*Journal of Advances and Scholarly Researches in Allied Education*
*Vol. XIV, Issue No. 2, January-2018, ISSN 2230-7540*

# Improvement in Interpolation Exposure System Using Genetic Algorithm

**Jagdish Kaur***

Assistant Professor, Department of Computer Science, DAV College for Women Ferozepur Cantt

***Abstract – In the current scenario society is facing so many issues because of outsider's interference in our communication media with other person/organisation. So for the security reasons there must be a safe and secure intrusion detection system. Intrusion detection has become an important area of research in the current system. The existing system is not completely perfect and secure. So, there is the need to make the existing system more secure. In this paper, firstly we are going to discuss about the existing intrusion detection system SNORT and its disadvantages then we will discuss about the various research areas which are in use to enhance the performance of existing IDS system with the help of genetic algorithm.***

***Keyword – Intrusion Detection System, Genetic Algorithm, Snort, Network attack, Denial of service.***

----------X----------

## I. INTRODUCTION

This research paper talked about how Genetic Algorithm (GA) can be used to enhance the performance over existing wireless intrusion detection system. In an existing system SNORT rule cannot be implemented at run time. In snort all rules or expected behavior is already stored in rule set. If the behavior of network connection diverges from expected normal behavior which is stored in rule set, it will be considered as trespass. The main aim of this article is to generate rules at run time i.e. add the rule in rule set with genetic algorithm.

## II. INTRUSION DETECTION SYSTEM

Virus detection systems checks the various resources over network and identifying whether a system or a network is being used by an authorized person or not. Two basic methods of detecting intrusion are: misuse detection and anomaly detection. Misuse detection system put into effect on the basis of pattern or signature. It is arranged into various techniques such as signature **based, rule based** and **data mining** (Aleksandar, et. al., 2005). Anomaly detection system describes the normal behavior of system. When the normal behavior of network changes it is considered as intrusion (Detection System) There are two types of intrusion detection system: passive and reactive. In passive system sensor identify the intrusion, log the information and send the alert on console. In reactive system, virus prevention system automatically send the response to the distrust activity by readjust the connection or by reprogramming the firewall system to block network traffic from malicious source (Detection System). Intrusion detection system model is not dependent upon any particular system application environment, system defenselessness or any type of intrusion. There are mainly six parts exist of this model: subject, object, audit record, profile, anomaly record and activity rule (Detection System). Intrusion detection system needs the use of metrics. A metric is a random variable z representing a quantitative measure over time. Metrics are basically of three types: event counter, time interval and resource measurement (Detection System). The effective implementation of expert system in intrusion detection system was very meaningful in development of effective detection based information security system. Expert system composed of set of rules which converts the knowledge of human "expert". These rules are used by system to make decision. Expert system allows the incorporation of human experience into computer application which is used to recognize activities which matched with the defined features of misuse and attack (Anderson, et. al., 1995).

Categories of intrusion detection system:

- √ Network based detection system identify the intrusion like denial of service, port scan, and crack into computer by checking the network traffics.
- √ Host based detection system will find intrusion in inner part of the system, not outside. It gathers information of individual computer such as web server.

- √ Protocol based detection system is installed on web server and it is used to observe protocols, monitoring the traffic between a connected device and system.[21]
- √ An intrusion detection system is collection of various components.
- √ Sensor system will generate security events.
- √ Console system will monitor event, alerts and control sensors.
- √ Engine system will record events logged by sensors in a data base (Scarfone and Mell, 2007).

## III. SNORT

SNORT is an open source intrusion detection system that is used on Windows or Linux operating system. Snort is basically a rule based detection engine which is available free of cost. Snort is quite able to perform real time traffic, analysis, packet logging on internet protocol network. It can identify vast variety of attacks (Scarfone and Mell, 2007).

With the help of protocol analysis and content searching method, snort detects thousand of viruses such as worms, vulnerability exploit attempts, port scan and other behavior (Sectools.Org: 2006) (Top 125 Network Security Tools) Snort could have three modes: sniffer mode, packet logger mode, network intrusion detection system mode.

- √ To print the TCP/IP packet on the screen in this mode just type:. /snort –v
- √ If you want to see application data in transmission: . /snort –vd
- √ For any further detail type: . /snort –vde
- √ You can record the packet to disk in Packet logger mode : . /snort –dev –l. /log

Network intrusion detection system mode examine the network traffic against a user –defined domain: /snort –dev –l. /log –h 172.18.7.217 –c snort.conf.

Each snort rule has two parts header and content of data packet. A snort rule is: Alert tcp any any -> 172.18.7.218 111

## IV.DRAWBACKS IN EXISTING SYSTEM

(Alserhana at. el., 2009). Studies the high speed testing of performance of snort in a very high speed network. The performance was based on two cases: 1) whether snort and attacker is on different operating system platforms. 2) Whether snort and attacker on same operating system platform. In the first test snort only detect 20% of attack at 1.0 gbps speed of network traffic, when snort installed on Window XP Service Pack2 and was generated from Linux 2.6. In second test snort detect 100% attack up to 400 mbps but only capture 30% of attack at 1.0 gbps. CPU usage by snort is 80% at 500 mbps with the current input traffic but only 30% at 1.0 gbps. The performance of snort goes down as there is increase in network traffic. Different problems occur in existing system (Gong, et. al., 2005).

- √ Fidelity problem is occurred when data packets travel across long path and it can be modified by an attacker.
- √ Resource usage problem occurred because component of intrusion detection system has to be run all the time while there is no intrusion occurred.
- √ Reliability problem occurred because the component of intrusion detection system is implemented as a separate program, they are susceptible to tempering and an hacker can disable or modify them.

So to overcome these problems we are using Genetic Algorithm (Gong, et. al., 2005).

## V. GENETIC ALGORITHM

It is almost technically not possible to develop a system which is having no vulnerabilities. So, virus detection system has become an important area of research. If an intrusion changes path with small degree from the already defined pattern then it will consider as normal and if normal behavior changes with small degree it may be treated as intrusion. Intrusion detection system provides many methods which recognize and differentiate between normal and intrusion data. Genetic algorithm can be used to tune the membership function of IDS (Owais, et. al., 2008). Genetic Algorithm is a family of computational model based on principles of evolution and natural selection. GA convert the problem into a model by using chromosomes like data structure and evolve the chromosomes using selection, recombination and mutation operator (Sinclair, et. al., 1999). (Learning to Network Intrusion Detection, 2003).

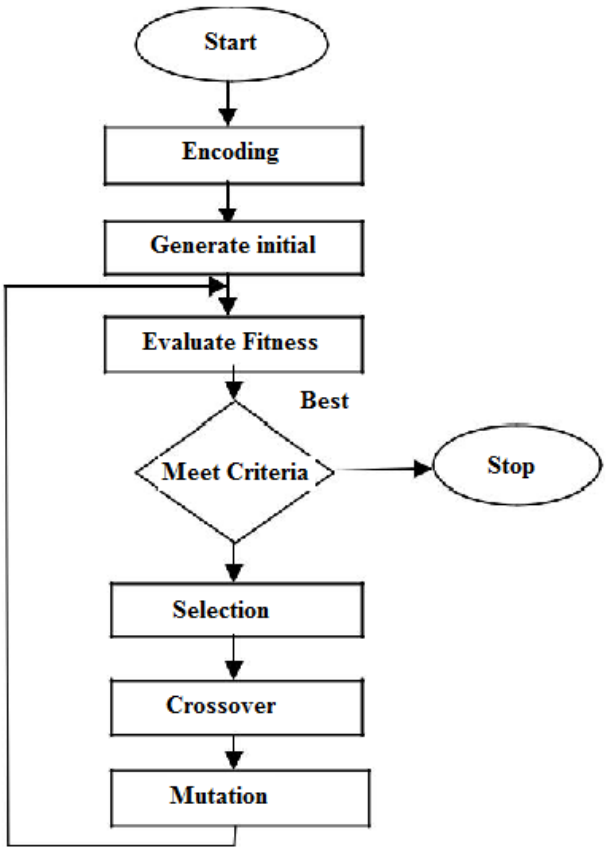


**Figure1.Genetic algorithm process (Owais, et. al., 2008).**

Firstly a number of individual are selected based on user defined fitness function, the remaining are discarded. Next, a number of individual are selected and paired with each other. Each pair produces one offspring by applying crossover operator. At the end a certain number of individual are selected and mutation operator applied i.e. a randomly selected gene of individual abruptly changes its value (Darrell, 1994).

## VI. RELATED WORK

It is quite clear from the previous research (Gong, et. al., 2005) that there are three factor of Genetic Algorithm:

√ Fitness function

√ Representation of individual

√ Genetic Algorithm parameters.

Genetic Algorithm based intrusion detection system divided into two parts: pre calculation part and intrusion detection part. In pre calculation part, a set of chromosomes is created using training data in offline environment (Darrell, 1994). In intrusion detection part, the created rules are used to categorize incoming network connections in real time environment using testing process i.e. selection, crossover and mutation (Darrell, 1994). After creating rule it will be very easy to detect intrusion. Pre calculated data is used in this part to find out fitness of each chromosome. False positive rates will be much slower if we can use better method in the detection process (Gong, et. al., 2005). There are so many network features, which are selected to form a classification rule. These features are: duration, protocol, source_port, destination_port, source_ip, destination_ip and attack_name (Darrell, 1994). In the real world there exist vast range of intrusions and they tend to change with the time and become complicated very rapidly. So, proposed intrusion detection system can provide useful tact's to upload and update new rules to the system to detect intrusion. It is cost effective and adaptive (Darrell, 1994). Genetic algorithm can be used to create the rule for detecting normal and anomalous connections. These rules are stored in rule set in the form of if {condition} then {act}. Here condition part can check for matching the current network connections and rules in the rule set if any connection having same source IP address, destination IP address, destination port number and connection time then this connection will be stop because it matches with the blacklisted IP address. Final goal of applying GA is to generate rule that match only anomalous connection (Hoque, et. al., 2012). These rules are tested on past connection and used to filter the new connection. This paper presents that implementation of GA is unique as it consider both temporal and spatial information of network connection during encoding the problem (Hoque, et. al., 2012). If any function produces more and more new rule then add them to the existing rules. Functional advantage is that every time new rules generate, the number of rules overall doubles. So administrator has no need to keep account of all these rules (Li, 2004).

In genetic algorithm three sub problem arise: 1) coding the chromosomes 2) selecting GA operator 3) find a valid fitness function. Key idea of this approach is automatically construct the rule of ID. This approach implements the heuristic search in the space of network information and finds the same type of attack (Keerthi, et. al., 2011).

## VII. ARCHITECTURE OF INTRUSION DETECTION SYSTEM

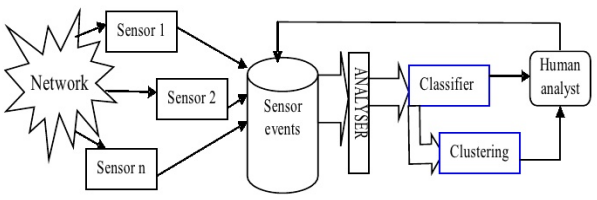

**Figure2.Genetic**

IDS need to collect network data for analysis which contains normal and abnormal data. After doing this task, network sniffer will analyze the data and will send it to genetic algorithm. Fitness function will be applied in the rule set to add the rule which is stored in rule base [22]. GP work on the population of parse tree, which is made up of internal nodes and leaf nodes. Internal nodes are called primitive functions and leaf nodes are the terminal (Jian, et. al., 2004). Input of the program is given by terminal, which are the independent variable and set of constant. The rule generated by using GP is in the form "if antecedent then consequent". Three genetic operators are used crossover, mutation and dropping condition. New rule evolved using dropping are like this: if condition1 and condition2 the consequence can be change to if condition1 and any then consequence. A removal approach is also introduced to the simulated artifacts attribute because of over optimistic evaluation of network anomaly detectors. New system outperform over existing system. Limitation of GP is that the algorithm needs two passes during training, resulting in the inefficiency of detector (Jian, et. al., 2004). (Yin, et. al., 2005). Binary code has a continuous function of discrete mapping error for some multidimensional and high precision requirement of continuous function optimization. They use gray code coding because it improve the GA local search capability. Selection of population size is one of the most important parameter in GA. If the population size is too large then it will lower the efficiency of GA. If it is too small, it may improve the speed but lower the diversity of population and it will cause premature conversion (Yin, et. al., 2005). This system created lot of selection methods such as random search, adjacent search, multipoint search and best individual multipoint search because the existing selection operator roulette wheel leads to "premature conversion" and slowdown search process. They only use three point crossovers; position can be randomly selected with no repetition. By using improved GA their work effectively improved the ID rate (Yin, et. al., 2005).

## VIII. CONCLUSION

The new genetic algorithm is new technique to detect intrusions in the system. According to the new intrusions introduced in the system it automatically uploads and update new rules to the system. Genetic algorithm is unique because this algorithm treats both temporal and spatial information during converting encoding the problem as a major source. New rules are generated at run time, so administrator has no need to keep track of all these rules.

## REFERENCES


Aleksandar L., Vipin K., and Jaideep S. (2005). Massive Computing Managing Cyber Threats, Issues, Approaches, and Challenges. Intrusion Detection: A Survey: Computers/General Information. Springer, 2005.

Anderson, D., Frivold, T. & Valdes, A. (May, 1995). Next -generation Intrusion Detection Expert System (NIDES): A Summary. SRI International Technical Report SRICSL-pp. 95-07.

Ch. S. Keerthi, N. V. L, P. L. prasanna, B.M. Priscilla, M. V. B. T. Santhi (2011). "Intrusion Detection System Using Genetic Algorithm" International Journal of P2P Network Trends and Technology-Volume1 issue2-2011.

Chuanhuan Yin, Shengfeng Tian, Houkuan Huang and Jun He (2005). "Applying Genetic Programming to Evolve Learned Rules for Network Anomaly Detection" L. Wang, K. Chen, and Y.S. Ong (Eds.): ICNC 2005, LNCS 3612, pp. 323 – 331, © Springer-Verlag Berlin Heidelberg 2005.

Denning, Dorothy (1986). An intrusion detection model .IEEE Transaction on software Engineering, vol.se-13, no.2.

en.wikipedia.org/wiki/intrusion_detection system.

F. Alserhani, Monis Akhlaq, I. U. Awan, A. J. Cullen, J. Mellor, Pravin Mirchandani (2009). "Snort Performance Evaluation" Informatics Research Institute, University of Bradford, Bradford, BD7 1DP, United Kingdom.

Guan Jian,Liu Da-Xin, Cui Bin-Ge (2004). "An Induction Learning Approach for Building Intrusion Detection Models Using Genetic Algorithem" proceeding of IEEE 5th world conf. On Intelligent Control and Automation. June 15-19.2004,P.R.China.

K. Scarfone, and P. Mell (2007). Guide to Intusion Detection and Prevention Systemsǁ, National Institute of Standards and Technology NIST. Computer Security.

Learning to Network Intrusion Detection (2003). "In Proceedings of 1999 Annual Computer Security Applications Conf. (ACSAC), pp. 371-377. Phoenix, Arizona. URL: http://www.acsac.org/1999/papers/fri-b-1030-sinclair.pdf (30 Oct. 2003).

M.S. Hoque, M.A. Mukit, M.A.N. Bikas (2012). "An implementation of intrusion detection system using Genetic Algorithm" International Journal of Network Security & its Application (IJNSA),Vol.4,no.2.

McHugh, John (2001). "Intrusion and Intrusion Detection." Technical Report. CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University.

QIAO Pei-li, CHEN Shi-feng, SU Jie (2009). " The Research of NIDS Based on Improved GA" Proceeding of IEEE conference.

R. H. Gong, M. Zulkernine, and Purang (2005). A software Implementation of a Genetic Algorithm Based Approach to Network Intrusion Detection‖, SNPD/SAWN'05, IEEE.

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

Sectools.Org: 2006 Results;http://sectools.org/tools2006.html

SecTools.Org: Top 125 Network Security Tools; http://sectools.org/tag/ids/.

Sinclair, Chris, Lyn Pierce, and Sara Matzner (1999). "An Application of Machine

Snort User's Manual, http://www.snort.org.

W. Li (2004). "Using Genetic Algorithm for Network Intrusion Detection", Proceedings of the United States Department of Energy Cyber Security Group.

Whitley, Darrell (1994). "A Genetic Algorithm Tutorial." Statistics and Computing 4: pp. 65-85.

---

**Corresponding Author**

**Jagdish Kaur***

Assistant Professor, Department of Computer Science, DAV College for Women Ferozepur Cantt

**E-Mail – armaanpreet29@gmail.com**