IOSR Journal of Engineering (IOSR JEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 45-49

An Evolutionary Approach for Intrusion Detection Using Genetic Algorithm Operators

Ms. Kanchan Gawande[1],Ms. Yamini Laxane[2]
[1,2]*MCA, SRPCE, Nagpur*

Abstract: *today the growths of information technology and internet users impact the importance of data on the network. For every organization operational as well as history data play very important role thus it a valuable asset to any organization. But unfortunately the threat (Intrusion) to the same is also exploding rapidly. Special & new types of attacks are introduced day by day. So the need for better and more efficient intrusion detection systems increases. The primary 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. In this paper we presents evolutionary algorithm technique i.e. Genetic Algorithm for Intrusion Detection System. It also provides a concise introduction to the parameters and evolution process of a GA and how to implement it in real IDS.*

Keywords – *DDOS Attack, Evolutionary algorithm, GA-RIDS, Genetic Algorithm, Intrusion, IDS, threats*

I. Introduction

The major problem with today's intrusion detection systems is a very high rate of fake alarms triggered off by the attacker. So efficient way to protect network against malicious attacks is always difficult in the computer network therefore improved monitoring of malicious attacks will require mixing of multiple monitoring systems. Many analytical series and mathematical models arefrequently used toobtainpotential benefits of multiple sensors for dropping false alarms. Now days,the number of attacksagainstlargecomputersystemsornetworksisrisingatarapidpace.

Todays threats to information cyber security is Distributed Denial-of-Service (DDoS) [3] attack. In which the victim network element(s) are bombarded with a very high volume of fictitious attacking packets originated from a huge number of Zombies. The main aim of the attack is to overload or busy the victim so that victim is incapable of performing normal services or transactions. To protect network computers, servers, routers from becoming the handlers, due to distributed denial-of-service (DDoS) attacks, an evolutionary genetic algorithm approach can be adopted as a positive shot weapon to avoid these attacks. The central idea of this paper is to explore parameters for evolution process [6] of Genetic Algorithm which actually helps to detect malicious packet on the network and eventually helps to block the respective affected IP addresses.

Genetic algorithm is basically an evolutionary approach which is helpful for search and optimization purpose. They include the concept of Darwin's theory of survival. So many researchers have introduced the use of genetic algorithm (GA) in intrusion Detection and it hasvery high success rates. We have also trying to use GA based approach to find and detect the malicious packets and IP addresses on the network. The main key reason behind selecting GA for this task is due to inherent evolutionary treatment in the algorithm which help us to define our own fitness function based on which only those members or rules are selected that satisfy our fitness criterion.

With the above approach we are going to design GA based system and implement fitness function for the processes of GA. The key intent is to get high prediction rate and less false rates on incoming network traffic captured by the IDS. The training of the system is carried out on the some predefined rules and other testing is done on the real time data set file generated by the any firewall system. The results generated after execution of proposed algorithm are thus justifying the desired choices, like performance, applicability of genetic algorithm for Intrusion Detection System.

II. Literature survey

The recent intrusion detection technique changes rapidly by using many new evolved techniques to generate more efficient results. There are various approaches for solving intrusion detection problems on the network.

B. Uppalaiah, T. Bharat et al. [7] has discussed the Genetic Algorithm to the Intrusion detection system for detecting DoS, R2L, U2R, Probe from DD99CUP data set. The implemented architecture of the system along with software technique is also discussed in this paper. The time to get thorough with three features to describe the data will be reduced with a combination of Genetic Algorithm based IDSs. This system is flexible

for usage in different application areas with proper attack taxonomy. Genetic Algorithm detects the intrusion and correlation techniques identify the features of the network connections uniquely .The results shows that we have specified set of rules and high Dos, R2L, U2R, Probe attack detect rate. By optimizing the parameters present in the GA algorithm reduces the trainingtime.

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

Anup Goyal and Chetan Kumar [9] has proposed a new learning approach to identify more harmful/attack type of connections. The discuss algorithm takes into consideration of different fields in network connections such as network service on the destination, type of protocol and status of the connection to generate a classification rule set. Each and every rule in rule set is designed in such a way that it 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 specific rule set that can be applied to the IDS to identify and classify different types of attack connections.

Brian E. Lavender [10] proposed the mixing of genetic algorithms (GA) into SNORT to improve SNORT at performing Network Intrusion Detection (NID).Shaik Akbar et al. [11] have discussed an algorithm which identifies attack type using Genetic Algorithm. The proposed algorithm considers different parameters like protocol type, src_bytes and duration to evolve a new rule set. The specified Genetic Algorithm approach is used on KDDCUP 99 dataset in order to generate a intrusion detection rule set which applied on Intrusion Detection System to identify different types ofattacks.

III. Introduction Of Geneticalgorithm

Genetic algorithms are a branch of evolutionary algorithms [8] used in search and optimization techniques. The three dominant functions of a genetic algorithm i.e., selection, crossover and mutation correspond to the biological process: The survival of the fittest (As shown in Figure1).

In genetic algorithm, there is a population of strings (called chromosomes or the genotype of the genome), which encode and indent solutions (called individuals, creatures, or phenotypes).[09] Traditionally, solutions are represented in binary as strings of 0s and 1s, but other encodings are also possible. The evolution usually starts from a population of randomly generated individuals and evolves over generations. In each generation, the fitness of every individual in the population is evaluated, multiple individuals are stochastically selected from the current population (based on their fitness), & modified (recombined and possibly randomly mutated) to form a new population[5]. The new population is then used in the next iteration of the algorithm. Commonly, the algorithm terminates when either a maximum number of individuals are there in a generation, or a satisfactory fitness level has been reached for the population. If the algorithm has terminated due to a maximum number of individuals, a satisfactory solution may or may not have beenreached.

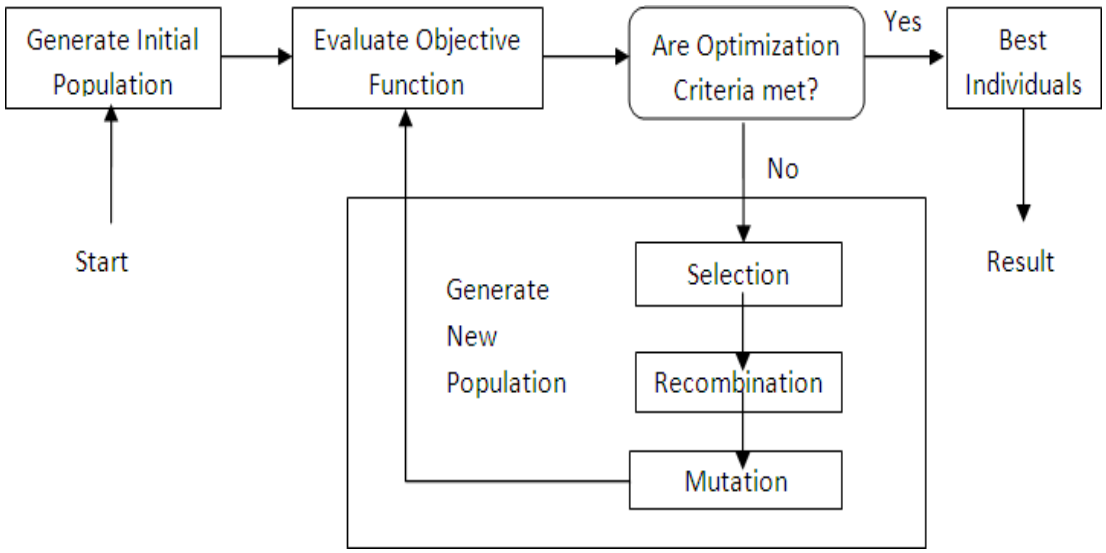

Figure 1: *Genetic Algorithm Working structure*

3.1 GENETIC ALGORITHM APPROACH

GA evolves the population of chromosomes (individuals) as the process of natural selection.[12] It generate(s) new chromosome(s) (offspring) during its process. GA process uses a set of genetic operators (selection operator, crossover operator and mutation operator), and evaluate chromosome using the fitness function.GA consists of population of chromosomes that reproduced over set of generations according to their fitness in an environment. Chromosomes that are most fit are most likely to survive, mate, and bear children.GA terminate the process by define fixed maximal number of generations or as the attainment of an acceptable fitness level, or if there are no improvements in the population for some fixed generations, or for any other reason. The standard GA processes is shown in figure 2. It contains various steps which includes: encoding chromosomes, generating initial population, fitness function evaluation, then applying one of the operators. The process will stop when we get the bestindividuals.

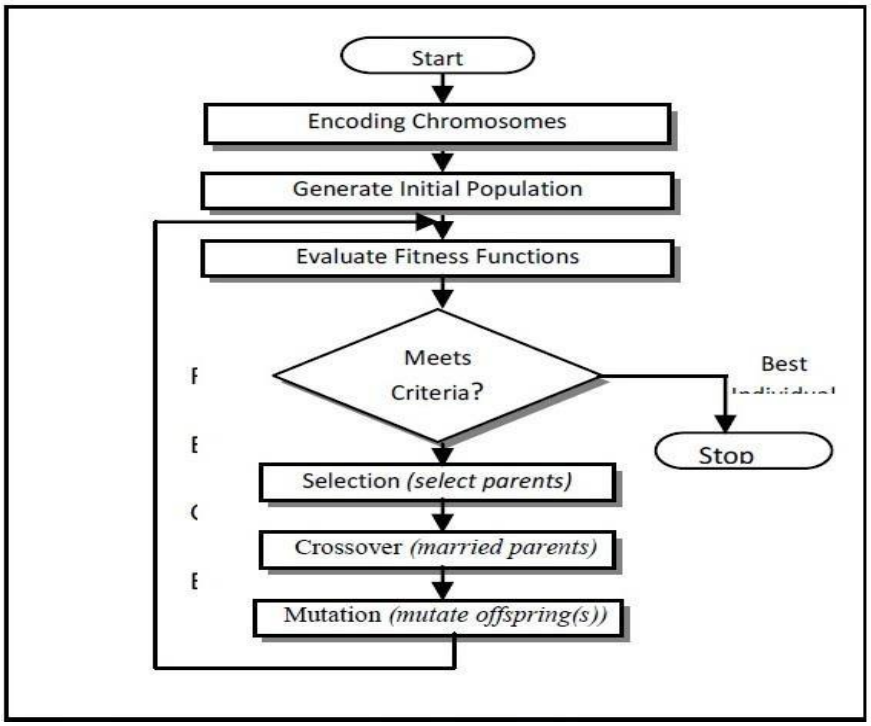

Figure 2: *Genetic algorithm Approach*

3.2 FREQUENTLY USED GENETIC ALGORITHMOPERATORS

- ChromosomesEncoding

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

- Fitness functionObjective.

Fitness function (or objective function) [11] defines the problem constraints; it measures the performance of all chromosomes in the population.

- Selection operatorRole.

Determines which chromosome(s) [10] 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 operatorRole.

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

- Mutation operatorRole.

New genetic material could be introduced into the new population through mutation process.
[10] This will increase the diversity in the population. For each offspring mutation randomly alters some gene(s). Some encoding schema's: binary encoding and real-number encoding.

IV. System overview

The proposed system overview is shown in figure 3 which starts from capturing firewallentriesi.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 bestindividuals.

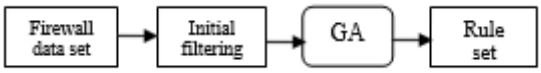

Figure 3: *architecture of Genetic Algorithm*

The detail 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.

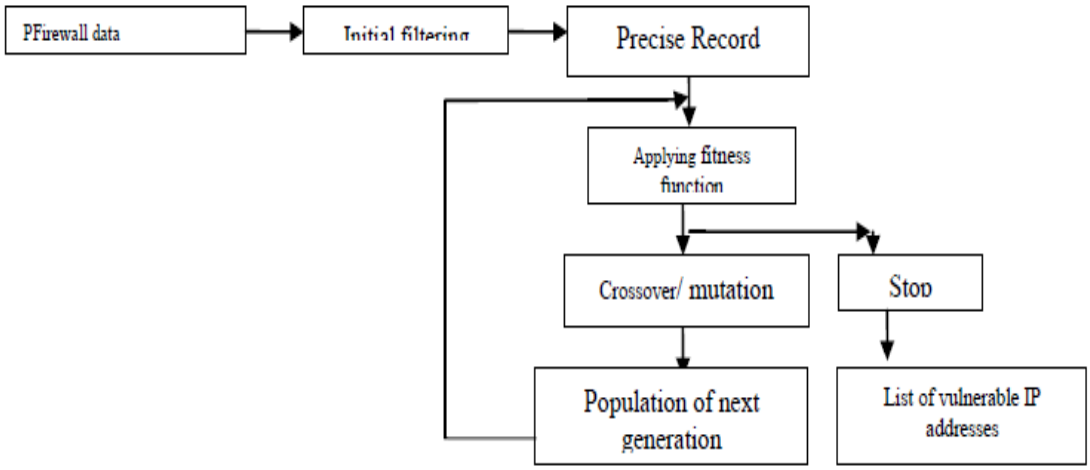

Figure 4: *Detailed architecture of GA-RIDS.*

V. Conclusion

In this paper we have successfully find the effective rule set which can detect existing as well asnewintrusions.Soastheresultgenerated;thesystemcanbeintegratewithanyoftheintrusion detection technique system to improve the ability and 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.
Thevariousoperatorslikeselection,crossoveraswellasmutationarealsodiscussed.

In this proposed system we are utilize single filtration to the system but in future we have a plantoapplymultiplefilterstoimprovethesystemperformanceandtoreducetimecomplexityof execution. Here we are planning to apply the proposed system output to the security system like firewall machine to block the traffic whose IP address entries aremade.

References

[1]. T. Lunt, A. Tamaru, F. Gilham, R. Jagannathan, P. Neumann, H. Javitz, A. Valdes, and T. Garvey. "A real-time intrusion detection expert system (IDES)" - final technical report. Technical report, Computer Science Laboratory, SRI International, Menlo Park, California, February1992.

[2]. K. Ilgun, R. A. Kemmerer, and P. A. Porras. "State transition analysis: A rulebased intrusion detection approach". IEEE Transactions on Software Engineering, 21(3):181–199, March1995

[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 "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,April.2010,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 intrusiondetection"

[7]. B.Upalhaiah, K. Anand, B. Narsimha, S. Swaraj, T. Bharat, "Genetic Algorithm Approach to Intrusion Detection System" ISSN:

0976-8491 (online) | ISSN : 2229-4333 (print), IJCST VOL3, ISSUE 1, JAN- MARCH 2012.

[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 detectionsystem",

[10]. Atul Kamble, "Incremental Clustering in data mining using genetic algorithm", IJCTE, Vol 2, No. 3, June,2010

[11]. Shaik Akbar, Dr. J. A. chandulal, Dr. K. Nageswara Rao, G. Sudheer Kumar, "troubleshooting technique for intrusion detection sytem using genetic algorithm", IJWBC, vol 1(3), december2011

[12]. Suhail Owais, Vaclav Snasel, Pavel Kromer, Ajith abrahim,"Survey: Using genetic algorithm approach in intrusion detection system techniques", 7th computer information system and industrial management applications,2008 IEEE