International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-6, March 2020

Securing the Network by the Intruder using Predictive Accession

Vaibhavi Pandya, Jitendrasinh Raulji

Abstract: ***Today, it is very crucial to deliver a immense level security to protect highly delicate and private information. Intrusion Detection System is an essential technology in Network Security. So my aim is to use IDS system and meliorate the performance of the IDS. The main target of Intrusion detection and prevention systems (IDPS) is to determine the feasible incidents, logging clue about them and in report attempts. Intruder is the person who tries to interrupt the network. So, it is essential to present a high level security to defend extremely susceptible and confidential information. Key aim of this thesis is to secure the network from the intruders identifying them also predicting them for the next transactions within the network. For that modified genetic algorithm is used to rank the parents and produce better individuals for the prediction of the intruders and provide better security to the network. Also improve the performance of genetic parameters.***

Keywords : Genetic algorithm, IDS, intruder, rank matrix.

I. INTRODUCTION

Internet is widely use now a days for worldwide communication. Due to wide use of internet security of the system is very crucial part and more and more intruders are developed to mischief the systems. An intrusion is "a collection of actions that aspire to understand the confidentiality, integrity or accessibility of different resource". [1] Therefore, the security from the injurious intruder is vital part for the computer network system. Intrusion detection system is one of the imperative security techniques. Intrusion detection system may be a system to perceive events in computers or network and analyses and monitoring the systems truthfulness and secrecy.[2] The Intrusion detection system is also used for detecting the discarded access traffic, unofficial access of the computer system, exploitation of the computer system etc.

Intrusion detection system perform different task like,[3]

- Keep eye on user activity and detect the anomalous behavior.
- Verify the system errors.
- Evaluate the truthfulness of system.

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author
Vaibhavi Pandya, Computer Engineering, Parul Polytechnic Institute, vadodara, India. Email:vaibhavi.pandya270014@paruluniversity.ac.in
Jitendrasinh Raulji, Computer Engineering, Parul Polytechnic Institute, vadodara, India. Email: Jitendrasinh.raulji@paruluniversity.ac.in

A. There are two types of IDS:

- "Network based IDS":-A network-based intrusion detection system (NIDS) is used to check out network flow to defend a system from network-based threats where the data is traffic crosswise the network.[4]
- "Host based IDS":- Host based intrusion detection (HIDS) system works on the single host. The data is composed from an article host system. "The accuracy of system, application action, file changes, host based network traffic, and system logs are monitors by HIDS agent".[4]

B. Intrusion detection techniques:

- "Anomaly based technique":- Intrusions are sensed by investigating some deviations from the common actions or normal pattern. Here main profit of this technique is they can perceive earlier cryptic attacks.
- "Signature based IDS or misuse based IDS":- In this technique the current movement is associated to known signature or known intrusion consequence that can be specific outline or progression of data or events. There is detriment like it can perceive only known attacks for which they defined signature previously. [5]

C. Challenges of IDS systems

There are some challenges which are face by any organization which used IDS system as security providers:

- One of the most commonly define challenge is false positive alarm which is high because the legitimate and not dangerous traffic also sometimes define as an intruder so false alarm rate is high.
- IDS technologies have required a lot of enrichment for security. Therefore it is very essential for organizations to apparently describe their anticipation from the IDS implementation. Today's IDS technology offers some mechanization like give the alerts to administrator if the disclosure of a malicious activity, ignore the spiteful connection for a configurable period of time, dynamically changing a router's access control list in order to stop a malevolent connection etc. It is also important to analyze the logs on regular basis also monitors logs daily for the detection of malicious activity which is harmful.
- IDS cannot give historical analysis of the log files and it is done on manual basis. Therefore it is very important to any administrator to handle incident and responding plan if any intruder is detected and also provide security person to handle it well.

D. Genetic algorithm

Genetic Algorithm is a programming technique who forms its basis from the biological evolution.

This algorithm is used for the difficulty solving strategy and provides best possible solution of the problem.[6] Genetic algorithm coverts the obstacle in to explicit domain model using chromosomes and evolve chromosomes using selection, crossover and mutation functions.

Genetic algorithm starts with the initial population from which selects the chromosomes and apply crossover, mutation function. Finally best fitted chromosome is chosen out as ultimate outcomes once the optimization measure is met. Genetic algorithm is conventional forward technique, but it could be complex in some cases. There are also corresponding executions of genetic algorithms but occasionally series of restrictions needs to be measured with explicit selection process. The final objective is to examination the solution space in a fairly short-range of time. [7]

The rest of the paper is described as follows. Section II described related work of IDS using genetic algorithm in tabular format. Section III described proposed methodology. In section IV, experimental result and discussion is given. Section V gives the conclusion of this paper.

II. RELATED WORK

Suhail Owais, Václav Snášel, Pavel Krömer and Ajith Abraham [8] have proposed survey of genetic algorithm in intrusion detection system. They give information about IDS systems classification genetic algorithm and their parameters, and different work done on genetic approach in IDS. Sanoop Mallissery, Jeevan Prabhu and Raghavendra Ganiga [9] have stated survey of IDS methods. They describes about various IDS methods and fuzzy clustering for IDS. The main advantage of this paper , it is effective for outlier detection . Srinivasa K G, SaumyaChandra, Siddharth Kajaria, Shilpita Mukherjee [10] proposed IGIDS: Intelligent Intrusion Detection System Using Genetic Algorithm in which they use GA for pruning best individuals in the rule set database. Using this algorithm IDS performs quick and sharp and has high detection rate with less false positives. The main drawback is, they have to be trained for every new attack, lot of authorize traffic classified as attack. Shaik Akbar**,** Dr.K.Nageswara Rao and Dr.J.A.Chandulal [11] have carryout rule based genetic algorithm for IDS. They use GA for identify and classify different types of attack connections to produce a set of rules that can be applicable to the IDS to. Using this created system which gives high-quality correctness, detect complex attacks. Main drawback of this system is, it is complex and required more training time. Mayank Kumar Goyal, Alok Aggarwal and Neelam Jain [12] have stated about effect of change in Rate of Genetic Algorithm Operator for misuse IDS. In this work they describe about set of classification rules which are produced from a predefined intrusion habits and apply crossover operation make mutation rate is constant. From this implementation they gives information about if Crossover too much, good piece of individuals get split and some individuals with high fitness's to be copied directly to the next population. Limitation of this system is, lot of mutation breaks high quality genes and break off them from being passed on. Salah Eddine Benaicha, Lalia Saoudi, Salah Eddine Bouhouita Guermeche, Ouarda Lounis [13] have implemented IDS using GA. They perform to efficiently detect various types of network intrusions GA approach with an improved initial population and selection operator. From this work, expand the performance of the detection rate and also reduces the false positive rate. Here they use DARPA dataset which is required to enhance for more detection. Nimmy Cleetus and Dhanya K A [14] proposed GA with different feature selection method for ID. They describe about, how to discovering the most dominant features for classification using GA. IDS with various feature selection methods like information gain, mutual correlation, and cardinality of features. From this work done they conclude that accuracy of 87.54% using Information gain based feature selection method. Dheeraj Pal and Amrita Parashar [15] proposed IDS using GA. They provides an intrusion detection system (IDS), by modifying the genetic algorithm to network intrusion detection system applied attribute subset reduction on the basis of Information gain. They conclude that system's training time and complexity reduced and also detect attack with more efficiently by Generated rule. Main drawback of this system is generated rules were biased to the training dataset.

III. PROPOSED METHODOLOGY

For the proposed system first apply genetic algorithm. Using genetic algorithm first extracts the features. After that find best fitted chromosomes and select that chromosomes. Here one function rank base matrix is added in my proposed work for the better selection of the individuals. Then apply crossover and mutation function for the best individuals. In proposed work rank matrix operator concept is introduce detect intruders. This modified the genetic algorithm and improved the performance. Therefore the proposed system deals with classification of intruders using rank matrix as well as predicting them for more security.

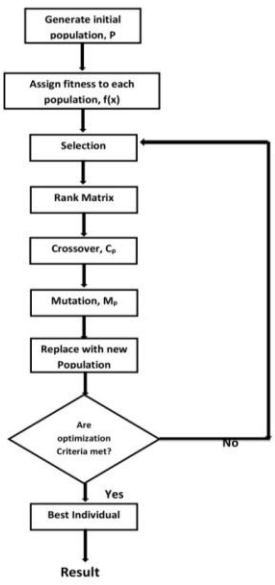

Fig 1: Proposed flow Diagram

A. Proposed algorithm

Input: network audit data, no of generation, initial population.
Output: A rules set.

1. Generate initial population.
2. Assign fitness to each population
   F(x)= w1*AB/N + w2*AB/A
   Where, w1=0.2 w2=0.8
   N= total no of records
   AB= support which is the number of network connections Correspond to the rule If A then B.
   A= confidence which is the number of network connections, which correspond to state A (condition),
3. Select chromosome in to new population based on highest fitness.
4. Generate rank matrix.
5. Apply crossover, C_p where C_p is the crossover rate.
6. Apply mutation, M_p where M_p is mutation rate.
7. Replace with new population.
8. If optimization criteria met
9. Best individuals
10. Else

Go to step 3.

B. Rank matrix

For rank matrix first select 25 individuals of any attack from the dataset. Then after select predefined rules of this attack. Make the group of five individuals from that 25 individuals and match this group to the main rule of individuals and give the rank based on the highest matching. From that create new five parents and make new parents using rank matrix. Here as an example one rule for the port scan is taken and make the rank matrix.

Rule to be match:-00,00,05 -0001 -0000001 -0000001 192.168.001.030 192.168.000.020 port-scan

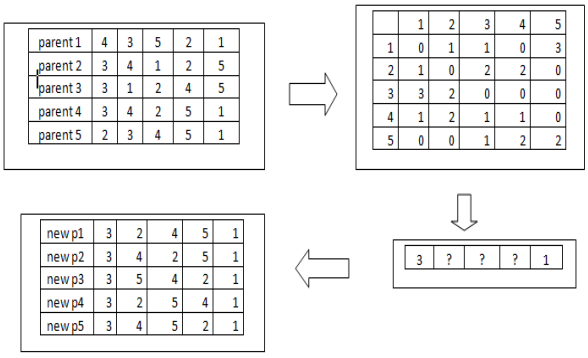

Fig 2: rank matrix

IV. EXPERIMENTAL RESULT

For implementation we use java library. In front end J2EE platform is used. Proposed system provides better security to the network from detecting the intruders. For the experiment evaluation we used DARPA dataset which is contain different type of attack and normal connection type data. From that we first apply as input fir the GA implementation.

A. Performance of crossover probability

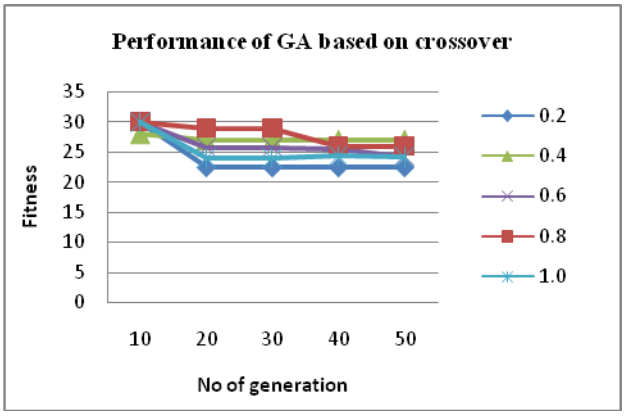

Fig 3: graph for crossover

As a result graph I try to improve crossover probability. If crossover range is high the most individuals are selected for the crossover and provide best individuals for the rule generation. Therefore I try to improve performance of the algorithm so I test different probabilities and the result is provided in to graph. From the graph 0.8 crossover probability gives higher result.

B. Generation of the genetic algorithm

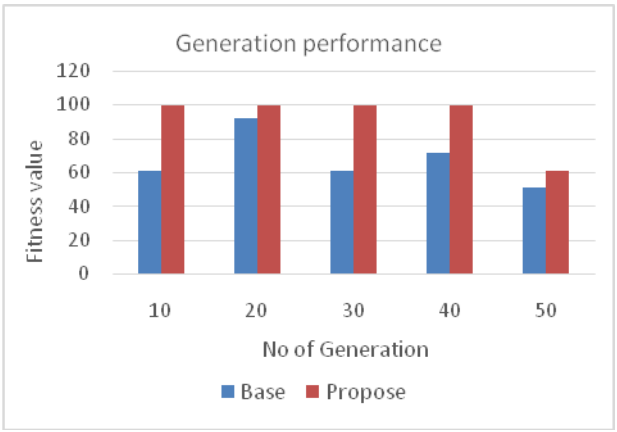

Fig 4: generation vs fitness performance

As a result graph here if the no of generation increase the fitness value of the rules or individuals are given in to the graph. From the result graph here we can say that the fitness value of the rank based generated rules were high compare to the base system. From this graph the result of proposed work is improved with compare to base system.

Table I: summarize result

	No of Generation				
	10	20	30	40	50
base	60.4	96	58.9	85.8	56
propose	100.1	100.2	100.1	100	60

C. Top five rules and their fitness value

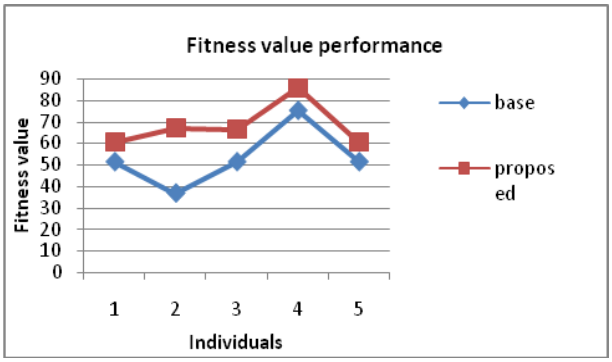

Fig 5: fitness vs individuals

As a result graph here the performance of the fitness value is describe. From the graph here we can say that the fitness of the proposed top five individuals which are generated from the rank base matrix and genetic algorithm combination is high. In the based system top five rules or individuals which are generated from frequently implemented genetic algorithm. So here we can say that the proposed system's fitness value is higher compare to base system.

Table II: summarize result

	Individuals				
	1	2	3	4	5
base	51.3	38.5	50	73.2	51
propose	60.2	65	64.9	84.6	60

V. CONCLUSION

Intrusion detection system is an important mechanism in Network Security. IDS detect the intruders which is harmful to the system. Intruders are any things like person, who tries to disturb the network. So, it is essential to present a high level security to preserve confidential information. The proposed algorithm modified genetic algorithm is used for rank the parents and produce better individual for improve the result. Using modified genetic algorithm for IDS provide better performance from the intruder detection. Using the proposed model generated rules have higher fitness and better feature selection compare to base system which is provide better performance to the IDS system to detect and predict the intruders and secure the system.

REFERENCES

1. Ravale, Ujwala, NileshMarathe, and Puja Padiya. "Feature Selection Based Hybrid Anomaly Intrusion Detection System Using K Means and RBF Kernel Function." Procedia Computer Science 45 (2015): 428-435.
2. Chakraborty, Nilotpal. "Intrusion Detection System and Intrusion Prevention System: A Comparative Study." International Journal of Computing and Business Research (IJCBR) ISSN (Online) (2013): 2229-6166.
3. Asif, Muhammad Kamran, et al. "Network Intrusion Detection and its strategic importance." Business Engineering and Industrial Applications Colloquium (BEIAC), 2013 IEEE. IEEE, 2013.
4. Jaiganesh, V., S. Mangayarkarasi, and P. Sumathi. "Intrusion detection systems: A survey and analysis of classification techniques." International Journal of Advanced Research in Computer and Communication Engineering2.4 (2013).
5. Ravale, Ujwala, NileshMarathe, and Puja Padiya. "Feature Selection Based Hybrid Anomaly Intrusion Detection System Using K Means and RBF Kernel Function." Procedia Computer Science 45 (2015): 428-435.
6. Anita, T., and D. Rucha. "Article: Genetic Algorithm-Survey Paper." IJCA Proceedings on NCRTC 5 (2012): 25-29.
7. Li, Wei. "Using genetic algorithm for network intrusion detection."Proceedings of the United States Department of Energy Cyber Security Group (2004): 1-8.
8. Owais, Suhail, et al. "Survey: using genetic algorithm approach in intrusion detection systems techniques." Computer Information Systems and Industrial Management Applications, 2008. CISIM'08. 7th. IEEE, 2008.
9. Mallissery, Sanoop, Jeewan Prabhu, and Raghavendra Ganiga. "Survey on intrusiondetection methods." Advances in Recent Technologies in Communication and Computing(ARTCom 2011), 3rd International Conference on. IET, 2011.
10. Srinivasa, K. G., et al. "IGIDS: Intelligent intrusion detection system using genetic algorithms." Information and Communication Technologies (WICT), 2011 World Congress on. IEEE, 2011.
11. Akbar, Shaik, K. Nageswara Rao, and J. A. Chandulal. "Implementing rule based genetic algorithm as a solution for intrusion detection system." Int. J. Comput. Sci. Netw. Secur 11.8 (2011): 138.
12. Goyal, Mayank Kumar, Alok Aggarwal, and Neelam Jain. "Effect of change in rate of genetic algorithm operator on composition of signatures for misuse intrusion detection system." Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on. IEEE, 2012.
13. Benaicha, Salah Eddine, et al. "Intrusion detection system using genetic algorithm." Science and Information Conference (SAI), 2014. IEEE, 2014.
14. Cleetus, Nimmy, and K. A. Dhanya. "Genetic algorithm with different feature selection method for intrusion detection." Computational Systems and Communications (ICCSC), 2014 First International Conference on. IEEE, 2014.
15. Pal, Dheeraj, and Amrita Parashar. "Improved Genetic Algorithm for Intrusion Detection System." Computational Intelligence and Communication Networks (CICN), 2014 International Conference on. IEEE, 2014.

AUTHORS PROFILE

Vaibhavi Pandya, I am Working at Computer Engineering Department, Parul Polytechnic Institute, vadodara, India. I have guided many final year projrct of diploma and degree students.I completed my Master of Engineering from Gujarat Technological University in 2016.I also completed my Bechlor engineering from same university in 2013.I published a survey paper on indrusion detection system using genetic algorithm in jan-2016.

Jitendrasinh Raulji, I am Working at Computer Engineering Department, Parul Polytechnic Institute, vadodara, India. I am also working as EDC(Entrepreneure Development Cell) coordinator at department level.I have guided many final year projrct of diploma and degree students.I completed my Master of Engineering from Gujarat Technological University in 2015.I also completed my Bechlor engineering from same university in 2012.I published a review paper on Fuzzy C_Mean algorithm in April-2015.