ISSN 2664-4150 (Print) & ISSN 2664-794X (Online)
**South Asian Research Journal of Engineering and Technology**
*Abbreviated Key Title: South Asian Res J Eng Tech*

**| Volume-2 | Issue-6 | Nov-Dec -2020 |** **DOI: 10.36346/sarjet.2020.v02i06.003**

**Review Article**

# Enhancement in Intrusion Detection System for WLAN Using Genetic Algorithms

Dr. Vikash Kumar Garg[1*], Dr. S. Jagadeesh Soundappan[2], Er. Mandeep Kaur[1]

[1]Assistant Professor, Department of CSE, BGIET Sangrur, Punjab, India
[2]Associate Professor, Department of CSE, BGIET Sangrur, Punjab, India

***Corresponding Author**
Dr. Vikash Kumar Garg

**Article History**
Received: 13.11.2020
Accepted: 23.12.2020
Published: 30.12.2020

**Abstract:** The rapid need of Information Technology and that too wireless usage demands a great deal of security in order to keep all the data sources and equipment's secure. So we need a secured network to secure all these. But Secured data communication over Internet and any other network is always under threat of intrusions and misuses. So Intrusion Detection System has become necessary in terms of network security. There are various approaches that have been used before in Intrusion Detection Systems but all of the approaches have some types of flaws in it. So the scope of betterment is always there. In this paper we proposed an Intrusion Detection System (IDS) by applying Genetic Algorithm (GA) to effectively detect the network intrusions. Various Parameters and evolution processes for GA are discussed in detail and implemented so that to overcome the flaws that was present in previous Intrusion Detection Systems.

**Keywords:** Intrusion Detection, wireless networks, IDS, GA, Chromosomes, Genes.

## 1. INTRUSION DETECTION SYSTEM

A wireless network is not as secured as a Wired Network because in wired network we can put the check on wires but in wireless data is transferred via air so any intruder can access the data by using various hacking techniques. In wireless networks it is very difficult to secure the network for lifetime and detect various attacks by Intruders. Some commonly used attacks are more in wireless environment as compared to wired one and some extra efforts should be used to prevent those. An Intrusion Detection System aim to detect the different attacks against network and system. Because of the multitude of methods of intrusions, there are several reasons why IDS is essential to any network, both wired and wireless. While the wireless IDS technology is new, we need to find out its capabilities and how it can help in providing a robust level of security for wireless networks. Additionally, we need to know what types of IDS are available and the drawbacks that come with using a wireless IDS.

## 2. NETWORKING ATTACKS

This section is an overview of the four major categories of networking attacks. Every attack on a network can comfortably be placed into one of these groupings.

- **Denial of Service (DoS):** A DoS attack is a type of attack in which the hacker makes a computing or memory resources too busy or too full to serve legitimate networking requests and hence denying users access to a machine e.g. apache, smurf, neptune, ping of death, back, mail bomb, UDP storm etc. are all DoS attacks.
- **Remote to User Attacks (R2L):** A remote to user attack is an attack in which a user sends packets to a machine over the internet, which s/he does not have access to in order to expose the machines vulnerabilities and exploit privileges which a local user would have on the computer e.g. xlock, guest, xnsnoop, phf, sendmail dictionary etc.
- **User to Root Attacks (U2R):** These attacks are exploitations in which the hacker starts off on the system with a normal user account and attempts to abuse vulnerabilities in the system in order to gain super user privileges e.g. perl, xterm.

- **Probing:** Probing is an attack in which the hacker scans a machine or a networking device in order to determine weaknesses or vulnerabilities that may later be exploited so as to compromise the system. This technique is commonly used in data mining e.g. saint, portsweep, mscan, nmap etc.

## 3. CLASSIFICATION OF INTRUSION DETECTION SYSTEM

IDS can be classified in two main categories. They are shown below:

i. **Host Based Intrusion Detection:** HIDSs checks the information found on single or multiple host systems, including the content of operating system, files of operating system and various application files.
ii. **Network Based Intrusion Detection:** NIDSs evaluate information taken from various network communications, analyzing each packet that is routed from source to destination. It also takes into account the stream of packets across the network.

## 4. COMPONENTS OF INTRUSION DETECTION SYSTEM

An intrusion detection system normally consists of three functional components. The first component of an intrusion detection system, also known as the event generator, is a data source. The second component of an intrusion detection system is known as the analysis engine. This component takes information from the data source and examines the data for symptoms of attacks or other policy violations. The analysis engine can use one or both of the following analysis approaches:

- **Misuse/Signature-Based Detection:** This type of detection engine detects intrusions that follow well-known patterns of attacks (or signatures) that exploit known software vulnerabilities. The main limitation of this approach is that it only looks for the known weaknesses and may not care about detecting unknown future intrusions.
- **Anomaly/Statistical Detection:** An anomaly based detection engine will search for something rare or unusual. They analyses system event streams, using statistical techniques to find patterns of activity that appear to be abnormal. The primary disadvantages of this system are that they are highly expensive and they can recognize an intrusive behavior as normal behavior because of insufficient data

The third component of an intrusion detection system is the response manager. In basic terms, the response manager will only act when inaccuracies (possible intrusion attacks) are found on the system, by informing someone or something in the form of a response.

## 5. PROBLEMS WITH EXISTING SYSTEMS

i. The information used by Intrusion Detection System is obtained from Audit or from Packets on a network. Packets have to travel a long distance from the origin to IDS and finally to destination and in this process can potentially be destroyed or modified by an attacker.
ii. The Intrusion Detection System Continuously monitoring even when there is no intrusion occurring, because the components of IDS have to run all the time. This pure wastage of resources.

## 6. IDS USING OUR GENETIC ALGORITHM

By using various ways IDS can be implemented. We have chosen Genetic Algorithm to make our IDS. A genetic Algorithm has many operator, processes and parameters which decide its arrival to an optimal solution. A short description of the parameters, operators and processes is handy. The genetic algorithms start processing by initially selecting a random population of chromosomes. Each chromosome is composed of a finite number of genes, which is predefined in every implementation. These chromosomes are the data representing the problem. This initial population is refined to a high quality population of chromosomes, where each chromosome satisfies a predefined fitness function.

According to the requirements of the solution needed, different gene positions in a chromosome are encoded as numbers, bits, or characters. Each population is refined by applying mutation, crossover, inversion, and selection processes. The working of a genetic algorithm when applied to intrusion detection can be viewed as a sequence of following steps:

i. The packet capturing module or sniffer present in the intrusion detection system collects the information about the network traffic or logs.
ii. The intrusion detection system applies genetic algorithms to the captured data. The genetic algorithm at this stage has classification rules learned from the information collected.
iii. The intrusion detection system then applies the set of rules produced in the previous phase to the incoming traffic. Application of rules to captured data results in the population initialization, which in turn results in the creation of a new population with good qualities. This population is then evaluated and a new generation with better qualities is created. Then genetic operators are applied to the newly created generation until the most suitable individual is found.

## 7. CONCLUSION

Intrusion detection methods based on genetic algorithms have attracted most of the attention from the research community and the industry during the past so many years. The requirements for building efficient intrusion detection systems and the features of genetic algorithms are the main reason behind genetic algorithms getting such an attention from the intrusion detection research community. This survey provides an introduction to intrusion detection and genetic algorithms. The generics of genetic algorithm based intrusion detection systems are discussed. Also, the work done by different researchers in the direction of applying genetic algorithms for intrusion detection is surveyed. In near future we will try to improve our intrusion detection system with the help of more statistical analysis and with better and may be more complex equations.

## REFERENCES


- Bace, R. G. (2000). Intrusion Detection. *Macmillan Technical Publishing.*
- Bobor, V. (2006). Efficient Intrusion Detection System Architecture Based on Neural Networks and Genetic Algorithms. Department of Computer and Systems Sciences, Stockholm University / Royal Institute of Technology, KTH/DSV.
- Bridges, S. M., & Vaughn, R. B. (2000). Fuzzy Data Mining And Genetic Algorithms Applied To Intrusion Detection. *Proceedings of 12th Annual Canadian Information Technology Security Symposium*, pp. 109-122.
- Folino, G., Pizzuti, C., & Spezzano, G. (2005). GP Ensemble for Distributed Intrusion Detection Systems. *ICAPR*, 5462.
- Ilgun, K., Kemmerer, R., & Porras, P. A. (1995). State Transition Analysis: A Rule-Based Intrusion Detection Approach. *IEEE Transaction on Software Engineering*, 21(3), 181-199.
- Kayacık, H. G., Zincir-Heywood, A. N., & Heywood, M. I. (2005). Selecting Features for Intrusion Detection: A Feature Relevance Analysis on KDD 99 Intrusion Detection Datasets.
- Kumar, S. (1995). Classification and Detection of Computer Intrusions. *Purdue University*.
- Kumar, S., & Spafford, E. (1995). A Software architecture to Support Misuse Intrusion Detection. In *The 18th National Information Security Conference*, pp. 194204.
- Lu, W., & Traore, I. (2004). Detecting New Forms of Network Intrusion Using Genetic Programming. *Computational Intelligence*, vol. 20, pp. 3, Blackwell Publishing, Malden, pp. 475-494.
- Pillai, M. M., Eloff, J. H. P., & Venter, H. S. (2004). An Approach to Implement a Network Intrusion Detection System using Genetic Algorithms. *Proceedings of SAICSIT*, pp: 221-228.
- Planquart, J. P. Application of Neural Networks to Intrusion Detection. *SANS Institute Reading Room*