International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 01 | Jan 2020 www.irjet.net p-ISSN: 2395-0072

# Intrusion Detection System using Genetic Algorithm

**Fathullah Safi**[1]

[1]*M.Tech scholar at the Department of Computer Science, Sharda University, Greater Noida, India.*

---

**Abstract -** *Today we are suffering from many problems because of intruder interference in our communication with other person/organization. We need a very safe and secure intrusion detection system. So, intrusion detection has become a crucial area of research the prevailing systems aren't completely flawless and secure. So, there is the need to improve the existing system. In this paper, firstly we are discussing about the prevailing network intrusion detection system, attacks and its drawback then discuss about different research areas which were happening to improve the performance of existing system with the assistance of genetic algorithm.*

***Key Words***: **Intrusion Detection System, Genetic Algorithm, Network attacks**

## 1. INTRODUCTION

An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

Although intrusion detection systems monitor networks for potentially malicious activity, they're also disposed to false alarms. Hence, organizations got to fine-tune their IDS products once they first install them. It means properly fixing the intrusion detection systems to acknowledge what normal traffic on the network seems like as compared to malicious activity.

Intrusion prevention systems also monitor network packets inbound the system to see the malicious activities involved in it and directly sends the warning notifications.

### 1.1 Classification of intrusion detection Intrusion detection system (IDS) is basically classified into 2 types:

**1. Network Intrusion Detection System (NIDS):**

Network intrusion detection systems (NIDS) are found out at a planned point within the network to look at traffic from all devices on the network. It performs an observation of passing traffic on the whole subnet and matches the traffic that's passed on the subnets to the gathering of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of an NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying cracking the firewall

**2. Host Intrusion Detection System (HIDS):**

Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and can alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is shipped to the administrator to research. An example of HIDS usage are often seen on mission critical machines, which aren't expected to vary their layout

**Detection Method of IDS:**

**1. Signature-based Method:**

Signature-based IDS detects the attacks on the idea of the precise patterns like number of bytes or number of 1's or number of 0's within the network traffic. It also detects on the idea of the already known malicious instruction sequence that's employed by the malware. The detected patterns within the IDS are referred to as signatures. Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it's quite difficult to detect the new malware attacks as their pattern (signature) is not known.

**2. Anomaly-based Method:**

Anomaly-based IDS was introduced to detect the unknown malware attacks as new malware are developed rapidly. In anomaly-based IDS there's use of machine learning to make a trustful activity model and anything coming is compared thereupon model and it model and it's declared suspicious if it's not found in model. Machine learning based method features a better generalized property as compared to signature-based IDS as these models are often trained consistent with the applications and hardware configurations.

**GENETIC ALGORITHM**

Genetic Algorithms (GAs) are adaptive heuristic search algorithms that belong to the larger a part of evolutionary algorithms. Genetic algorithms are supported the ideas of survival and genetics. These are intelligent exploitation of random search given historical data to direct the search into the region of higher performance in solution space.

It is not technically feasible to create a system which has no vulnerabilities. So, intrusion detection has become a crucial area of research. If an intrusion slightly deviates from the already defined pattern then it will consider as normal and if normal behavior slightly changes it may be treated as intrusion. Intrusion detection system offer many techniques which recognize and differentiate between normal and intrusion data. Genetic algorithm are often wont to tune the membership function of IDS [4]. Genetic Algorithm may be a family of computational model supported principles of evolution and survival. GA converts the matter into a model by using chromosomes like arrangement and evolves the chromosomes using selection, recombination and mutation operator

**STRUCTURE OF GENETIC ALGORITHMS**

A genetic algorithm has many parameters, operators and processes which decide its arrival to an optimal solution. A brief explanation of the parameters, operators and processes as depicted in figure

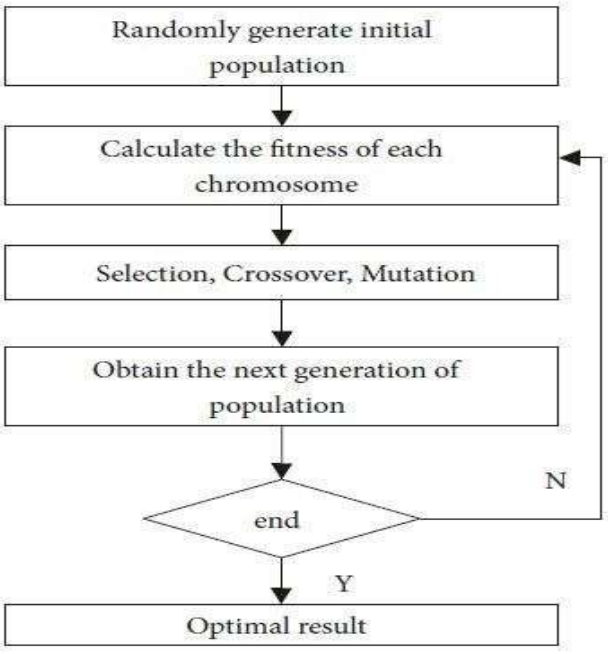


FIGURE 2: Process of GA.

**FUNCTIONING OF GENETIC ALGORITHMS**

The genetic algorithms start processing by initially selecting a random population of chromosomes. Each chromosome consists of a finite number of genes, which is predefined in every implementation [13]. These chromosomes are the data representing the problem. This initial population is refined to a top quality population of chromosomes, where each chromosome satisfies a predefined fitness function. According to the wants of the answer needed, different gene positions during a chromosome are encoded as numbers, bits, or characters. Each population is refined by applying mutation, crossover, inversion, and selection processes.

**RELATED WORK**

We have concluded from the previous research that there are three factor of genetic algorithm: 1) Fitness function 2) Representation of individual 3) GA parameters. Genetic Algorithm based intrusion detection system divided into two parts: precalculation phase and intrusion detection phase. In precalculation phase, a group of chromosomes is made using training d ata in offline environment. In intrusion detection phase, the generated rules are used to classify incoming network connections in real time environment using evaluation process i.e. selection, crossover and mutation. After generating rule it is very easy to detect intrusion. Precalculated data is employed during this phase to seek out fitness of every chromosome. If a far better equation is employed in these detection process false positive rates are going to be much slower. Seven network features are selected to make a classification rule. These features are: duration, protocol, source port, destination port, source IP, destination IP and attack name. In the world the kinds of intrusion change and become complicated very rapidly. So, proposed detection system can upload and update new rules to the system. It is cost effective and adaptive. GA are often wont to generate the rule for detecting normal and anomalous connections. These rules are stored in rule set in the form of if {condition} then {act}. Condition part check for matching the current network connection 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 are going to be stop because it matches with the blacklisted IP address. Final goal of applying GA is to get rule that match only anomalous connection.

**CONCLUSION**

In described techniques, Genetic Algorithm decreases the false +ve rate. Proposed detection system uploads and update new rule to the system. Implementation of Genetic Algorithm is exclusive because it considers both temporal and spatial information during encoding the matter. New rules are generated at run time, so administrator has no got to keep track of these rules.

**REFERENCES**

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

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

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

[4] *Sharmila Devi, **Ritu Nagpal "Intrusion Detection System Using Genetic Algorithm" Deptt. Of CSE, Guru Jambheshwar University of Science and Technology, Hisar-125001, Haryana

[5] Gowher Majeed Parry "Genetic algorithms in intrusion detection systems" International Journal of Innovation and Applied Studies January 2014

[6] Jiu-Ling Zhao, Jiu-Fen Zhao, Jian-Jun LI "INTRUSION DETECTION BASED ON CLUSTERING GENETIC ALGORITHM" Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, Guangzhou, 18-21 August 2005

[7] Amol Borkar, Akshay Donode, Anjali Kumari "A Survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and Protection System (IIDPS)" Proceedings of the International Conference on Inventive Computing and Informatics (ICICI 2017)