Real Time Intrusion Detection System Using GA

[1]Shaiwali Sahu, [2] Ajay Phulre
Department of Computer Science & Engineering ,
Shri Balaji Institute of Technology and Management , Betul, MP, India
Email – [1]saywaly@gmail.com, [2]aphulre@gmail.com

Abstract *Today, as the advancement of computer technology and internet for users the importance of data is increased and it becomes a precious asset to any of the firm. But unfortunately the threat (Intrusion) to the same is also increasing day by day. Special & unique types of attacks are introduced rapidly. So there is a need for better and more efficient intrusion detection systems also increases. The main problem with current intrusion detection systems (IDS) is high rate of false alarms. There is lot of techniques and areas which plays vital role in building security applications. This paper presents a technique of applying evolutionary algorithm i.e. Genetic Algorithm to Intrusion Detection System. It also provides a brief introduction to the parameters and evolution process of a GA and how to implement it in real IDS.*

Key Words: *DDOS; Evolutionary algorithm; GA-RIDS; Genetic Algorthm; Intrusion; IDS; threats*

1. INTRODUCTION:

The main problem with current intrusion detection systems is high rate of false alarms triggered off by attackers. Effective protecting the network against malicious attacks remains problem in both research and the computer network managing professionals. Improved monitoring of malicious attacks will require integration of multiple monitoring systems. A series of analytical and mathematical models are used to acquire potential benefits of multiple sensors for reducing false alarms. Today, the number of attacks against large computer systems or networks is growing at a rapid pace.

One of the major threats to cyber security is Distributed Denial-of-Service (DDoS) [3, 5] attack. In which the victim network element(s) are bombarded with high volume of fictitious attacking packets originated from a large number of Zombies. The aim of the attack is to overload the victim and render it incapable of performing normal transactions. To protect network servers, network routers [4, 8] and client hosts from becoming the handlers, Zombies and victims of distributed denial-of-service (DDoS) attacks. Genetic algorithm approach can be adopted as a sure shot weapon to these attacks. The central theme of this paper is to explore parameters and evolution process[6] of Genetic Algorithm which helps to detect malicious packet on the network and ultimately helps to block the respective IP addresses.

Genetic algorithm is an evolutionary algorithm which is helpful for search and optimization purpose. They incorporate the concept of Darwin's theory of survival. Many researchers have introduced the use of GA in intrusion Detection and reported very high success rates. We have used GA based approach to find and detect the malicious packets and IP addresses on the network. The main reason behind selecting GA for this task is due to inherent evolutionary treatment in the algorithm which allows us to define our own fitness function based on which only those members or rules are selected that satisfy our fitness criterion.

With this approach in mind we have designed GA based system and implemented fitness function on the processes of GA. The aim is to get high prediction rate and minimum false positive rates on network traffic captured by the system. The training of the system is carried out on the predefined rules while other resting is done on the real time data sets generated by the firewall system. The results generated after successful execution of the algorithm are thus justifying the choice, performance and applicability of genetic algorithm into the Intrusion Detection System.

2. LITERATURE REVIEW:

The Intrusion Detection System has undergone rapid changes and is using new evolved techniques to generate better results. There are several approaches for solving intrusion detection problems assizes on the network.

Wei Li [6] has describe GA based IDS with a methodology of applying genetic algorithm into network intrusion detection techniques. This implementation of genetic algorithm is unique as it considers both temporal and spatial information of DARPA data set Rule Set Rule Base Network Sniffer GA network connections during the encoding of the problem; therefore, it should be more helpful for identification of network anomalous behaviors.

B. Uppalaiah, T. Bharat et al. [7] presents the Genetic Algorithm for the Intrusion detection system for detecting DoS, R2L, U2R, Probe from DD99CUP data set. The architecture of the system along with implementation of the software for the proposed technique is also discussed. The time to get thorough with three features to describe the data will be reduced with a combination of Genetic Algorithm based IDSs. there system is more flexible for usage in different application areas with proper attack taxonomy. Genetic Algorithm detects the intrusion while correlation techniques identify the features of the network connections .The results shows that we have specified set of rules and

high Dos, R2L, U2R, Probe attack detect rate. In Optimizing the parameters present in the algorithm reduces the training time.

Srinivasa K G, SaumyaChandra et al.[8] presents IGIDS, where the genetic algorithm is used for pruning best individuals in the rule set database. The process makes the decision faster as the search space of the resulting rule set is much compact when compared to the original data set. This makes IDS faster and intelligent.

Anup Goyal and Chetan Kumar [9] has presented a machine learning approach known as Genetic Algorithm (GA), to identify such harmful/attack type of connections. The algorithm takes into consideration different features in network connections such as type of protocol, network service on the destination and status of the connection to generate a classification rule set. Each rule in rule set identifies a particular attack type. For this experiment, they implemented a GA and trained it on the KDD Cup 99 data set to generate a rule set that can be applied to the IDS to identify and classify different types of attack connections.

Brian E. Lavender [10] proposed the integration of genetic algorithms (GA) into SNORT to enhance SNORT at performing Network Intrusion Detection (NID).

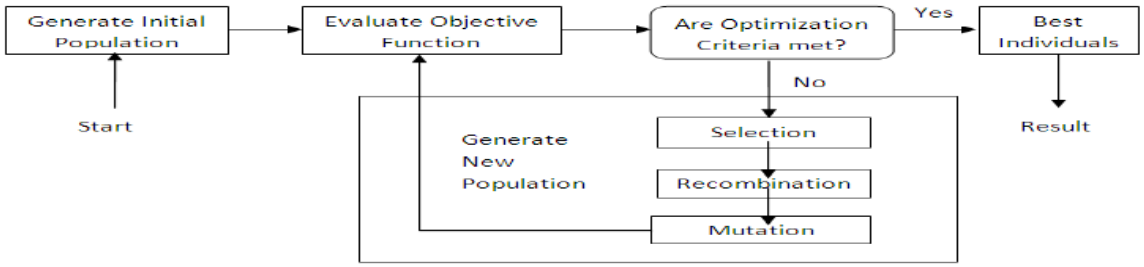

Figure 1: General Architecture of a Genetic Algorithm

3.IMPLEMENTED METHODOLOGY:

The proposed system overview is shown in figure 2 which starts from capturing firewall entries i.e. firewall data sets and then initial filtering is done on the basis of rule defined by the system. This précised data is then input to the GA based algorithm which generates the best individuals.

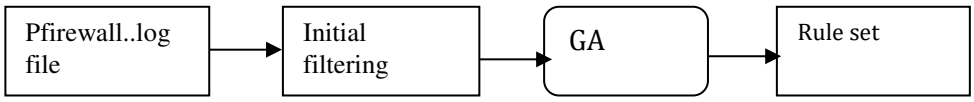

Figure 2: Implemented process of Genetic Algorithm

The detail proposed architecture is shown in figure 4. It starts from initial population generation from pfirewall.log file generated by the firewall system. The packets are the filtered out on the basis of rules. Then the précised data packets go through several steps namely selection, crossover and mutation operation. These processes gets generate best individuals. The generated individuals are the verified by the fitness function to generate the population for next generation.

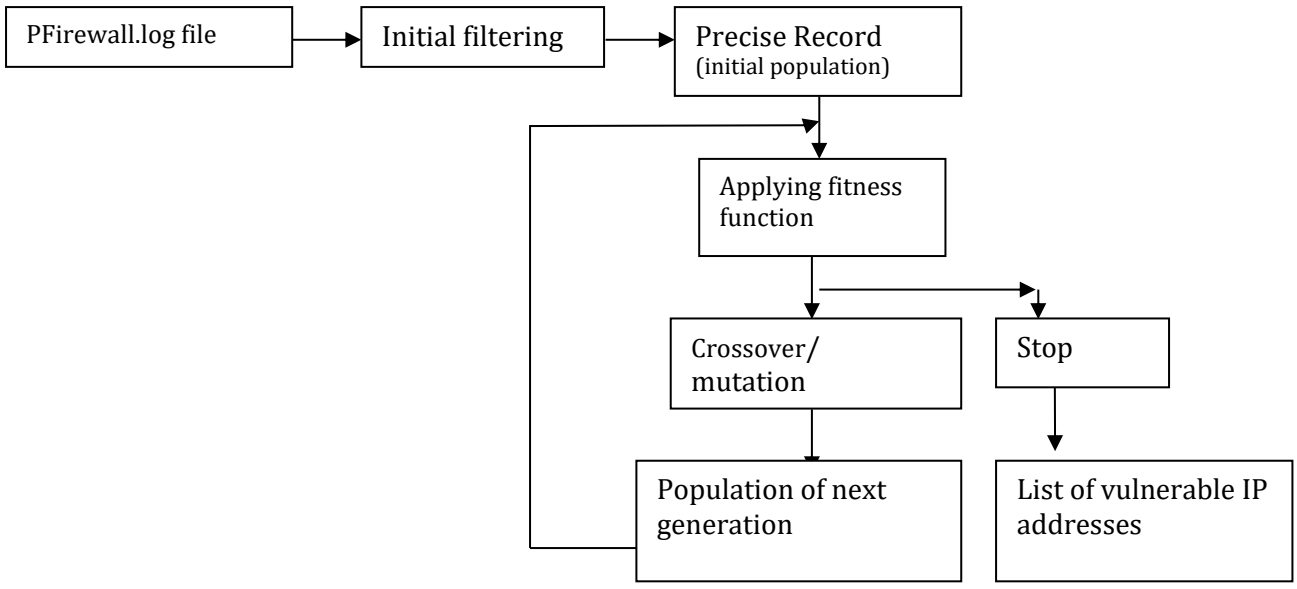

Figure 3: Detailed system architecture for GA-RIDS.

- Encoding of the Chromosomes.

In the GA process it is important to represent the data into some of the encoding formats. There are many encoding methods to represent data string for GA's further process.
Like, binary encoding and real valued encoding.

- Applying fitness function.

Fitness function (or objective function) [12] defines the problem constraints; it measures the performance of all chromosomes in the population.

- Selection operator.

Determines which chromosome(s) [12] from the population will be chosen for recombination; depends on the fitness of the chromosome. The selected chromosomes are called parents. Such selection methods are: fitness-proportion selection, roulette-wheel selection, stochastic universal sampling, local selection and rank selection.

- Crossover operator.

The parents' chromosomes are recombined by one of the crossover methods. It produce one or more new chromosome(s) called offspring(s). Such methods are: Single Point Crossover, Multipoint Crossover, Uniform Crossover and Arithmetic Crossover.

- Mutation operator.

New genetic material could be introduced into the new population through mutation process. [12] This will increase the diversity in the population. For each offspring mutation randomly alters some gene(s). Some

4. EXPERIMENTAL RESULTS AND DISCUSSION:

For experimental analysis our focus is to generate list of IP addresses and there packets which are vulnerable to the server or destined system. The testing is done on the entries generated by the firewall system of machine in pfirewall.log file. The training is done on the predefined data rules. The pfirewall.log file contains the entries of incoming packets with various fields like date/time, action, protocol, srcip, destip, srcport, destport, size, flag, ack, type and info. But for making the connection profile we have used only 5 important fields of it. These are src-ip, dst-ip, src-port, dst-port and size.

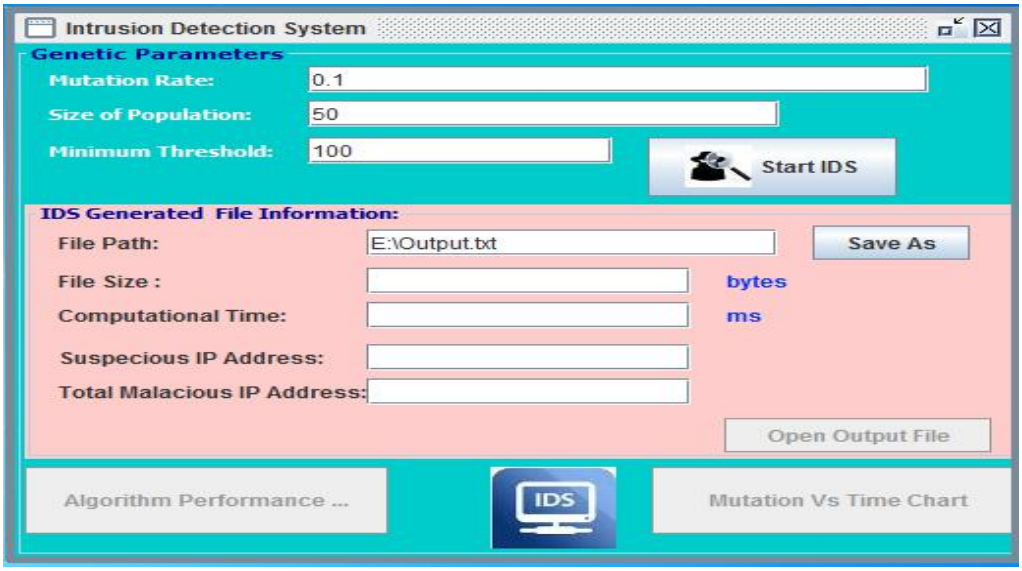

Fig4: IDS Main Frame

For this experiment we have used java software as the frontend tool which code overall GA operator and there evolution process. The training data is stored into the mysql server which is used as the backend to the system. For this experiment we used windows based system with dual core processor (i5) system having 1TB hard disk space and 2 GB RAM to execute the implemented algorithm.

Fig 4 shows IDS main frame having default values for GA like mutation rate, size of population and minimum threshold on which implemented algorithm work to find the malicious ip address on real time.

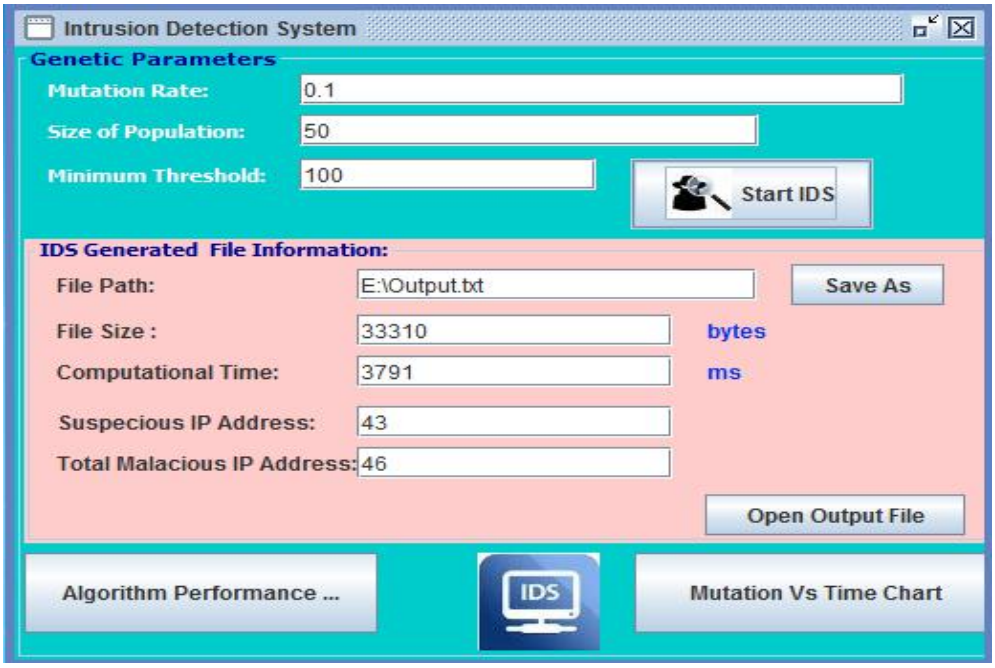

Fig5: IDS Result Frame

Above figure 5 shows the result of IDS with default mutation rate, population and threshold value where we found 43 suspicious IP address and 46 malicious IP address with computational time 33310 mile second. Here fig 6 and fig 7 display the graphical representation of given input with total suspicious and malicious ip address bar chart along with impact of mutation rate over performance time

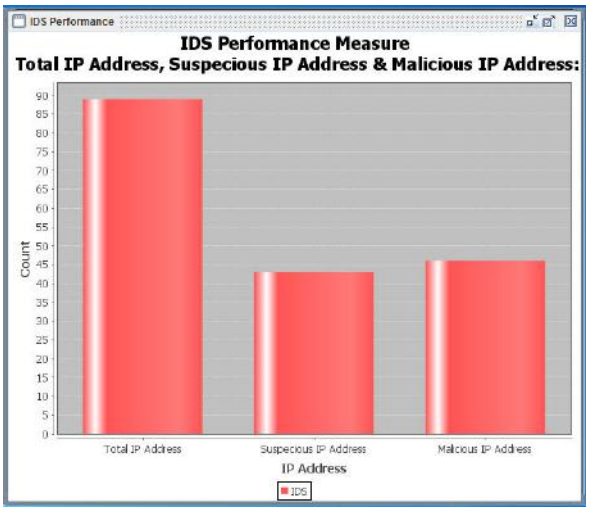

Fig6:Performace Analysis of IDS

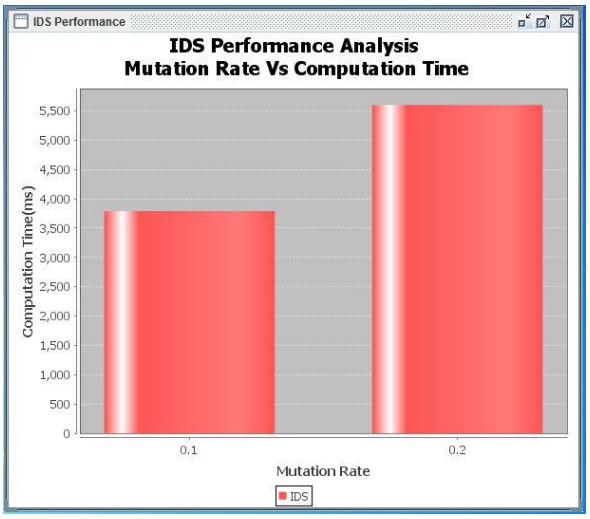

Fig7 IDS Mutation rate Vs Computional time

4. CONCLUSION:

In this paper we have successfully evolved the proper rule set which can detect existing as well as new intrusions. So as the result generated; the system can be integrate with any of the IDS system to improve the efficiency and the performance. The system can also be able to integrate to the input to the firewall system. In this paper, we have discussed the GA processes and evolution operators also discussed the overall implementation of GA into proposed system. The various operators like selection, crossover and mutation are also used.

We are applying single filtration to the system but in future our plan is to apply multiple filters to enhance the system performance and to reduce time complexity of execution. Again we are planning to apply the proposed system output to the security system like Firewall machine to block the traffic whose IP address entries are made.

REFERENCES:

1. T. Lunt, A. Tamaru, F. Gilham, R. Jagannathan, P. Neumann, H. Javitz, A. Valdes, and T. Garvey. (February 1992) "A real-time intrusion detection expert system (IDES)" - final technical report. Technical report, Computer Science Laboratory, SRI International, Menlo Park, California,.
2. K. Ilgun, R. A. Kemmerer, and P. A. Porras.(March 1995) "State transition analysis: A rulebased intrusion detection approach". IEEE Transactions on Software Engineering, 21(3):181–199,
3. John E. Dickerson, and Julie A. Dickerson "Fuzzy Network Profiling for Intrusion Detection" Electrical and Computer Engineering Department Iowa State University Ames, Iowa, 50011.
4. Rui Zhong, and Guangxue Yue (April.2010) "DDoS Detection System Based on Data Mining" ISBN 978-952-5726-09-1 (Print) Proceedings of the Second International Symposium on Networking and Network Security (ISNNS '10)Jinggangshan, P. R. China, 2-4, ,pp.062-065.
5. Dietrich, S., Long, N., and Dittrich, D. 2000. Analyzing distributed Denial of service attack tools: The shaft case. In Proceedings of 14th Systems Administration Conference. New Orleans, Louisiana, USA, 329-339.
6. Wei Li "Using Genetic Algorithm for network intrusion detection"
7. B.Upalhaiah, K. Anand, B. Narsimha, S. Swaraj, T. Bharat, (JAN-MARCH 2012) "Genetic Algorithm Approach to Intrusion Detection System" ISSN: 0976-8491 (online) | ISSN : 2229-4333 (print), IJCST VOL3, ISSUE 1,.
8. Shrinivasa K G, Saumya chandra, Sidharth Kajaria, Shilpita mukharjee, "IGIDS: Intelligent intrusion detection system using Genetic Algorithm", 978-1-4673-0126-8/11/2011 IEEE.
9. Anup Goyal, Chetan Kumar, "GA-NIDS : A genetic algorithm based network intrusion detection system",
10. Atul Kamble,(June, 2010) "Incremental Clustering in data mining using genetic algorithm", IJCTE, Vol 2, No. 3,
11. Shaik Akbar, Dr. J. A. chandulal, Dr. K. Nageswara Rao, G. Sudheer Kumar,(December 2011) "troubleshooting technique for intrusion detection sytem using genetic algorithm", IJWBC, vol 1(3),
12. Suhail Owais, Vaclav Snasel, Pavel Kromer, Ajith abrahim, (2008) "Survey: Using genetic algorithm approach in intrusion detection system techniques", 7th computer information system and industrial management applications, IEEE