International Conference On Emerging Trends in Engineering and Management Research
NGSPM's Brahma Valley College of Engineering & Research Institute, Anjaneri, Nashik(MS) (ICETEMR-16)
23rd March 2016, www.conferenceworld.in ISBN: 978-81-932074-7-5

NETWORK INTRUSION DETECTION & PREVENTION SYSTEM USING FUZZY LOGIC AND GENETIC ALGORITHM

Umesh Patil[1], Rahul Gunjal[2], Akshay Gadhe[3], Rushikesh Kulkarni[4] ,Mrs. Seema Mandlik[5]

[1,2,3,4,] Student, Department of Information Technology, MIT AOE, Alandi, SavitribaiPhule Pune University.Maharastra,(India)

[5] Asst. Professors, Department of Information Technology, MIT AOE, Alandi, SavitribaiPhule Pune University.Maharastra,(India)

ABSTRACT

Now a day is very important to maintain a high level security to keep information safe and secure between different organizations. The data communication over internet is always under threat of intrusions and misuses. Thus the intrusion Detection Systems have become a need in network security. Fuzzy logic and Genetic Algorithm are two techniques that can use combine to classify network attack information. Fuzzy rule is a machine learning algorithm that can classify network attack data, while a genetic algorithm is an optimization algorithm that can use to find appropriate fuzzy rule and give the best solution. The objective of this paper is to describe a fuzzy genetic based learning algorithm and discuss its usage to detect intrusion in a computer network.

Keywords **IDS, IPS, Intrusion, *Fuzzy logic, Genetic Algorithm.***

I. INTRODUCTION

An intrusion can be defined as an unauthorized entry to other area, but in terms of computer science, by compromising the basic computer network security goals viz. confidentiality, integrity and privacy. Intrusion Detection is the process of monitoring the events happen in a host computer system or network and analyzing them for signs of possible incidents of security threats and violations of computer security practices, acceptable use standard security policies [5]. Intrusion Detection System (IDS) is a software or hardware component. Intrusion Prevention System (IPS) is the technology of both detecting of intrusion and taking preventive actions. Previously proposing intrusion detection techniques based on different classification algorithms. Most Classification techniques for intrusion detection can be categories into two types, first is supervised learning approach second is unsupervised learning approach [2]. Supervised learning approach, Consists of current data input attributes and produce desirable output and the algorithm produce an inferred function, which is called a classifier or regression function. This approach has high accuracy, low false-alarm with fast computing time.

Unsupervised learning approach, consists of current data input attributes and produce output. Fuzzy logic is a super set of Boolean logic that has been extended to handle the concept of partial truth-to-truth values between completely truth and completely false.

II. HISTORY & DEVELOPMENT

Data Security has been a most prior issue ever since the assessment of computers and their applications. According to study of Intrusion detection has been live field of research and development about more than four decades now. It begins from 1980 with the publication of John Anderson's Computer Security threat monitoring and surveillance. It is the starting research papers on this area. Dorothy Denning's seminal paper, "An Intrusion Detection Model "published in 1987 provided the information about rules framework. After that, for the past three decades, improvement in this research and great size commercial investments, Intrusion Detection technology is not ripe and ineffective. In the begin days of computers, hackers very rarely used automated tools to attack's into system. They need high level of expert and they followed their own new techniques to perform malicious actions. Today outline is quite different.

A number of intrusion tools and software are present today that can be used to exploit scripts according to known vulnerabilities. **Figure-1** depicts the relation between the relative Experience of attack and attackers from 1980 to present days. Before the development of new IDS, intrusion detection consisted of a manual finding or detection of anomalies. Due to the availability of huge processing speed it now became possible to detection of "real-time" and gives trigger alerts to the control panel if intrusions were detected. Due to the huge amount of financial losses problem of the computer downtime, loss of image, or even personal data being affected, now days the demand for not only being alerted in the occurred event of an attack, but also to prevent the attack has become an absolute necessity. Especially with the begin of Probing, User to Root Attacks, Remote to User Attacks, Denial of Service and Distributed Denial of Service attacks, the market needs have grown stronger and stronger for Intrusion Prevention Systems (IPS) rather than mere intrusion detection[3].

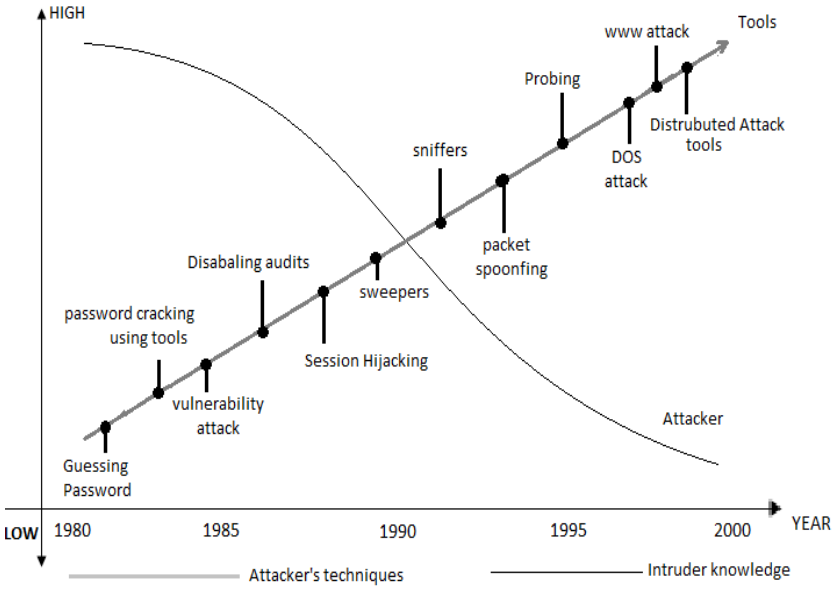

Figure 1: Attack Sophistication Vs Intruder Technical Knowledge

III. INTRUSION DETECTION SYSTEMS

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways. Intrusion detection is the act of detecting unauthorized traffic and unsure activity on a network or a device. An Intrusion Detection System (IDS) can be a piece of software or a physical appliance that detectors network traffic in order to detect unwanted activity and events such as unlawful and malicious traffic, traffic that break security policy, and traffic that violates acceptable use scheme[4]. Number of IDS tools will also store a detected event in a log to be reviewed at a later date or will combine events with other data to make decisions regarding policies or damage control. The key futures of IDS can be pointed out as follows

1. Recording information related to notice events.
2. Inform Administrators of important notice events.
3. Producing reports.

IV. METHODS OF INTRUSION DETECTION SYSTEM

The two basic techniques used by Intrusion Detection Systems for detecting intruders are Misuse Detection (also called signature based detection) and Anomaly Detection.

4.1 Signature Based Detection

The signature is a pattern that corresponds to a known threat. In signature based detection, observed events are compared against the pre-defined signatures in order to identify possible unwanted traffic. This type of detection technique is very fast and easy to configure. Signature-asked detection is very effective at detecting known threats but largely ineffective at detecting previously unknown threats, threats disguised by the use of evasion techniques, and many variants of known threats. An attacker can slightly modify an attack to render it undetectable by a signature based IDS. Still, IDS using signature based methodology, though having limited capability, can be very accurate [1].

Misuse Detection system tries to match data with known attack pattern. In this system every signature requires entry in a database which is one of the big challenges. It may hundreds or even thousands of entries and each packet is compared with all the entries in the database. Signature detection involves searching network traffic for a series of malicious bytes or packet sequences. The main advantage of this technique is that signatures are very easy to develop and understand if we know what network behavior we are trying to identify. For instance, we might use a signature that looks for particular strings within exploit particular buffer overflow vulnerability. The events generated by signature based IDS can communicate the cause of the alert.

Advantages

1) It raises fewer false alarms because they can be very specific about what it is they are looking for.

Disadvantages

1) Any new form of misuse is not detected.
2) Resource consuming and slows down the throughput.

4.2 Anomaly Based Detection

Anomaly-based detection is the process of comparing definitions of what activity is considered normal against Observed events to identify significant deviations. An IDS using anomaly-based detection has profiles that represent the normal behavior of such things as users, hosts, network connections, or applications. The profiles are developed by monitoring the characteristics of typical activity over a period of time. The major benefit of Anomaly based detection technique is that they can be very useful for detecting unwanted traffic that is not specifically known. For instance, anomaly-based IDS will detect that an Internet protocol (IP) packet is malformed. It does not detect that it is malformed in a specific way, but indicates that it is anomalous.

Advantage

1) New form of attack can be detected.

Disadvantages

1) It raises high false alarm
2) Limited by training data

4.3 Combined Anomaly And Misuse Detection

Research has also been conducted into intrusion detection methodologies which combine the anomaly detection approach and the misuse detection approach. These techniques seek to incorporate the benefits of both of the standard approaches to intrusion detection. The combined approach permits a single intrusion detection system to monitor for indications of external and internal attacks. While a significant advantage over the singular use of either method separately, the use of a combined anomaly/misuse detection mechanism does possess some disadvantages. The use of two knowledge bases for the intrusion detection system will increase the amount of system resources which must be dedicated to the system. Additional disk space will be required for the storage of the profiles, and increased memory requirements will be encountered as the mechanism compares user activities with information in the dual knowledge bases. In addition, the technique will share the disadvantage of either method individually in its inability to detect collaborative or extended attack scenarios.

V. METHODS OF INTRUSION DETECTION SYSTEM

There are four types of IDS technologies based on the type of events that they notice and the ways in which they are deployed.

1. Network Based
2. Host Based
3. Wireless
4. Network Behavior Anomaly Detection

5.1 Network Based Ids

Network based IDS Notice network traffic for a special network segment and analyzes the network and software protocol activity to detect suspicious activity. It is most specially denoted at a boundary between networks such as in routers, firewalls, virtual private networks etc. The main disadvantage of this type of intrusion Detection System is that it has a single point of failure. Moreover, it is weak against Denial of Service attacks. It monitors the whole network and denoted at the boundary of the network. But it is not suitable for securing each of the hosts within the network. If an intruder can bypass it, all the systems within the network would be in troubling the problem.**Figure-2** depicts the functioning of NIDS.

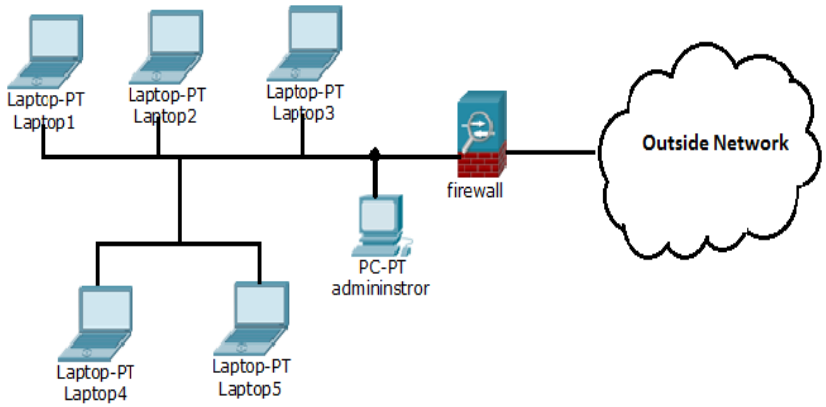

Figure 2: Functioning of NIDS

5.2 Wireless Ids

A wireless local area network Intrusion Detection System is similar to Network IDS in that it can examine network traffic. However, it will also examine wireless-specific traffic, including analyze for external users trying to connect to access point (AP), rogue APs, users outside the physical area of the company, and WLAN IDSs built into APs. As networks more and more support wireless technologies at various points of a topology, WLAN IDS will play huge roles in security. Many back NIDS tools will include improvements to support wireless traffic analysis.

5.3 HOST BASED IDS

In Host-based IDS (HIDS) technology, software engineer are installed on each of the computer hosts of the network to monitor the events occurring within that host only. HIDS notice network traffic and system-specific settings such as software calls, local security policy, local log audits. It performs log notice, file integrity checking, policy monitoring, root kit detection, real-time alerting and active reply. HIDS are most commonly deployed on critical hosts such as publicly accessible servers and servers containing sensitive data. HIDS minimize the problems incurred in Network based IDS technology of securing special hosts in the network. But they cause a substantial overhead for the hosts running them**.Figure-3** depicts the functioning of HIDS.

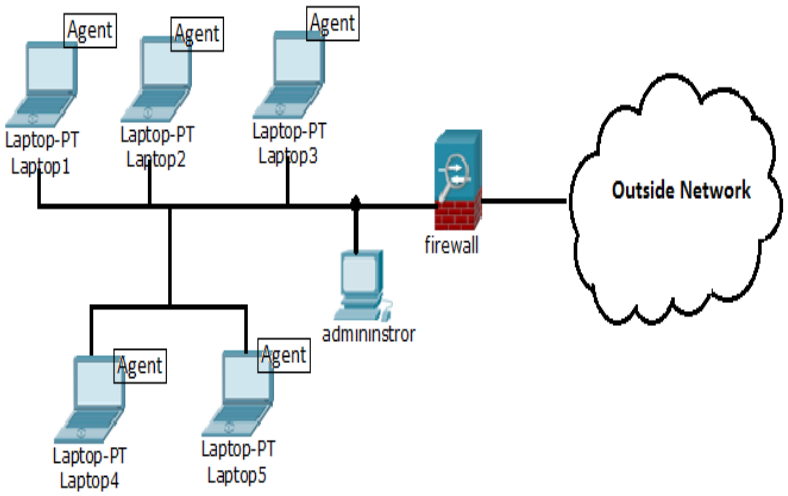

Figure 3: Functioning of HIDS

VI. INTRUSION PREVENTION SYSTEMS

Intrusion prevention system (IPS) is the process of detecting intrusion malicious activities and managing responsive actions on those detected intrusions together. Intrusion prevention systems combine the best features of a firewall and IDS. IPS are monitoring real time intrusion or which match specific profiles and will trigger the generation of alerts and it can drop, block that traffic in real time pass through in system or network. The mainly IPS focused is measures to stop an attack in progress. IPS can be termed as the new generation of IDS with practice to protect computers from attacks. IPS is an intelligent device or software that is capable of not only monitoring malicious activities, but also to take appropriate preventive actions to secure the system or the network. IDS are accurately suited for network attack monitoring and for alerting administrators about malicious activities. Because of its speed, performance and passive limitations have opened the door for development of IPS to challenge it as theproactive defense choice. The key functionalities of IPS are as follows

1) IPS detects and takes preventive actions against malicious attacks.

2) IPS stops the attack itself no more efforts required.

3) IPS changes the security environment.

VII. FUZZY LOGIC

It has been shown by Baruah that a fuzzy number [a, b, c] is defined with reference to a membership function. $\mu(x)$ lying between 0 and 1, $a \leq x \leq c$. Further, he has extended this definition in the following way. Let $\mu 1(x)$ and $\mu 2(x)$ be two functions, $0 \leq \mu 2(x) \leq \mu 1(x) \leq 1$. He has concluded $\mu 1(x)$ the fuzzy membership function, and $\mu 2(x)$ a reference function, such that $(\mu 1(x) - \mu 2(x))$ is the fuzzy membership value for any x. Finally he has characterized such a fuzzy number by $\{x, \mu 1(x), \mu 2(x); x \in \Omega\}$. The complement of μxis always counted from the ground level in Zadehian's theory [6], whereas it actually counted from the level if it is not as zero that is the surface value is not always zero. If other than zero, the problem arises and then we have to count the membership value from the surface for the complement of μx. Thus it could conclude the following statement –

Complement of μx = 1 for the entire level Membership value for the complement of μx = 1- μx. My system forwarded a definition of complement of an extended fuzzy set where the fuzzy reference function is not always zero. The definition of complement of a fuzzy set proposed by Hassan [4], Baruah [6], In the two classes classification problem, there are two classes where every object should be classified. These classes are called positive (abnormal) and negative (normal). The data set used by the learning algorithms consists of a set of objects, each object with n+1 attributes. The first n attributes define the object characteristics (monitored parameters) and the last attribute defines the class that the object belongs to the classification attribute. A fuzzy classifier for solving the two class classification problem is a set of two rules, one for the normal class and other for the abnormal class, where the condition part is defined using only the monitored parameters and the conclusion part is an atomic expression for the classification attribute.

VIII. GENETIC ALGORITHM

A Genetic Algorithm (GA) is a programming technique that refers biological evolution as a problem solving scheme. It is based on Darwinian's principle of evolution and survival of fittest to compute a population of candidate solutions towards a predefined fitness [1].The defined GA based intrusion detection system contains two modules where each works in a particular stage. In the training stage, a set of classification rules are invented from network audit data using the GA in an offline environment. In the intrusion detection stage, the generated rules are used to classify incoming network connections in the real-time environment. Once the rules are generated, the intrusion detection system becomes simple, experienced and well organized one.GA contains an evolution and natural selection that uses a chromosome-like data structure and finds the chromosomes using selection, recombination and mutation operators. The process usually starts with randomly generated population of chromosomes, which constitute of all possible solution of a problem that are referred as candidate solutions. From each chromosome different positions are encoded as bits, numbers. These positions could be referred to as genes. An evaluation function is used to calculate the propriety of each chromosome according to the possible solution; this function is known as "Fitness Function". During the process of evaluation "Crossover" is used to simulate natural reproduction and "Mutation" is used to mutation of species. For survival and combination the selection of chromosomes is essential towards the fittest chromosomes. When GA is used for solving various problems three factors will have vital impact on the effectiveness of the algorithm and for the applications.

1) The fitness function
2) The representation of individuals
3) The GA parameters.

VIII. CONCLUSION

In this paper some basic concepts of IDS are introduced and discussed. The different neural network approaches, techniques and methods are discussed in this review paper. We also discussed the concept of IPS and combine approach of IDS and IPS i.e. IDPS.As IDS technologies further to evolve, they will more closely resemble their real-world counterparts. Instead of isolated sensor units, the IDS of the future will combine of sensor units that report to master visualization consoles which are accountable for checking whether alerts from

the sensors agree or correlate to likely event-chains. In the future, IDS, firewalls, VPNs, and related security technologies will all come to interoperate to a much higher degree. As IDS data becomes more reliable because of more coverage, firewalls and VPN administrators will be more comfortable with reacting based on the input from the IDS. The actual generation of IDS (HIDS and NIDS) are quite powerful already; as continue to improvement IDS becomes the backbone of the more flexible security systems as expected

IX. ACKNOWLEDGEMENT

We take this opportunity to thank our Head of the Department Prof. S. M. Bhagat for their valuable guidance and for providing all the necessary facilities.

REFERENCES

[1] P. Jongsuebsuk+, N. Wattanapongsakorn+, C. Charnsripinyo," Real-Time Intrusion Detection with Fuzzy Genetic Algorithm", +Department of Computer Engineering King Mongkut's University of Technology Thonburi, Bangkok, Thailand National Electronics and Computer Technology Center 112 Phahonyothin Road, Klong Luang, Pathumthani, Thailand IEEE 2013

[2] Mostaque Md. Morshedur Hassan, "Network Intrusion Detection System Using Genetic Algorithm and Fuzzy Logic", Journal of Innovative Re-search in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 1, Issue 7, September 2013

[3] Prof. C. Vaidya, Dr. M. Raghuwanshi,"Survey: Learning Techniques for Intrusion Detection System (IDS)",International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 1, Issue 2, Feb 2014. ISSN 2348 4853.

[4] V. Jyothsna, V. V. Rama Prasad,"A Review of Anomaly based Intrusion Detection Systems", International Journal of Computer Applications (0975 8887) Volume 28 No.7, September 2011.

[5] S. N. Pawar"INTRUSION DETECTION IN COMPUTER NETWORK USING FGA", Associate Professor (E &TC),Jawaharlal Nehru Engineering College, Aurangabad, MS, India, IEEE JOURNAL ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 3, MARCH 2012.

[6] NilotpalChakraborty , "Intrusion Detection System And Intrusion Prevention System: A Comparative Study" International Journal of Computing and Business Research (IJCBR) ISSN (Online) : 2229-6166 Volume 4 Issue 2 May 2013.