMES

In this step, we have to calculate the fitness function of each chromosomes or genes [24] by this Formula.

Fitness = 1 / (1+**F_obj**)

Where F_obj = f (x) = (a + 2b + 3c + 4d) - 41)

STEP-03 SELECTION: -

This is the first iteration of fitness calculation. Here only two topmost fitness value of chromosomes are selected above all genes .from above 93.7 % fitness value and 96 % fitness value chromosomes are selected for further steps. Now we have to perform this step again and again, means same operation in iteration 2 and iteration 3 by changing the matrix value and calculate fitness value again for each newly generated chromosomes and select the highest value row or genes or chromosomes for further steps.

STEP -04

If we want to more and more accuracy with fitness value, then there are basically two types of Genetic Algorithm operators namely –

1. CROSSOVER
2. MUTATION.

1. CROSSOVER

The first step in the reproduction process is the recombination (crossover). In it the genes of the parents are used to form an entirely new chromosome. The typical recombination for the GA is an operation requiring two parents, but schemes with more parent's area also possible. Two of the most widely used algorithms are Conventional (Scattered) Crossover and Blending (Intermediate) Crossover. In this section taking two topmost fitness value genes and apply the crossover operation on them then develops new chromosomes and now we have to calculate the fitness value of that new produced genes. After applying crossover, there are two newly generated genes or chromosomes, now we have to calculate the fitness value of these new produced genes .and compare with previous two highest fitness value chromosomes. Now we have to select those two genes that holds the highest fitness value. Here two highest value genes, we have to select them for further calculation. For further fitness calculation need to apply Mutation operation on it.

2. MUTATION:-

In simple word the mutation is nothing but by changing any position value and then calculate the fitness vale for it. The newly created by means of selection and crossover population can be further applied to mutation. Mutation means, that some elements of the row or genes are changed. Those changes may be caused by mistakes during the copy process of the parent's genes. In the terms

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

of GA, mutation means random change of the value of a gene in the population .The chromosome, which gene will be changed and the gene itself are chosen by random as well. Now after performing the Mutation operation, we have to select two topmost fitness valued chromosomes among 4 genes .only 2 genes we have to select. We need to perform same operations for different matrix combination of NSL-KDD Dataset and calculate fitness value for more accuracy.

VIII. RESULTS

Now in an intrusion detection system based on genetic algorithm, need to implement or perform the operation more and more for great accuracy of fitness calculation. So we need to perform all our experiments in MATLAB by taking NSL-KDD as a dataset.

IX. NSL-KDD DATASET

The inherent drawbacks in the KDD cup 99 dataset has been revealed by various statistical analyses has affected the detection accuracy of many IDS modelled by researchers. NSL-KDD data set is a refined version of its predecessor. It contains essential records of the complete KDD data set. There are a collection of downloadable files at the disposal for the researchers.

X. CONFUSION MAT R IX

Confusion matrix is a matrix that represents result of classification. It represents true and false classification results. The followings are the possibilities to classify events and depicted in Table [23].

– **True positive (TP):** Intrusions that are successfully detected by the IDS.

– **False positive (FP):** Normal/non-intrusive behaviour that is wrongly classified as intrusive by the IDS.

– **True Negative (TN):** Normal/non-intrusive behaviour that is successfully labelled as normal/non-intrusive by the IDS.

– **False Negative (FN):** Intrusions that are missed by the IDS, and classified as normal/non-intrusive [23].

Table 1: Performance Measures

Actual Class	**Predicted Class**	
	Attack	**Normal**
Attack	**True Positive (TP)**	**False Negative (FN)**
Normal	**False Positive (FP)**	**True Negative (TN)**

XI. PERFORMANCE MEASURES

1. **Accuracy: -** Accuracy refers to the portion of data classified an accurate type in total data [22].

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

2. **Sensitivity: -** Measures the amount of true positives that is the ability of the classification on predicting the correct values in the class presented.it is also called True Positive Rate (TPR) [22].

$$\text{Sensitivity (TPR)} = \frac{TP}{TP+FN}$$

3. **Specificity: -** Measures the proportion of the accurate negatives that is the ability of the classification on predicting the accurate values for the cases that are the reverse of the desired one .it is also called True Negative Rate (TNR) [22].

$$\text{Specificity (TNR)} = \frac{TN}{FP+TN}$$

Table 2: Comparison Table of Result

S. No.	Data Set Used	Methodology	Performance Measure	
			Accuracy	Specificity
1.	KDD CUP 99 Dataset	EDGS uses Heuristic algorithm	0.87	0.74
			0.92	0.95
2.	NSL-KDD Dataset	Genetic algorithm	0.92	0.96
			0.93	0.97

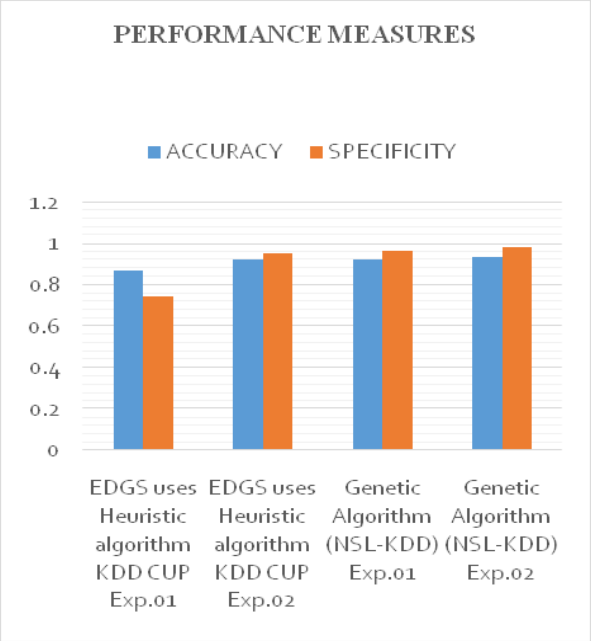

Fig.2:- Graph of Comparison of performance Measures

XII. PURPOSE TO USE NSL-KDD DATASET INSTEAD OF KDD 99

The main difference between NSL-KDD and KDD 99 is the no. of data having. The KDD 99 having 65,536 rows and 41 features (columns). But NSL-KDD having data with less number of rows. NSL-KDD dataset having 25,193 rows and 41 features.so can say that by using NSL-

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

KDD dataset perform the same accuracy with less number of data. It is also the process of optimization.so to find out the same accuracy and fitness value with less number of data is done by using NSL-KDD dataset.

XIV. CONCLUSION AND FUTURE WORK

In this paper, presenting and implemented an Intrusion Detection System by applying genetic algorithm that will efficiently detect various types of network intrusions and malicious activities. To implement neural network means in future can make an ensemble model of intrusion detection system for more accuracy and we can use the NSL-KDD dataset benchmark because this dataset gives more accuracy by using less number of feature selection. This thesis includes perform other intrusion detection system also by feature reduced. In simple word can say that the optimization operation will done. And measure the performance of our system we used the standard NSL-KDD benchmark dataset and obtained reasonable detection rate. In near future we will try to enhance our intrusion detection system by using two models or can say that with IDS based on genetic algorithm combine with any other models that may be based on data mining or may be any method.

REFERENCES

[1] R.Elamaran and R.Mala, "A Study on Network Intrusion Detection System (NIDSs) In Virtual Network Structure", International Journal of Computer Sciences and Engineering (IJCSE), Vol. 03, Issue - 11, November-2015, pp.59 – 164.

[2] Mostaque Md. Morshedur Hassan, LCB College, Maligaon, Guwahati, Assam, India, "Current Studies on Intrusion Detection System, Genetic Algorithm and Fuzzy Logic", International Journal of Distributed and Parallel Systems, Vol. 4, Issue-2, March-2013,pp.35-47.

[3] Y.Dhanalakshmi and Dr. I. Ramesh Babu, "Intrusion Detection Using Data Mining Along Fuzzy Logic and Genetic Algorithms", Dept. of Computer Science & Engineering , Acharya nagarjuna University, Guntur, A.P. India International Journal of Computer Science & Network Security (IJCSNS), Vol.8, Issue-2, Februry-2008 ,pp.27-32.

[4] Zorana Banković, José M. Moya, Álvaro Araujo, Slobodan Bojanić and Octavio Nieto-Taladriz, "A Genetic Algorithm based Solution for Intrusion Detection", Journal of Information Assurance and Security(JIAS) , Vol.4 , Issue-3 , June-2009, pp.192-199.

[5] Shelly Xiaonan Wu, Wolfgang Banzhaf, "The use of computational intelligence in intrusion detection systems: a review", Applied Soft Computing, Vol.10, Issue-01, January-2010, pp.1–35.

[6] Mohammad Sazzadul Hoque, Md. Abdul Mukit & Md. Abu Naser Bikas, "An Implementation of Intrusion Detection System using Genetic Algorithm" , Department of Computer Science and Engineering, Shahjalal University of Science and Technology, Sylhet, Bangladesh, International Journal of Network Security and Its Applications (IJNSA),Vol.4, Issue-2,March-2012, pp.109-120.

[7] S Selvakani Kandeeban, and Rengan S Rajesh , Department of Computer Applications, Jaya Engineering College1 Chennai, Tamilnadu, 602 024, India. Dept. of CSE, MS University, Tirunelveli, Tamilnadu, 627 009, India, "Integrated Intrusion Detection System using Soft computing", International Journal of Network Security, Vol.10, Issue-2, March -2010,pp.87-92.

[8] W. Lu and I. Traore, Department of Electrical and Computer Engineering, University of Victoria, Victoria B.C., Canada "Detecting New Forms of Network Intrusion Using Genetic Programming", Computational Intelligence, vol. 20, Issue-03, August -2004, pp.475-494.

[9] K. Burbeck & N.Y. Simmin (2007), Department of Computer and Information Science, Linkoping University ,Sweden, "Adaptive Real-Time Anomaly Detection with Incremental Clustering", Information Security Technical Report, Vol. 12, Issue- 1 ,07-March- 2007 ,pp.56–67.

[10] T.S. Chou, K.K. Yen & J. Luo , "Network Intrusion Detection Design using Feature Selection of Soft Computing Paradigms", International Journal of Computational Intelligence, Vol. 4, Issue-3, 2008 , pp.196–208.

[11] Bhavani M. Thuraisingham, Latifur Khan, Mamoun Awad , University of Texas at Dallas, Dallas , USA,"A New Intrusion Detection System using Support Vector Machines and Hierarchical Clustering", The International Journal on Very Large Data Bases, Vol.16, Issue-04,October-2007 ,pp.507–521.

[12] S. M. Aqil Burney,M. Sadiq Ali Khan and Jawed Naseem, Department of Computer Science ,University of Karachi , Pakistan, "Efficient Probabilistic Classification Methods for NIDS", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 8 ,Issue-08 , November-2010, pp.168-172.

[13] Baoyi Wang; Feng Li; Shaomin Zhang, "Research on Intrusion Detection Based on Campus Network", Intelligent Information Technology Application, Vol.01, 2009, pp.468-471.

[14] L.Dhanabal, Dr. S.P. Shantharajah , Assistant Professor [SRG], Dept. of Computer Applications, Kumaraguru College of Technology, Coimbatore, India, Professor, Department of MCA, Sona College of Technology, Salem, India , "A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 6, June 2015 , pp.446-452.

[15] Purushottam Patil, Dr. Yogesh Sharma and Dr. Manali Kshirsagar, Research Scholar (Computer Science & Engineering), Faculty of Engineering & Technology, Jodhpur National University, Jodhpur (RJ), India,Professor (Mathematics), Department of Applied Science, Faculty of Engineering & Technology,Jodhpur National University, Jodhpur(RJ), India Professor & Dean (Student Affair), Department of Computer Technology, Yashwantrao Chavan College of Engineering, Nagpur(MS), India , "Network Based Intrusion Detection System using Genetic Algorithm: A Study" , International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 3, Issue 2, March – April 2014 , pp.282-286.

[16] Anubhavnidhi , Abhashkumar Roney Michael , "Implementing an Intrusion Detection System using a Decision Tree".

[17] Vidhya N. Gavali , Sunil Sangve , Computer Dept, Pune University, "Anomaly Network Intrusion Detection: A review" , International Journal of Innovative Research in Advanced Engineering (IJIRAE), Volume 2, Issue 4,April 2015 , pp.90-95.

[18] Melanie Middlemiss, Information Science Department, University of Otago, "Framework for Intrusion Detection Inspired by the immune system" Conference ,July 2005 , pp.1-14.

[19] Nalini.N and Raghavendra Rao G,"Network Intrusion Detection via a hybrid of Genetic Algorithms", International Journal of Information Processing , Vol. 1, No. 1, March/April 2007, pp.104-111.

[20] Ren Hui Gong, Mohammad Zulkernine, Purang Abolmaesumi , School of Computing , Queen's University , Kingston, Ontario, Canada , "A Software Implementation of a Genetic Algorithm based approach to Network Intrusion Detection", Proceedings of the Sixth International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing and First ACIS International Workshop on Self-Assembling Wireless Networks (SNPD/SAWN'05), 2005 , pp.1-8.

[21] Wei Li , Department of Computer Science and Engineering, Mississippi State University, Mississippi State, "Using Genetic Algorithm for Network Intrusion Detection",2004 , pp.1-8.

[22] Blessy Rajra M B, Student, Department of Computer Science Ponjesly College of Engineering Nagercoil, India, Dr. A J Deepa ME., Ph.D, P.G, Associate Professor, Department of Computer Science Ponjesly College of Engineering Nagercoil, India," Enhanced Detection Guard System Against Malwares In Network", International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE), Vol .02, Issue 04, June 2016, pp.34-39.

[23] Gulshan Kumar, Assistant Professor, Shaheed Bhagat Singh State Technical Campus, Ferozepur,Punjab,"Evaluation Metrics for Intrusion Detection Systems - A Study", International Journal of Computer Science and Mobile Applications, vol. 02 , Issue 11 , November 2014 , pp.11-17.

[24] Denny Hermawanto, Indonesian Institute of Sciences (LIPI), INDONESIA, "Genetic Algorithm for Solving Simple Mathematical Equality Problem".