DOI: 10.21917/ijsc.2012.0047

ANOMALY DETECTION IN NETWORKING USING HYBRID ARTIFICIAL IMMUNE ALGORITHM

D. Amutha Guka
Department of Computer Science, Mother Teresa Women's University, Tamil Nadu, India
E-mail: amuthaguka@yahoo.co.in

Abstract
Especially in today's network scenario, when computers are interconnected through internet, security of an information system is very important issue. Because no system can be absolutely secure, the timely and accurate detection of anomalies is necessary. The main aim of this research paper is to improve the anomaly detection by using Hybrid Artificial Immune Algorithm (HAIA) which is based on Artificial Immune Systems (AIS) and Genetic Algorithm (GA). In this research work, HAIA approach is used to develop Network Anomaly Detection System (NADS). The detector set is generated by using GA and the anomalies are identified using Negative Selection Algorithm (NSA) which is based on AIS. The HAIA algorithm is tested with KDD Cup 99 benchmark dataset. The detection rate is used to measure the effectiveness of the NADS. The results and consistency of the HAIA are compared with earlier approaches and the results are presented. The proposed algorithm gives best results when compared to the earlier approaches.

Keywords:
Anomaly Detection, Artificial Immune System

1. INTRODUCTION

For the past two decades there is rapid development of communication networks through computers. Internet is one of the important infrastructures in this modern world. The number of internet users is rapidly increased for business applications and other online applications. But the internet users face number of problems like cyber crime, cyber threats etc.

The network security is to protect of networks and their services from unauthorized modification, destruction or disclosure. The important function of computer security is to prevent anomaly. Anomaly detection is another significant method used to secure computer system. The major objective of anomaly detection is to detect unauthorized use, misuse and abuse of computer systems.

Excellent Intrusion Detection System (IDS) will act as a house burglar alarm. If unauthorized users try to enter the computer system network, the IDS will give information to the owner [1]. Anomaly detection is the process of monitoring and analyzing events of a computer system or network and tries to find anomalies. The important goal of an IDS is to prevent an attack and also to detect it as quickly as possible and alert the right people who can then take the appropriate action.

There are two types of anomaly detection systems one is a host based IDS and the other one is network node based IDS. Both have their own advantages and disadvantages.

A host-based IDS (HIDS) is an application installed on the host for monitoring purposes [2]-[4]. It analyses the operating system, network packets or logs, running applications and if an anomaly is detected, an alarm is sent to a central monitoring instance.

A network-based IDS (NIDS) is a commercial product installed on some special hardware which is positioned on a network node. It captures and analyses network packets that go through the node it monitors. One single NIDS or sensor, intelligently placed, can monitor several hosts independently of their operating system [5]. The captured network packets are analyzed locally and if an attack is detected, an alarm message is sent to a central monitoring instance.

There are two different detection mechanisms IDS can use to find anomalies or attack attempts: the misuse detection and the anomaly detection.

The misuse detection approach is used in commercial products, monitors and analyses system events looking for a known event or sequence of events that represents an attack; this event or sequence of events is stored in the form of a signature. One disadvantage of the misuse detection is that if the signatures database is not up to date or if a new attack is used for which there exists no signature yet, the IDS will find nothing suspicious. Another problem that can exist is if the signatures are too specifically bound to a given attack, the IDS will not be able to detect variants of the attack. It is nevertheless due to this specificity that the false positive or false alarms rate is very low.

The anomaly detection method is used to detect unusual behaviours (i.e. anomalies). The anomaly IDS needs to create a normal/attack behaviour profile and train the system on this normal/attack. The anomaly IDS compares the intruder data with normal/attack profile and it finds whether it is normal or attack.

Because of its complexity in anomaly detection more number of researchers is doing research in this area. In last three decades more number of research papers has been published in the area anomaly detection. In the network security the primal issue is anomaly detection.

In this paper a hybrid AIS is developed for the anomaly detection in networking, which is based on NSA. In this NSA detectors are generated using Genetic Algorithm.

2. NATURAL IMMUNE SYSTEM AND AIS

One of the most complex systems in our body is Natural Immune System (NIS). The main purpose of the immune system in our human body is to protect the body from damage that can be caused by harmful entities that are either from body itself or from foreign. The NIS is very complex and difficult to understand [6]. The complexity NIS represents an advantage since it provides a rich source of inspiration for bio-inspired computing.

There are two main parts in the NIS, one is the immune system and the other one is adaptive immune system [7]. When an attack occurs, the natural immune system is the first one to generate a response. This response is not specific, but in many cases, it is able to repel the attack. If the natural immune system fails in thwarting the anomaly, then the adaptive immune system takes over. The adaptive response is more specific, resulting in a more effective response.

The adaptive immunity is the most interesting part of the NIS [8]. The past encounters (virus, bacteria, foreign molecules, etc) are identified in the adaptive immune system with antigens in such a way that the next time the antigen appears. This mechanism is called immune memory [9]. Another interesting mechanism of the adaptive immune system is the self/non-self recognition [10]. The NIS is able to recognize which cells are its own (self) and which are foreign (non-self); thus, it is able to build its defence against the attacker instead of self-destructing.

An important feature of the human immune systems is its ability to maintain diversity and generality. It is able to detect a vast number of antigens with a smaller number of antibodies. In order to make this possible, it is equipped with several useful functions [11]. One such function is the development of mature antibodies through the gene expression process. The human immune system makes use of gene libraries in two types of organs called the thymus and the bone marrow. When a new antibody is generated, the gene segments of different gene libraries are randomly selected and concatenated in a random order, see Fig.1. The main idea of this gene expression mechanism is that a vast number of new antibodies can be generated from new combinations of gene segments in the gene libraries.

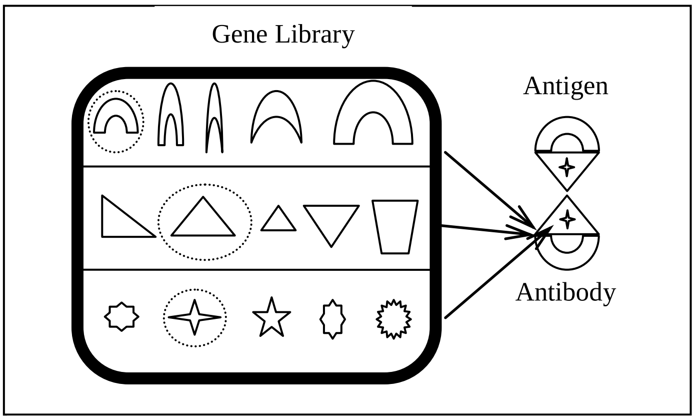

Fig.1. Gene Expression Process

However, this mechanism introduces a critical problem. The new antibody can bind not only to harmful antigens but also to essential self cells. To help prevent such serious damage, the human immune system employs negative selection. This process eliminates immature antibodies, which bind to self cells passing by the thymus and the bone marrow. From newly generated antibodies, only those which do not bind to any self cell are released from the thymus and the bone marrow and distributed throughout the whole human body to monitor other living cells. Therefore, the negative selection stage of the human immune system is important to assure that the generated antibodies do not to attack self cells.

The Artificial Immune System (AIS) is a relatively new field that mimics the mechanisms of the NIS. The AIS is used to solve the problems.

Artificial Immune System is defined as a computational intelligence which is inspired by theoretical immunology and observed immune functions, principles and models, which are applied to problem solving. The field of AIS is relativity new and draws upon work by many theoretical immunologists to name a few.

3. GENETIC ALGORITHM [12]

Genetic Algorithms (GAs) are adaptive search and nontraditional optimization algorithms based on mechanics of natural selection and natural genetics. They are robust in complex search spaces and are versatile in their application. The main characteristics of GAs are as follows:

i. GAs work with the coding of the parameter set not the parameter themselves.
ii. GAs search from a population of points, not from a single point.
iii. GAs use payoff (objective function) information, into derivatives or other auxiliary knowledge.
iv. GAs use probabilistic transition rules, not deterministic rules.
v. GAs is based on the principle of the survival of the fittest.

Genetic algorithm is a search and optimization technique operated on the principle of the “survival of the fittest”, where weak individuals die before reproducing while stronger ones survive and bear many offspring and breed children, which often inherit the qualities that are, in most cases superior to their parents.

3.1 UNDERLYING PRINCIPLES OF GA

To really appreciate the technique, the analogy to the biological systems must be understood. Moreover, the GA uses many of the same terms which biologists use. The nature of a living organism is described by the specific structure of the DNA molecules, which are present in the cell. The DNA is really information coded chemically and can be thought of very long strings of bits. One such string is called chromosome and each bit is called a gene [13, 14].

When a cell in an organism reproduces, it first duplicates its DNA. The cell reproduced may be just like the parent or it may be different.

3.2 GA OPERATORS

GAs begins with a population of strings created randomly. Thereafter, each string in the population is evaluated. The population is then operated by three main operator’s; reproduction, crossover and mutation to create a better population. The population is further evaluated and tested for termination. If the termination criteria are not met, the population is again operated by the above three operators and evaluated. This procedure is continued until the termination criteria are met. One cycle of these operators and the evaluation procedure is known as a generation in GA terminology [15-17].

3.2.1 Reproduction:

Rank selection method is used for reproduction. The individuals in the population are ranked according to fitness, and the expected value of each individual depends on its rank rather than on its absolute fitness [18]. Ranking avoids giving for the largest share of offspring to a small group of highly fit individuals, and thus reduces the selection pressure when the fitness variance is high. It also keeps up selection pressure when the fitness variance is low: the ratio of expected values of individuals ranked i and i+1 will be the same whether their absolute fitness difference are high or low.

The linear ranking method proposed by Baker [19] is as follows. Each individual in the population is ranked in increasing order of fitness from 1 to N. The expected value of each individual 'i' in the population at time 't' is given by The expected value of each individual 'i' in the population at time 't' is given by,

$$\text{Expected Value (i, t)} = (min) + (max\text{-}min) \times \frac{\text{rank(i,t)-1}}{\text{N-1}} \qquad (1)$$

where, N = Sample size, min = 0.4 and max = 1.6.

After calculating the expected value of each rank, reproduction is performed using Monte Carlo simulation by employing random numbers.

An example for Reproduction operation is given below:

Table.1. Rank Order Selection Method

Rank	Expected Value	Probability	Cumulative Probability	Random Number	New rank
1	0.40	0.02	0.02	0.174	7
2	0.46	0.023	0.043	0.177	7
3	0.53	0.027	0.07	0.774	17
4	0.59	0.03	0.1	0.662	16
5	0.65	0.033	0.133	0.142	6
6	0.72	0.036	0.169	0.684	16
7	0.78	0.039	0.208	0.269	9
8	0.84	0.042	0.25	0.851	18
9	0.91	0.046	0.3	0.111	5
10	0.97	0.049	0.345	0.165	6
11	1.03	0.052	0.397	0.264	9
12	1.09	0.055	0.452	0.952	20
13	1.16	0.058	0.51	0.678	16
14	1.22	0.061	0.571	0.973	20
15	1.28	0.064	0.635	0.732	16
16	1.35	0.068	0.703	0.752	16
17	1.41	0.071	0.774	0.64	16
18	1.47	0.074	0.848	0.258	9
19	1.54	0.077	0.925	0.454	13
20	1.60	0.08	1	0.616	15

Reproduction will select against those string in subsequent generations. n strings, n random numbers between zero and one are created at random. Then a string that represents a chosen random in the cumulative probability range for the string is copied to the mating pool. This way, the string with a higher fitness value will represent a larger range in the cumulative probability values and therefore has a higher probability of being copied into the mating pool. On the other hand, a string with a smaller fitness value represents a smaller range in cumulative probability values and has a smaller probability of being copied into the mating pool. This is the reproduction operation.

3.2.2 Crossover:

In the crossover, new strings are created by exchanging information among strings of the mating pool. In crossover operator two strings are picked from the mating pool at random and some portions of the strings are exchanged between the strings. The two strings participating in the crossover operation are known as parent strings and the resulting strings are known as child strings [20].

The single point crossover is used in this HAIA. In single point crossover, one crossover point is selected, string from beginning of chromosome to the crossover point is copied from one parent, and the rest is copied from the second parent. Single point crossover operation is used in this HAIA, explained in the following Fig.2.

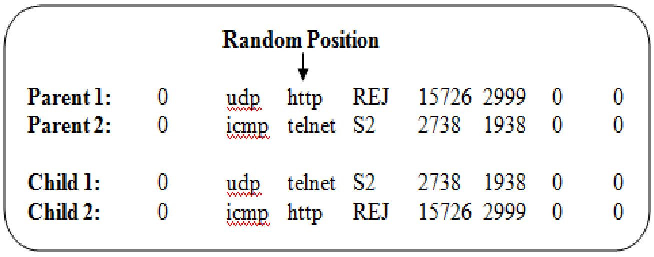
Random Position
Parent 1: 0 udp http REJ 15726 2999 0 0
Parent 2: 0 icmp telnet S2 2738 1938 0 0
Child 1: 0 udp telnet S2 2738 1938 0 0
Child 2: 0 icmp http REJ 15726 2999 0 0

Fig.2. Single Point Crossover

The crossover operator is carried out with a probability known as crossover probability (Cp). Crossover is nothing but exchange of a portion of strings at a point called crossover site. The two strings, which take part in the crossover operation, are also selected at random. Here partial mapped crossover is performed i.e., crossover site is selected and the genes of one string between the sites are swapped with another string.

3.2.3 Mutation:

Mutation is also done randomly for each gene and it depends upon another parameter called mutation probability (Mp). Here one gene is selected at random and the mutation operation is performed. The inversion mutation is followed in this HAIA. In this inversion mutation, an attribute comes out from one chromosome and goes to another chromosome, while a feature from latter chromosome comes to the former chromosome. Thus the genes are mutually interchanged.

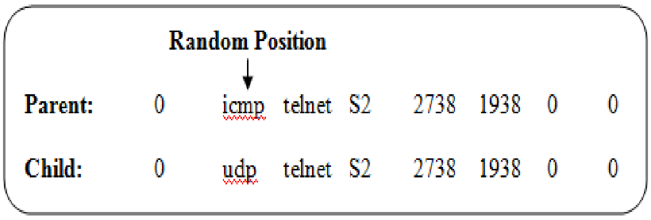
Random Position
Parent: 0 icmp telnet S2 2738 1938 0 0
Child: 0 udp telnet S2 2738 1938 0 0

Fig.3. Single Point Mutation

4. THE HYBRID ALGORITHM

Forrest et al. [21], [22] proposed AIS based negative selection algorithm for various anomaly detection problems.

The normal behaviours of the patterns are called 'self'. This algorithm defines 'self' as normal behaviour patterns of a monitored system. It generates a number of random patterns that are compared to each self defined pattern.

If any randomly generated pattern matches with the self pattern, this pattern fails to become a detector and thus it is removed. Otherwise, it becomes a 'detector' pattern and monitors subsequent profiled patterns of the monitored system shown in the Fig.4.

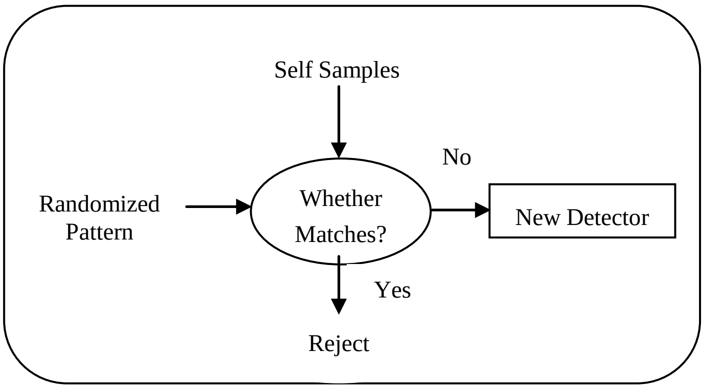

Fig.4. Detector Set Generation in AIS

During the monitoring stage, if a 'detector' pattern matches any newly profiled pattern, it is then considered as a new anomaly which must have occurred in the monitored system shown in the Fig.5.

The proposed HAIA is similar to the AIS based negative selection algorithm. Only the detectors are generated by using GA shown in the Fig.6. All other procedures are similar to negative selection algorithm shown in Fig.5.

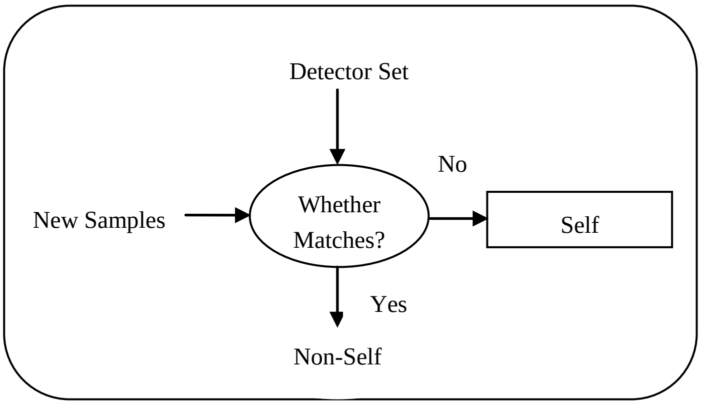

Fig.5. Negative Selection Algorithm in AIS

Initially the KDD Cup 99 dataset is separated as normal file and attack file. From the normal and attack file random data records are chosen for training. The GA parameters are selected. Initial random population is generated and it is evaluated by using fitness function and then the initial population is stored as an initial detector set.

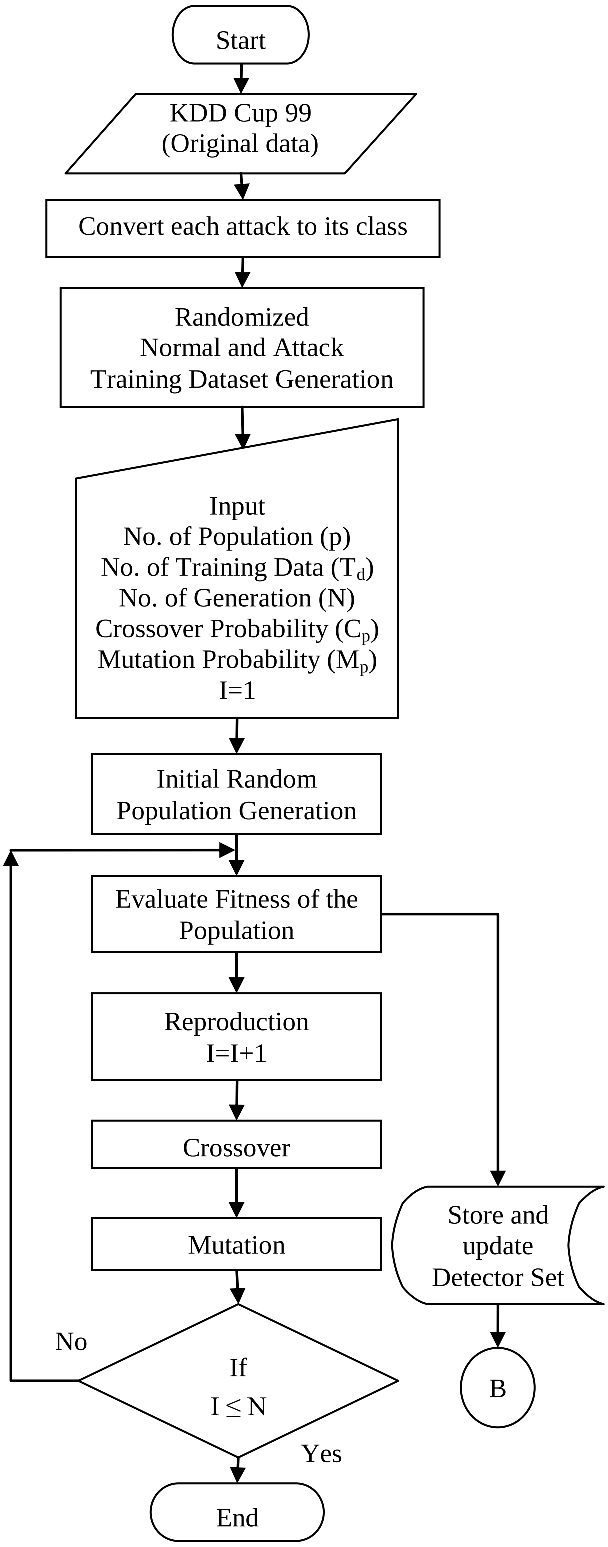
Start
KDD Cup 99 (Original data)
Convert each attack to its class
Randomized Normal and Attack Training Dataset Generation
Input
No. of Population (p)
No. of Training Data (T_d)
No. of Generation (N)
Crossover Probability (C_p)
Mutation Probability (M_p)
I=1
Initial Random Population Generation
Evaluate Fitness of the Population
Reproduction I=I+1
Crossover
Mutation
Store and update Detector Set
B
No
If I ≤ N
Yes
End

Fig.6. HA Detector Set Generation

After that the GA iteration process starts, once iteration is over then the detector set is updated based on the higher value of fitness function. Once the number of iteration is over then the output from this process is a well formulated detector set.

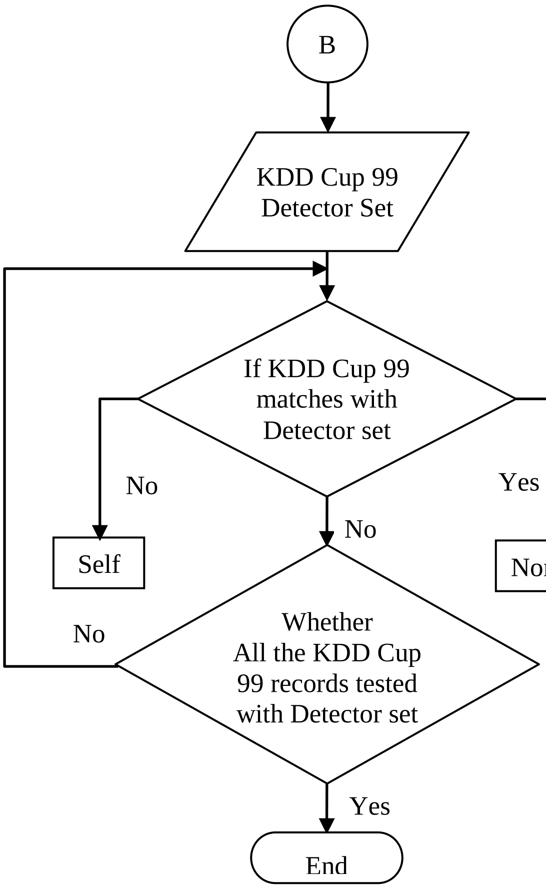
B
KDD Cup 99 Detector Set
If KDD Cup 99 matches with Detector set
No
Yes
Self
Non self
No
Whether All the KDD Cup 99 records tested with Detector set
No
Yes
End

Fig.7. HA Anomaly Detection

Once the detector set is generated from the GA then overall KDD Cup 99 dataset is compared with the detector set. If there are any matches then that particular record is identified as an anomaly.

4.1 FITNESS FUNCTION

The efficiency of this HAIA is based on how effectively the detector set is generated. The detector set is generated by using the GA and the fitness function will decide the effective detector set. The fitness is determined by using the following equations:

$$\text{Fitness of the string} = NF - AF$$
$$NF = A/B \qquad (2)$$
$$AF = C/D$$

where, NF = Normal fitness

AF = Attack fitness

A = Number of normal training data match with string (at least 5 fields)

B = Total number of normal training data

C = Number of attack training data match with string (at least 5 fields)

D = Total number of attack training data

4.2 HAIA MEASURING PARAMETERS

The anomaly is identified by using HAIA. The effectiveness of the HAIA is measured by Detection Rate (DR) and False Alarm Rate (FAR) are calculated using the following equation:

$$DR = \frac{TP}{TP + FN} \qquad (3)$$

$$FAR = \frac{FP}{TN + FP} \qquad (4)$$

where, DR = Detection rate

FAR = False alarm rate

TP = True positive – anomalous elements identified as anomalous;

TN = True negative – normal elements identified as normal;

FP = False positive – normal elements identified as anomalous

FN = False negative – anomalous elements identified as normal

5. EXPERIMENTATION

This section presents the details of the development and testing of HAIA for Anomaly Detection system. The HAIA model is developed using VB in HP Pavilion dv4 Notebook PC with 2.20 GHz processor with 2.97 GB of RAM.

In the experimental testing the following input parameters are considered in the KDD Cup 1999 dataset. The KDD Cup 1999 dataset contains 494020 records, each with 41 attributes out of which only first eight attributes (shown in the Table.2) are considered in this HAIA.

Table.2. KDD Cup99 Selected Input Features Details

Sl. No.	Attributes
1	duration
2	protocol_type
3	service
4	flag
5	src_bytes
6	dst_bytes
7	land
8	wrong_fragment

The twenty two numbers of attack types in addition to normal records are available in the KDD Cup 1999 benchmark dataset. Table.3 shows the description of attacks with total number of records.

Table.3. KDD Cup 1999 Attack Details

Sl. No.	Name of intruder	No. of records	Sl. No.	Name of intruder	No. of records
1	smurf	280790	13	phf	4
2	guess_passwd	53	14	nmap	231
3	pod	264	15	multihop	7
4	teardrop	979	16	neptune	107201
5	portsweep	1040	17	warezmaster	20

6	ipsweep	1247	18	loadmodule	9
7	land	21	19	perl	3
8	ftp_write	8	20	warezclient	1020
9	back	2203	21	spy	2
10	imap	12	22	rootkit	10
11	buffer_overflow	30	Normal		97277
12	satan	1589	**Total**		494020

5.1 STEPS INVOLVED IN HAIA

```
Step1: Random population is generated by using random numbers from the KDD Cup 99 dataset. Only first eight features of the dataset are generated.
       Example:
              0, udp, telnet, REJ, 15726, 2999, 0, 0
              0, icmp, http, S2, 2738, 1938, 0, 0
Step2: Evaluate Fitness (Objective Value Calculation) for each string
        Detector set creation
              If it is first generation
              Store all strings as detector set
       Else
              Take the best string (fitness) from this population replace with detector set's worst string
Step3: Reproduction
              Rank order selection method used.
              The linear ranking method proposed by Baker is as follows: Each individual in the population is ranked in increasing order of fitness from 1 to N. The expected value of each individual 'i' in the population at time't' is given by using Eq.(1)
Step4: Crossover
       For all pair of strings
       Generate a random number (r) which falls 0 to 1.
       if r < crossover probability (Cp=0.6) then
              Generate random number (p) which falls 1 to number of fields
              Interchange the field (p) between the pair
       Else
              Go to next pair
Step5: Mutation
       For each string
         Generate a random number (r) which falls 0 to 1.
       if r < mutation probability (Mp = 0.02) then
              Generate random number (p) which falls 1 to number of fields
              Change the field by using random no.
       Else
              Go to next string
Step6: Termination criteria
              If Termination criteria (number of generation) is satisfied then STOP
       Else
              Go to Step 2.
Step7: Anomaly Detection
              For each string in KDD Cup 99 test data
              Compare the first 6 fields of test string with detector set strings (which is created from GA)
              If no. of fields match with detector set string is greater than or equal to 4 then
              The test string is identified as anomaly
       Else
              Go to next test string
       End
```

The HAIA algorithm tested on KDD Cup 99 dataset with various testing parameters. The Table.4 shows the Population (P) size, Training data (T) size, number of generation (G), DR and FAR. The result shows (Table.4) that if the population size and the number of iteration is more than the DR and FAR is low.

Table.4. KDD Cup 99 HAIA Results

P	T	G	Execution	DR (%)	FAR (%)
10	50	10	1:54:24	99.25	1.05
10	10	10	1:54:41	99.25	1.05
100	**5000**	**10**	**2:35:49**	**28.99**	**49.73**
5	50	5	1:55:48	99.27	1.02
100	**5000**	**100**	**2:28:32**	**28.99**	**49.73**
20	100	10	1:57:46	98.43	2.17
20	100	10	1:58:04	98.43	2.17

The performance of the proposed HAIA is compared with some other anomaly detection approaches. In [23], Guisong Liu et al. tested Hierarchical neural network principal component analysis and presented the performance comparison. The proposed HAIA is compared with all other literature based approaches. The average result of the proposed HAIA gives best detection rate when compared to the earlier NN based approaches [23-29], which is shown in the Table.5. In this HAIA entire KDD Cup 99 dataset is tested and the DR is 99.27%.

Table.5. HAIA Results Comparison with Other Approaches

Results From	Methods	DR
Proposed	HAIA	**99.27**
Literature	Hierarchical neural network principal component analysis (HPCANN) [23]	97.10
	Multiple-Level Hybrid Classifier (MLHC) [24]	90.90
	Back Propagation Learning (BPL) [25]	99.20
	Radial Basis Functions (RBF) [25]	98.00
	Principal Component Analysis Self-Organizing Map (PCASOM) [26]	94.60
	Support Vector Machine (SVM) [27]	99.60
	C45 [28]	95.00
	Principle Components Classifier (PCC) [29]	97.90

6. CONCLUSION

This paper has presented the design and development of HAIA which consists of GA and NSA for NADS. The data required for the development of model have been obtained through the KDD Cup 99 dataset. Totally 22 numbers of attacks from the KDD Cup 99 dataset were considered in the developed model. Simulation results show that this HAIA approaches are very much effective in detecting the various attacks in the system. The effectiveness of the proposed method has been demonstrated through different attacks detection in the NADS. The proposed HAIA technique will be suitable for any network. This approach can be extended to all other NADS benchmark datasets with more number of attack types.

ACKNOWLEDGMENT

The author wishes to thank the Mother Teresa Women's University, Kodaikanal for the support of this research work and the reviewers for their valuable suggestions.

REFERENCES

[1] Bace and P Mell. "*Intrusion Detection Systems*", NIST Special Publication 800-31. 2001.

[2] Samhain URL: http://www.la-samhna.de/samhain

[3] Prelude URL: http://prelude-ids.org

[4] Snort URL: http://www.snort.org

[5] McHugh J, "Intrusion and intrusion detection", *International Journal of Information Security*, Vol. 1, No. 1, pp. 14-35, 2001.

[6] Janeway C A, "How the immune system recognizes invaders", *Scientific American*, Vol. 269, No. 3, pp. 72-79, 1993.

[7] Varela F, Coutinho A, Dupire B and Vaz N, "Cognitive networks: immune and neural and otherwise, "*Theoretical Immunology: Part Two, SFI Studies in the science of Complexity*, pp. 359-371, 1988.

[8] Dasgupta D, "An overview of artificial immune systems and their applications", *Artificial immune systems and their applications*, pp. 3- 23, Springer-Verlag, Inc., 1999.

[9] Kuby J "*Immunology*". W. H. Freeman and Co., 3rd edition, 1997.

[10] Coutinho A, "The self non-self discrimination and the nature and acquisition of the antibody repertoire," *Annals of Immunology. (Inst. Past.)*, Vol. 131D, 1980.

[11] Kim J and Bentley P, "The Human Immune System and Network Intrusion Detection", *7th European Conference on Intelligent Techniques and Soft Computing (EUFIT '99), Aachen, Germany*, pp. 1244 - 1252, 1999.

[12] P Venkumar and K Chandra Sekar, "Design of Cellular Manufacturing System using Non-Traditional Optimization algorithms" in *Operations Management Research and Cellular Manufacturing: Innovative Methods and Approaches*, Publisher: IGI Global, pp. 99-136, 2011.

[13] Goldberg D.E, "*Genetic algorithms in search optimization and machine learning. Reading, MA*", Addison-Wesley, 1989.

[14] Gen M and Cheng R, "*Genetic algorithms and engineering design. MA*", Wiley Inter science Publication, 1997.

[15] Venugopal V and Narendran T, "TA genetic algorithm approach to the machine component grouping problem with multiple objectives", *Computer and Industrial Engineering*, Vol. 22, pp. 469–480. 1992.

[16] Saniee Abadesh M, Habibi J and Lucas C, "Intrusion detection using a fuzzy genetics-based learning algorithm", *Journal of Network and Computer Applications*, Vol. 30, pp. 414-428, 2007.

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

[18] Davis L (Ed.), "*Handbook of genetic algorithms*", New York: Nostrand Reinhold, 1991.

[19] Man K. F, Tang K. S and Kwong S, "*Genetic algorithms: Concepts and design*", London: Springer, 1999.

[20] Baker J. E, "Adaptive Selection Methods for Genetic Algorithms," *Proceedings of an International Conference on Genetic Algorithms and Their Applications*, pp. 101-111, Hillsdale, NJ: Lawrence Erlbaum Associates, 1985.

[21] Forrest S, Perelson A, Allen L and Cherukuri R, "Self-non self discrimination in a computer," *Proceedings of IEEE Symposium on Research in Security and Privacy*, pp. 202–212, 1994,

[22] Forrest S, Smith R.E, Javornik B, Perelson A.S, "Using genetic algorithms to explore pattern recognition in the immune system", *Evolutionary Computation*, Vol. 1, No. 3, pp. 191–211, 1993.

[23] Guisong Liu, Zhang Hi and Shangming Yang, "A hierarchical intrusion detection model based on the PCA neural networks," *Neuro Computing*, Vol. 70, No. 7-9, pp. 1561-1568, 2007.

[24] C Xiang and S.M Lim, "Design of multiple-level hybrid classifier for intrusion detection system", *Proceedings of the IEEE Workshop Machine Learning for Signal Processing*, pp.117–122, 2005.

[25] Z Chunlin, J Ju and K Mohamed, "Intrusion detection using hierarchical neural networks", *Pattern Recognition Letters*, Vol. 26, No. 6, pp. 779–791, 2005.

[26] G Liu and Z Yi, "Intrusion Detection Using PCASOM Neural Networks", *Proceedings of Third International Conference on Advances in Neural Networks*, Vol. 3973, Springer, Berlin, Heidelberg, pp. 240–245, 2006.

[27] C Wun-Hua, H Sheng-Hsun and S Hwang-Pin, "Application of SVM and ANN for intrusion detection", *Computers and Operations Research*, Vol. 32, No. 10, pp. 2617–2634, 2005.

[28] L Pavel, D Patrick, S Christin and K Rieck, "Learning Intrusion Detection: Supervised or Unsupervised", *International Conference on Image Analysis and Processing*, Vol. 3617, pp. 50–57, 2005.

[29] M Shyu, S Chen, K Sarinnapakorn and L Chang, "A Novel Anomaly Detection Scheme Based on Principal Component Classifier", *Proceedings of IEEE Foundations and New Directions of Data Mining Workshop*, pp. 172–179, 2003.