Analysis of Fitness Function in Designing Genetic Algorithm Based Intrusion Detection System

Prof. Jahnavi .S. Vithalpura[1] Prof. H.M.Diwanji[2]
[1]Assistant Professor [2]Associate Professor
[1,2]Department of Information Technology
[1,2]L. D. College of Engineering, Ahmedabad, Gujarat, India

Abstract— Network Intrusion detection system is tool to monitor & identify intrusion in computers networks. The genetic algorithm is employed to derive a set of classification rules from network audit data. Different data sets are used as an audit data .From these data sets only specific features are selected and represented as chromosomes, which represent rules. The weighted sum model, support-confidence framework or reward penalty framework is utilized as fitness function to judge the quality of each rule. Best rule collection or knowledge base improves IDS performance by improving detection rate and reducing false alarm rate. The weighted sum model is generally more helpful for identification of network anomalous behaviors. The support –confidence framework is simply identifying network intrusions or precisely classifying the types of intrusions. Reward penalty technique used to give reward to the good chromosome and to apply penalty on the bad chromosome. This paper gives detail study about research carried out in fitness function of genetic based intrusion detection system.

Key words: genetic algorithm, intrusion, network intrusion detection system, fitness function

I. INTRODUCTION

Security mechanisms of a system are designed to prevent unauthorized access to system resources and data. An unauthorized access to the resources of the computer is called an intrusion to a computer. The security mechanism tools that looks for unauthorized users those whom intrusions to computer is called IDS. A lot of research work has been carried out in developing new technique ranging from basic stastiscal methods to highly complex evolutionary methods for intrusion detection system.

The aim of this paper is to present a review of contributions from researchers that investigate and support the use of genetic algorithm in designing intrusion detection system the rest of the paper is organized as follows: Section II provides a brief introduction to Intrusion Detection System. Section III describes the basic concept of Genetic Algorithm. Section IV describes the technique of applying Genetic Algorithm to Intrusion Detection System. Section V presents the related work and a comparative analysis of existing studies. Finally, the discussion is concluded.

II. INTRUSION DETECTION SYSTEM

IDS must distinguish between authorized and unauthorized activity to the computer resources in order to recognize intrusions. Bace et al. in [1] defined IDS as the process of monitoring the events occurring in a computer system or networks and analyzing them for signs of intrusions and as attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer network.

A. Types of Intrusion Detection System:

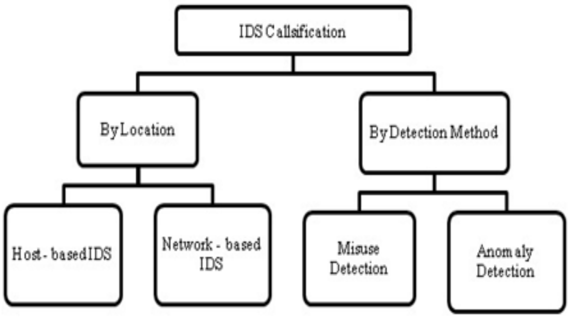

Fig. 1: Types of intrusion detection system

1) By Location:

IDS can also be classified into following categories on the basis of the where to monitor for intrusive activity.

a) Host Based IDS:

It will monitor computing system itself for intrusive activity and alert when there is some modification in important files of operating system or user.

b) Network Based IDS:

It will monitor packets traveling across network to find out malicious activity across networks, such as denial of services, port scan.

2) By Detection Method:

It can also be classified into

Following categories on the basis of the detection approaches:

a) Misuse based IDS (Signature Based IDs):

It will work by comparing user activity with stored pattern or signature knowledge base of known attacks. Such IDS check incoming connection with stored knowledge base if it is matching then it will block it.

b) Anomaly Based IDS:

It detect intrusions by searching for abnormal network traffic [3]. The abnormal traffic pattern can be defined either as the violation of accepted thresholds for frequency of events in a connection or as a user's violation of the legitimate profile developed for normal behavior. This approach classified into statistical Methods, data-mining methods and machine learning based methods.

B. Component of Intrusion Detection System:

Fig-2 adopted with modifications from [2], gives a generic architecture of an intrusion detection system.

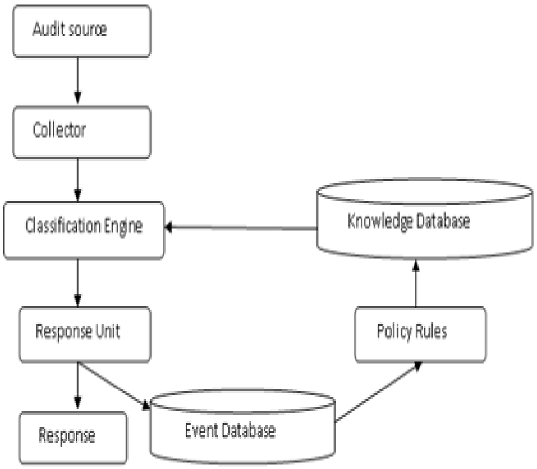

Fig. 2: Component of Intrusion Detection system [2]

– The audit source states the input to the intrusion detection system. The format of input data can be of any types depending upon the location and type of the intrusion detection system.
– The collector samples and preprocesses the audit source data. The data is converted into a standard format known to the internal components of the intrusion detection system.
– The knowledge database contains knowledge about attacks.
– The classification engine determines the validity of the received data by comparing it with the attack information stored in the knowledge database.
– The policy rules are used to configure the response and detect intrusion.
– The response unit produces different types of responses & alerts depending upon the events and their severity.
– The event database stores the detailed information about the events; it is used for various purposes like attack report generation, and framing new rules.

C. Intrusion Data Set Used:

All the researchers have implemented their genetic algorithm on the offline data such as DARPA1998 data or KDD CUP 99 data set.

1) DARPA 1998:

MIT Lincoln Laboratory (Defense Advanced Research Projects Agency (DARPA)) and Air Force Research Laboratory (AFRL) sponsorship, has collected and distributed the first standard datasets for evaluation of computer network intrusion detection systems.

This Data is DARPA 1998 data [5]. It consist of tcp dump and BSM list files. Each row in a list file corresponds to a separate session describing individual TCP/IP connection between two machines.

2) KDD CUP 99:

KDD CUP 99 data [6] derived from the KDD Cup competition. It is part of the data collected from the MIT Lincoln Labs 1998 DARPA Intrusion Detection Evaluation Program and is considered benchmark data for evaluating intrusion detection systems. The data is available in full (743M of network connections), or in a number of smaller datasets. From the observation of datasets, attacks fall into four main classes [7] namely,

a) Probe:

An attacker tries to gain information about the victim machine. His purpose is to check vulnerability on the victim machine. e.g., Port scanning.

b) Denial of Service (DoS):

An attacker tries to prevent legitimate users accessing or consume a service via back, land, Neptune, pod Smurf and teardrop.

c) Remote to Local (R2L):

The attacker tries to gain access to the victim machine by compromising the security via password guessing or breaking.

d) User to Remote (U2R):

In U2R, an attacker has local access privilege to the victim machine and tries to access super users (administrators) privileges via “Buffer overflow” attack.

D. Detection And Identification Of Attack And Non-Attack Behaviors Can Be Generalized [8] As The Follows:

1) True Positive (TP):

The amount of attack detected when it is actually attack.

2) True Negative (TN):

The amount of normal detected when it is actually normal.

3) False Positive (FP):

The amount of attack detected when it is actually normal, namely false alarm.

4) False Negative (FN):

The amount of normal data detected when it is actually attack, namely the attacks which can be detected by intrusion detection system.

III. Genetic Algorithm

Genetic Algorithms are search algorithms that are based on concepts of natural selection and natural genetics. The concepts of genetic algorithm approach are given by Holland [9] and it has been deployed to solve wide range of optimization problems.

GA evolves a population of initial individuals to a population of high quality individuals, where each individual represents a solution of the problem to be solved. Each individual is called chromosome, and is composed of a predetermined number of genes [10]. The quality of each rule is measured by a fitness function as the quantitative representation of each rule’s adaptation to a certain environment. During each stage, three genetic operators are applied sequentially to each child with certain probabilities, i.e. selection, crossover and mutation.

IV. Implementing GA in Intrusion detection system

When Intrusion detection system is implemented using genetic algorithm, it will be used as rule generating tool. The goal of the system is not to evolve a single best rule (global optimal), but to create a set of rules, knowledge base which is good enough to detect attacks (intrusions). The proposed GA-based intrusion detection approach contains two modules where each works in a different stage.

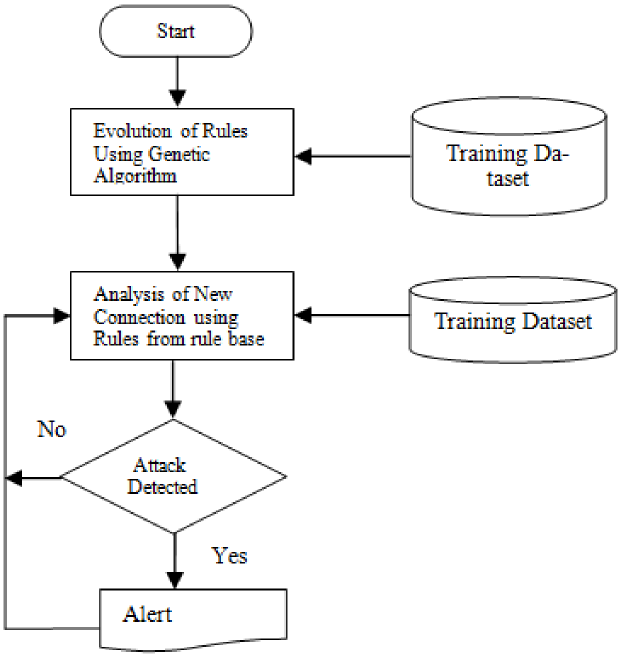
Start
Evolution of Rules Using Genetic Algorithm
Training Da-taset
Analysis of New Connection using Rules from rule base
Training Dataset
No
Attack Detected
Yes
Alert

Fig. 3: GA Based intrusion detection system[16]

- Training stage, a set of classification rules are generated from network audit data using the GA in an offline environment.
- Testing stage, In this stage, the generated rules are used to classify incoming network connections in the real time environment.

A. *Training Phase:*

1) *Encoding of Connections:*

The author describe in [14] that each rule is an *if-then* clause, which contains a "condition" and an "outcome". The first six features in Table 1 are connected using the logical AND operations and compose the "condition" part of a rule.

The feature "Attack name" is used in the outcome" part, which indicates the classification of a network record (at training stage) or connection (at intrusion detection stage) when the "condition" part of a rule is matched. The following shows a rule example that classifies a network connection as the denial-of-service attacks *neptune*.

if(duration="0:0:1"andprotocol="finger"and
source_port=18982anddestination_port=79and
source_ip="9.9.9.9"anddesnaion_ip="172.16.112.50")
then(attack_name="neptune")

The above rule expresses that if a network packet is originated from IP address 9.9.9.9 and port 18982, and sent to IP address 172.16.112.50 and port 79 using the protocol finger, and the connection duration is 1 second, then most likely it is a network attack of type neptune that may eventually cause the destination host out of service.

Feature	**Format**	**Number of Genes**
Duration	H:M:S	3
Protocol	Numeric	1
Source Port	Numeric	1
Destination Port	Numeric	1
Source IP	a.b.c.d	4
Destination IP	a.b.c.d	4
Attack name and IP	String	1

Table 1: Chromosome Representation Of A Rule[14]

Each rule is encoded as a chromosome using a fixed length vector, where each network feature is encoded us-ing one or more genes of different types (see the second and third column of Table 1). In the above example, the encoded form of the rule would look like as follows[14]:

{0, 0, 1, 2, 18982, 79, 9, 9, 9, 9, 172, 16, 112, 50, 1}

There are different encoding types used to represent-chromosome are: Binary encoding, value encoding, per-mutation encoding.

2) *Selection of Initial Population:*

If the value of the population size is too small, the algorithm might improve the speed, but reduce the diversity of the population, and is likely to cause genetic algorithm premature convergence; if the value of the population size is too large, the algorithm will make the operating efficiency of genetic algorithm lower. The general recommended range is [24] 20-300.

3) *Evaluating Each Chromosome Using Fitness Function:*

During the training phase, evaluation of chromosomes is carried out in order to determine their goodness. If a chromosome correctly classifies an attack, it is considered good; else, it is bad and is not selected for crossover to produce offspring. Thus, a chromosome which detects more attacks has higher fitness value and has higher chances for selection.

The different fitness models proposed by various researchers are: support and confidence model, reward-penalty model, weighted sum model.

4) *Selection:*

In this stage individual genomes are chosen from the population of string of chromosomes. The commonly used techniques for selection of chromosomes are[d] Roulette wheel, rank selection and steady state selection.

5) *Genetic Algorithm (GA) Operator:*

Genetic algorithms (GAs) use various operators viz. the crossover, mutation for the proper selection of optimized value. Selection of proper crossover and mutation operator depends upon the encoding method and as per the problem definition.

a) *Crossover:*

It is the process in which genes are selected from the parent chromosomes and new offspring is created. It is also called recombination, is the.

Crossover's objective is to get a new individual in the next generation, just like the marriage process of human society.

The search capability of GA greatly improves by their organization of crossover operation. Crossover is divided into single-point crossover, multi-point crossover, the uniform crossover, tree crossover, permutation encoding crossover.

b) *Mutation:*

Mutation can search new areas in contrast to the crossover. Crossover is referred as exploitation operator whereas the mutation is exploration one.

Mutation itself is a local random search, and when combined with selection and recombination it can ensure the effectiveness of the genetic algorithms, so that the genetic algorithms can have the local search capability and maintain the diversity of population to prevent nonmature Convergence. Mutation rate cannot be too larger. If mutation rate is more than 0.5 Pm, genetic algorithm will degrade into a random search.

Types of mutation are binary encoding (bit inversion), value encoding (changing number), and permutation encoding (order changing).

B. Testing Phase:

In this phase, the rules stored in the rule base are used to detect whether a real-time network connection is a normal connection or an intrusive attack. If the characteristics of new connection match with the 'condition' section of some pre-defined rule in the rule-base then the connection is considered as an attack else it is considered as a normal connection. If an attack is detected then IDS performs the necessary actions defined by the security policies of the organization. The algorithm of testing for GA-based IDS is presented below.

1) Algorithm:

Intrusion Detection (testing phase) [16]

2) Input:

Inflowing network connection

3) Output:

Decision if connection is intrusive or not

```
1) Loop Forever {fetch incoming packet}
2) for each rule in rule-base
3) Match rule with network connection
4) if rules match then
5) Mark current connection as an intrusion (and generate
an alarm as per security policies)
6) end if
7) end for each
8) end loop forever.
```

V. Related Work

The Intrusion Detection System has undergone rapid changes and is using new techniques to generate better results. Genetic Algorithm can be used in different ways in Intrusion Detection Systems.

Genetic Algorithm based intrusion detection approach discussed in this review paper is focused on a rule based Intrusion Detection System which uses only Genetic Algorithm to generate knowledge. For this purpose network connections are analyzed to describe the normal and abnormal behavior in the network. Three factors will have significant impact on the effectiveness of the algorithm [14]. They are:

a) The fitness function;

b) The representation of individuals

c) The GA parameters.

So we have analyzed fitness function of all the researchers who have implemented GA in a network based intrusion detection system.

Ren Hui Gong,[14] and Salah Eddine and Benaicha[15] has implemented GA based intrusion detection system and used support confidence framework based fitness function.

If a rule is represented as if A then B, then the fitness of the rule is determined using following equations:

support = |A and B| / N (1)

confidence = |A and B| / |A| (2)

fitness = w1 * support + w2 * confidence (3)

Here, N is the total number of network connections in the audit data, |A| is the number of network .w1,w2 are thresholds to control support and confidence respectively.

Ren Hui Gong has found nice property that the approach can be used for either simply identifying network intrusions (if w1=1, w2=0) precisely classifying the types of intrusions (if w1 = 0 and w2 = 1). But here problem is that whole training data set should be loaded into memory. They [15] has analyzed that Satisfactory results are produced, in terms of very high detection rate (99%), reinforced by a low rate of false positives (3%). The results are obtained by selecting the initial population for each type of attacks.

Zorana Bankovica [13] and V. Moraveji Hashmei, Z. Muda and W.Yasin [15] has used only 3 network feature to detect intrusion by applying PCA machine learning technique. To determine a fitness value of each rule, the following fitness function is deployed [15] & [13]:

$$\text{Fitness F=}\frac{\alpha}{A}-\frac{\beta}{B} \qquad (4)$$

where α is the number of correctly detected attacks, A is the total number of attacks in the training dataset, β Is the number of normal connections incorrectly characterized as attacks, i.e. false-positives, and B is the total number of normal connections in the training dataset. Scale of fitness values is [- 1, 1], where -1 is the lowest and 1 the highest value.

Fitness function used	Explanation of fitness function used	References	Research findings

support confidence model
support = |A and B| / N
confidence = |A and B| / |A|
fitness = w1 * support + w2 * confidence
	N is the total number of network connections in the audit data, |A| stands for the number of network connections matching the condition A, and |A and B| is the number of network connections that matches the rule if A then B. W1,w2 are thresholds used to control support and confidence respectively.	Ren Hui Gong,2005, [14]	+used for either simply identifying net work intrusions or precisely classifying the types of intrusions. 97% of the attacks detected correctly by this system.
			- requires the whole training data to be loaded into memory before any computation. For large training datasets, it is neither efficient nor feasible.

		Salah Eddine and Benaicha,2014[15]	+ got high detection rate & law false positive rate. Focus on size of Initial population . -need to work for new types of attack
Fitness F= $\frac{\alpha}{A}$ - $\frac{\beta}{B}$	where α is the number of correctly detected attacks, A is the total number of attacks in the training dataset, β is the number of normal connections incorrectly characterized as attacks, i.e. false-positives, and B is the total number of normal connections in the training dataset	Zorana Bankovic,2007 [13]	+three features of the network connections maintaining high detection rates and low false alarm rate without using complex soft computing techniques. + perform intrusion detection process fast and could be applied to high speed networks. + gained 95.62% as detection rate and 4.37% as false alarm.
		V. Moraveji Hashmei, Z. Muda and W.Yasin 2011[15]	

Weighted sum model
F=1 –penalty
	Where
	∆= |outcome- suspicious Level |
	Penalty=(∆*ranking)/100
	F=1 -penalty
		Wei Li 2004[18]	+ unique as it considers both temporal and spatial information of network connections in encoding the network connection information into rules in IDS.
			+Be more helpful for identification of network anomalous behaviours.
			+reward must be as more as the chromosome strength, the penalty mustbe as more as the chromosome weakness

F= f(x)/f(sum)	Where f(x) is the fitness of entity x and f is the total fitness of all entities	B. Uppalaiah K. Anand, B.Narsimha, S.Swaraj, T.Bharat2012[19]	+Uses only 3 networkfeatures; 83.65% of avg.success rate; process is faster and can be applied for high speed networks.
		Miss Priya U. Kadam, Mr. P. P. Jadhav 2013[20]	+An average detection rate of 91.025% and decrease the percentage of false alarms. her IDS should be capable in detecting complex intrusions
F= weight*packet_size	Where the pocket_size is the actual packet data size prescribed by the incoming packet data stream and weights the Vector which is applied to each chromosome.	Bharat S. Dhak,2012[21]	+Scope of experiment is focused to generate a list of vulnerable IP addresses; gained 96% of accuracy.
$F=(\sum_{k=0}^{n} Match * wi) - Rank * (\sum_{k=0}^{n} wi * \overline{match)}$	When the network connection and chromosomes get a successful match, the Match value is 1; when fails to match, it will be 0. And wi is the weight of the different domains in TCP /IP packets.If a clear normal link is classified as invasion, the value of the rank will belarger; butif an inconspicuous connection is classified as invasion, the value of Rank will be smaller. value of match is opposite of match.	Qiao Pei-li ; Chen Shi-Feng ; Su Jie[22]	He has improved all parameters of GA,Fitness function and initial population size. By doing improvement in GA, He reduce misstatement rate and omission rate and also improve detection rate.
Reward Penalty model based	Consider a rule: If A then B,	Firas Alabsi,Reyadh Naoum[23]	Uses 5-network features; Fitness function gives

F=2+(AB-A/AB+A)+(AB/X)-(A/Y)	((AB-A)/(AB+A))= strength of a record; AB/X= ratio of the strength of record to the strength of the strongest record; A/Y=ratio of the weakness of a record to the weakness of the weakest record		reward to good chromosomes and applies penalty on the badchromosomes; comparison between the newlyproposed and other existing fitness functions is presented.

Table 2: Comparison of Existing Studies on Fitness Function Used In GA Based IDs

High attack detection rate and low false-positive rate demonstrate advantage s of applying this tech niqueto intrusion detection without using any complementary technique typically used with other soft-computing techniques. He found that it will detect intrusion very fast so it will be applicable to high speed network.

. Wei Li [18] he calculated the fitness function by calculate the following four equations:

∆= |outcome- suspicious Level | [5]

Penalty=(∆*ranking)/100 [6]

F=1 –penalty [7]

Using equation (5) the outcome is calculated based on whether the A field of connection matched the preclassified data set and then multiply the weight of that field, the value of matched is 0 or 1.In the equation (6), the actual value of suspicious Level reflects observations from historical data.In the equation (7), ranking indicates whether or not the intrusion is easy to identify. Finally the value of fitness computed in equation (6) using the penalty.

Wei Li's implementation of genetic algorithm is unique as it considers both temporal and spatial information of network connections in encoding the network connection information into rules in IDS. This may lead to increased detection rates.However, no experimental results are available yet.

Uppalaiah, K. Anand, B. Narsimha, S. Swaraj and T. Bharat [19] suggest an intrusion detection system using genetic algorithm to generate rule set for eight types of attacks belonging to four categories. The proposed architecture deployed KDDCUP99 dataset. The datasets contains 41 features out of which only 3features have been used to specify each entry of the dataset.Uppalaiah [19] and Priya U. Kadam[20] has used follwoing fitness function to measure a chromosome.

Fintness = f(x)/f(sum) (8)

Where f(x) is the fitness of entity x and f is the total fitness of all entities .Uppalaiah [19] Uses only 3 network features; 83.65% of avg. success rate; process is faster , can be applied for high speed networks.Priya[20] has got An average detection rate of 91.025% and decrease the percentage of false alarms. her IDS should be capable in detecting complex intrusions. The results of the paper specify the set of rules and high R2l and U2r attack detection rate.

Bharat S. Dhak and Shrikant Lade [6] present a genetic algorithm based intrusion detection technique to detect malicious packets on the network and ultimately help to block the respective IP addresses. He has used firewall log file as a data set & gained 96% of accuracy.To determine a fitness value of each rule, the following fitness function is deployed

F=weight*packet_size (9)

Qiao Pei-li ,Chen Shi-Feng ; Su Jie[22] has improved all over operation of GA. He has improved all parameters of GA,Fitness function and initial population size. By doing improvement in GA, He reduce misstatement rate and omission rate and also improve detection rate.

Where Misstatement rate = (wrong alarm times/total incident times)× 100% Omission rate = (intrusion times do not detect/total intrusion times)× 100%

Qiao Pei-li has used following fitness function.

$$F = (\sum_{k=0}^{n} Match * \; wi) - \quad Rank * (\sum_{k=0}^{n} wi * \overline{match}) \qquad (10)$$

When the network connection and chromosomes get a successful match, the Match value is 1; when fails to match, it will be 0. And *wi* is the weight of the different domains in TCP /IP packets. If a clear normal link is classified as invasion, the value of the rank will be larger; but if an inconspicuous connection is classified as invasion, the value of Rank will be smaller. value of match is opposite of match.

Firas Alabsi,Reyadh Naoum[23] has used Reward Penalty based model. His fitness function is given below:

F=2+(AB-A/AB+A)+(AB/X)-(A/Y) (11)

The proposed fitness function works on the principle that reward and penalty are proportionate to the strength and weakness of chromosomes. In order to prove the validity of the new fitness function, the results of reward-penalty model based fitness function are compared with the results of the support-confidence model based fitness function. The results closely match with each other.

VI. Conclusion

This paper describes the various models or framework used to design a fitness function for GA based intrusion detection system. The comparative study could make researchers to use the best possible techniques to design a fitness function which will judge the quality of each rule. The generated rules are then used to detect or classify network intrusions in a real-time environment and it will improve intrusion detection rate and reduce false alarm rate.

References

[1] R. Bace, and P. Mell, ―Intrusion Detection Systems‖, National Institute of Standards and Technology NIST, 2001.USA

[2] M. Arvidson and M. Carlbark, "Intrusion Detection Systems: Technologies, Weaknesses, and Trends," 2003.

[3] S. Kumar, ―Classification and Detection of Computer Intrusions‖, Ph.D. Thesis, Purdue University, 1995.

[4] S. Kumar, and E. H. Spafford, ― A Software Architecture to support Misuse Intrusion Detection‖, Technical Report CSD-TR-5-009, 1995.

[5] MIT Lincoln Laboratory, DARPA datasets, MIT, USA. (http://www.ll.mit.edu/mission/communications/ist /corpora /ideval/data/1998data.html)

[6] KDD CUP 99 data set (http://kdd.ics.uci.edu/ databases/kddcup99/kdd cup)

[7] Santosh Kumar Sahu ,"A Detail Analysis on Intrusion Detection Data62sets" IEEE International Advance Computing Conference (IACC) 2014 pg-1348-1353

[8] Shelly Xiaonan Wu, Wolfgang Banzhaf, "The use of computational intelligence in intrusion detection system s: A review" Applied Soft Computing 10 (2010) 1–35 published by elsevier .com

[9] Holland J. "Adaptation in natural and artificial system." Ann Arbor. The University of Michigan Press; 1975.

[10] PolhlheimH,Genetic and Evolutionary Algorithms: Principles, Methods and Algorithms. <http://www.geatbx.com/docu/index.html>, accessed in 2006.

[11] S.Owais, V.Snasel, A.Abraham,"Survey: Using Genetic Algorithm Approach in Intrusion Detection Systems Techniques" 7th Computer Information Systems and Industrial Management Applications IEEE, 2008.

[12] RC Chakraborty, Fundamentals of Genetic Algorithm: AI Course, June 2010, available at http://www.myreaders.info/09genetic_Algorithms. pdf

[13] Zorana Bankovic, Dusˇan Stepanovic, Slobodan Bojanic,Octavio Nieto-Taladriz "Improving network security dsfusing genetic algorithm approach" computers and electrical engineering 33(2007)publish by elesevier pvt ltd.

[14] Ren Hui Gong, Mohammad Zulkernine, Purang Abolmaesumi, "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 (SNPD/SAWN'05) 2005 IEEE

[15] A.A. R, Townsend. -GAs – a Tutorial‖, 2003.

[16] Salah Eddine Benaicha, Lalia Saoudi, Salah Eddine Bouhouita Guermeche, Ouarda Lounis ,"Intrusion Detection System Using Genetic Algorithm/' Proceedings of the Science and Information Conference 2014 IEEE

[17] V. Moraveji Hashmei, Z. Muda and W. Yassin, "Improving Intrusion Detection using Genetic Algorithm", International Technology journal 12(11) pp. 2167-2173, 2013

[18] Li, Wei, "Using Genetic Algorithm for Network Intrusion Detection", ,Proceedings of the United States Department of Energy Cyber Security Group,(2004)

[19] B. Uppalaiah, K. Anand, B. Narsimha, S. Swaraj, T. Bharat, "Genetic AlgorithmApproach to Intrusion Detection System", IJCST Vol. 3, Issue 1, Jan-March 2012

[20] Miss Priya U. Kadam, Mr. P. P. Jadhav,"An effective rule generation for Intrusion Detection System using Genetics Algorithm" ,International Journal of Science, Engineering and Technology Research (IJSETR) Volume 2, Issue 10, October 2013

[21] Bharat S. Dhak, Shrikant Lade, " An Evolutionary Approach to Intrusion Detection System using Genetic Algorithm" .ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 2, Issue 12, Dec. 2012

[22] Qiao Pei-li ; Chen Shi-Feng ; Su Jie ,"The Research of NIDS Based on Improved GA" Wireless Communications, Networking and Mobile Computing, conference IEEE 2009

[23] Firas Alabsi and Reyadh Naoum(2012, April), "Fitness Function for Genetic Algorithm used in Intrusion Detection System", International Journal of Applied Science and Technology, Vol. 2, pp. 632-637

[24] Khalid Jebari ,"Selection Methods for Genetic Algorithms ",International Journal of Emerging Sciences , 333-344, December 2013