International Journal of Science Engineering and Advance Technology, IJSEAT, Vol 2, Issue 3, March - 2014 | ISSN 2321-6905

International Journal of Science Engineering and Advance Technology

Network Intrusion Detection Systems Using Genetic Algorithm

Sabbithi Suresh Kumar[1], T Rajendra Prasad[2]
[1]M Tech Student, KIET, Koringa,Andhra Pradesh,INDIA
[2]Assistant Professor, KIET, Koringa,Andhra Pradesh,INDIA
Emails:[1]sabbithisuresh@gmail.com,[2] rajendraprasad.tanukula@gmail.com

Abstract

Intruder Detection system is so important implementations which considers all network information like temporal and spatial which make the system to build the rule for IDS. This helps for the administrator to detect complex anomalous behaviors of the system. This work is focused on the TCP/IP network protocols.

Genetic Algorithm is used to generate dynamic IP for the network to avoid unauthorized data transfer and prevent from attack. The Intrusion Detection System can be viewed as a rule-based system (RBS) and Genetic Algorithm can be viewed as a tool to help generate knowledge for the RBS. This project shows how network connection information can be modeled as chromosomes and how the parameters in genetic algorithm can be defined in this respect.

Key words- IDS, GA, RBS, TCP/IP

1. Introduction

In recent years, Intrusion Detection System (IDS) has become one of the hottest research areas in Computer Security. It is an important detection technology and is used as a countermeasure to preserve data integrity and system availability during an intrusion.An Intrusion Detection System is a system for detecting intrusions and reporting them accurately to the proper authority. Intrusion Detection Systems are usually specific to the operating system that they operate in and are an important tool in the overall implementation an organization's information security policy, which reflects an organization's statement by defining the rules and practices to provide security.

A methodology of applying genetic algorithm into network intrusion detection technique is unique as it considers both temporal and spatial information of network connections during the encoding of the problem; therefore, it should be more helpful for identification of network anomalous behaviors.The project titled Intrusion Detection System In Networking Using Genetic Algorithm (IDS) is to identify the intruder and block the data from the intruder to avoid the system attack by the virus. This new system is a replacement of the existing system. In existing system, at run time it will not create a set of rules. The major components of the system are creating new set of rules during run time.Interest and knowledge about computer and network security is growing along with the need for it. This interest is, no doubt, due to the continued expansion of the Internet and the increase in the number of businesses that are migrating their sales and information channels to the Internet. The growth in the use of networked computers in business, especially for e-mail, has also fueled this interest. Many people are also presented with the post-mortems of security breaches in high-profile companies in the nightly news and are given the impression that some bastion of defense had failed to prevent some intrusion. One result of these influences is that that many people feel that Internet security and Internet firewalls are synonymous. Although we should know that no single mechanism or method will provide for the entire computer and network security needs of an enterprise, many still put all their network security eggs in one firewall basket.

Computer networks may be vulnerable to many threats along many avenues of attack, including:

Social engineering, wherein someone tries to gain access through social means (pretending to be a legitimate system user or administrator, tricking people into revealing secrets, etc.)

War dialing, wherein someone uses computer software and a modem to search for desktop computers equipped with modems that answer, providing a potential path into a corporate network
Denial-of-service attacks, including all types of attacks intended to overwhelm a computer or a network in such a way that legitimate users of the computer or network cannot use it
Protocol-based attacks, which take advantage of known (or unknown) weaknesses in network services
Host attacks, which attack vulnerabilities in particular computer operating systems or in how the system is set up and administered
Password guessing
Eavesdropping of all sorts, including stealing e-mail messages, files, passwords, and other information over a network connection by listening in on the connection.
Internet firewalls have been around for a hundred years—in Internet time. Firewalls can help protect against some of these attacks, but certainly not all. Firewalls can be very effective at what they do. The people who set up and use them must have the knowledge of how they work, and also be aware of what they can and cannot protect. An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

Existing System:

Traditional systems in place for intrusion detection primarily use a method known as "fingerprinting" to identify malicious users. They are complex.
They are rules dependent .If the behavior of the packets flowing in the network is new, then the system cannot take any decision. So they purely work in the basis of the initial rules provided.
The rules in the dataset are static unless the network administrator manually enters the rules. It does not provide any option for generating dynamic rule set.
It cannot create its own rule depending on the current situation.
It requires manual energy to monitor the Inflowing packets and analyze their behavior.
It cannot take decisions in runtime.
If the pattern of the packet is new and not present in the records, then it allows the packet to flow without analyzing whether it is a intruder or not.
The packet with a new behavior can easily passed without being filtered

Proposed System:

It uses Genetic algorithm, which an artificial intelligence problem-solving is based on the theory of Darwinian evaluation applied to mathematical models.
Intrusion Detection System compare learned user characteristics from an empirical model to all users of a system.
It includes both temporal and spatial information of the network traffic in the rule set.
It is both network based and host based system.
It can take decisions in runtime.

3.1 Advantages:

It eliminates the need for an attack to be previously known to be detected because malicious behavior is different from normal behavior by nature.
Using a generalized behavioral model is theoretically more accurate, efficient and easier to maintain than a fingerprinting system.
It uses a constant amount of computer resources per user, drastically reducing the possibility of depleting available resources.
Once installed, there is no need for any manual energy to monitor the system.
It generates its own rules depending on the real-time behavior of the packet.
It dynamically increases the rules in the dataset according to the packets flowing in the network and the decisions taken by the system. Due to the increase of rules in the rule set, the reliability of the system also increases.
It promotes a high detection rate of malicious behavior and a low false positive rate of normal behavior classified as malicious.

Design and Implementation

This is the server side interface which is preset in the server system and is solely under the control of the administrator. Any transaction in the network will be monitored by the Server. It receives the packet and reads the header information from the packet such as the Destination address, Source address, Port no. It sends each and every Inflowing packets header information's to the chromconvert module and then receives the converted real-time Chromosomes. The real time chromosomes are checked with the rule sets. If the particular chromosomes matches with the rules provided in the rule set, it takes the decision of whether allow or block depending on which rule set it matches.

The server also monitors the intermediate systems through which the packets are passed. These passer

systems are also taken into account to judge whether or not a real-time connection is considered an intrusion.

4.1 Chromosome Conversion:

The collected attributes are converted into Chromosomes within the range and in the same behavior. The process of a genetic algorithm usually begins with a randomly selected population of chromosomes. These chromosomes are representations of the problem to be solved.

According to the attributes of the problem, different positions of each chromosome are encoded as bits, characters, or numbers. These positions are sometimes referred to as genes and are changed randomly within a range during evolution. The set of chromosomes during a stage of evolution are called a population. An evaluation *function* is used to calculate the "goodness" of each chromosome

For example) a real time behavior rule looks like If {the connection has following information: source IP address 124.12.5.18;destination IP address: 130.18.206.55; destination port number: 21; connection time: 10.1 seconds}
then {stop the connection}

The following rule is converted into Chromosomes as:
(d, 1, 0, b, -1, -1, -1, -1, 8, 2, 1, 2, b, -1, -1, -1, 4, 2, 3, 3,
5, 0, 0, 0, 8, 0, 0, 0, 0, 0, 0, 4, 8, 2, 1, 1, 2, 0, 0, 0, 0, 0, 0, 7, 3, 2, 0, 0, 0, 0, 0, 0, 3, 8, 8, 9, 1).

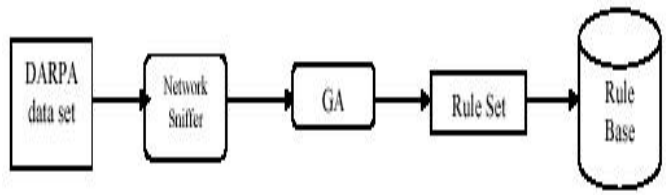
4.2 Genetic Algorithm Implementation:

The Genetic Algorithm is implemented, for selecting the best rule for matching with the connection. During evaluation, the selection of chromosomes for survival and combination is biased towards the fittest chromosomes. The members of this initial population are each evaluated for their *fitness* or goodness in solving the problem. From the initial population of chromosomes, a new population is generated using three genetic operators: *reproduction*, *crossover*, and *mutation*.
These are modeled on their biological counterparts.
With probabilities proportional to their fitness, members of the population are *selected* for the new population.
Pairs of chromosomes in the new population are chosen at random to exchange genetic material, their bits, in a mating operation called crossover. This produces two new chromosomes that replace the parents.
Randomly chosen bits in the offspring are flipped, called mutation.
The new population generated with these operators replaces the old population.
The algorithm has performed one *generation* and then repeats for some specified number of additional generations.
The population evolves, containing more and more highly fit chromosomes.
When the convergence criterion is reached, such as no significant further increase in the average fitness of the population, the best chromosome produced is decoded into the search space point it represents.

4.3 Creating rules in Dataset:

The Rules (Both Normal and Anomal) are created in the dataset, as the chromosomes for matching with the real time connection. The administrator can just specify the attributes that he thinks to be both normal and abnormal in the specified screen provided. The Entered behaviors are automatically converted into Chromosomes, and stored in the rule set to which he specified. These rules are responsible for providing knowledge for both the Intrusion Detection System and Genetic algorithm.

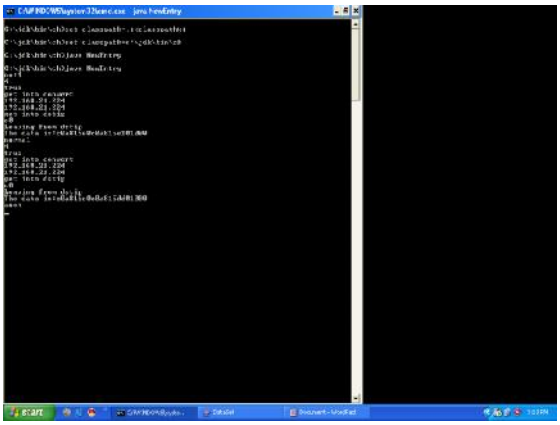
System Architecture:



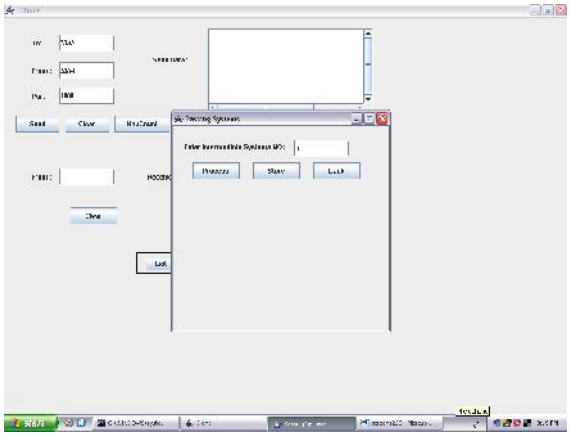
The Figure shows the structure of this implementation. We need to collect enough historical data that includes both normal and anomalous network connections. This is the first part inside the system architecture. The network sniffers analyze this data set and results are fed into Genetic Algorithm for fitness evaluation. Then the Genetic Algorithm is executed and the rule set is generated. These rules are stored in a database to be used by the Intrusion Detection System.

ISSN 2321-6905

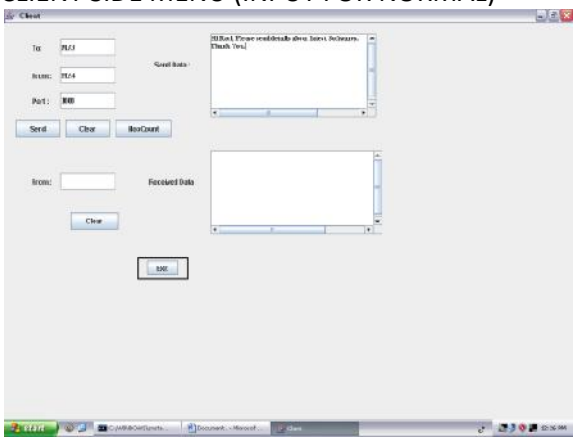
Experimental results



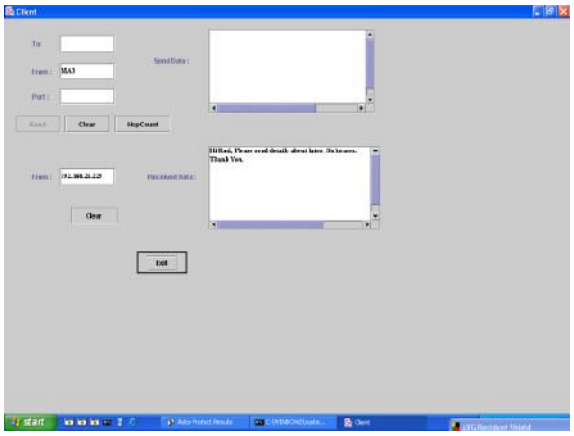
NORMAL & ANOMALOUS DATA SET OUTPUTS



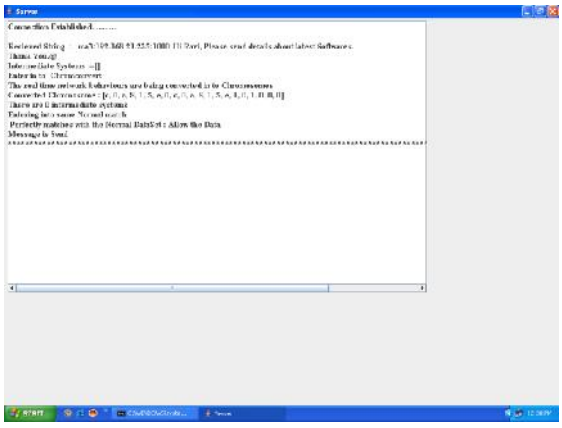
CLIENT SIDE MENU (INPUT FOR NORMAL)



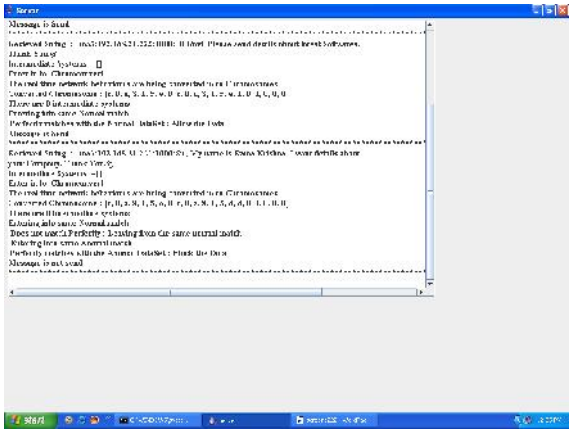
CLIENT SIDE MENU (OUTPUT FOR NORMAL)



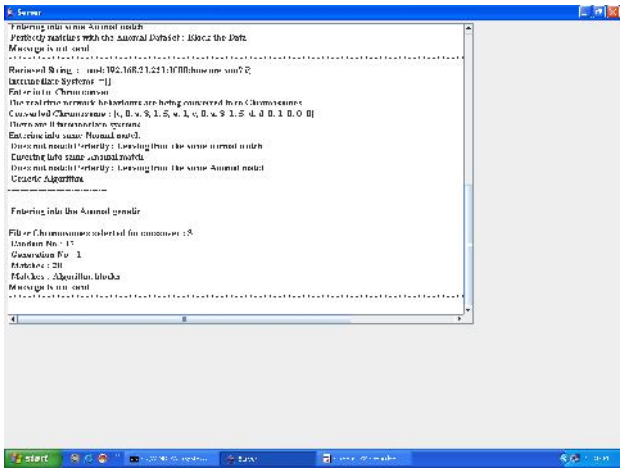
SERVER SIDE MENU FOR NORMAL



SERVER SIDE MENU FOR ANOMALOUS



CLIENT SIDE MENU (INPUT FOR GENETIC ALGORITHM)



SERVER SIDE MENU FOR GENETIC ALGORITHM

CONCLUSION:

The software development is very flexible and much functionality can be added to it, to enhance performance of this project titled "Intrusion Detection System In networking Using Genetic Algorithm". By using genetic algorithm, during run time the new set of rules will added in the dataset. A brief overview of Intrusion Detection System, Genetic algorithm, and related detection techniques are discussed. This implementation of genetic algorithm is unique as it considers both temporal and spatial information of network connections during the encoding of the problem; therefore, it should be more helpful for identification of network anomalous behaviors. The project was successfully completed within the time span allotted.

Future work includes creating a standard test data set for the genetic algorithm proposed and applying it to a test environment. Detailed specification of parameters to consider for genetic algorithm should be determined during the experiments. Combining knowledge from different security sensors into a standard rule base is another future.

REFERENCES

[1] M. Botha, R. Solms, "Utilizing Neural Networks For Effective Intrusion Detection", ISSA,2004.

[2] R. Graham, "FAQ: Network Intrusion Detection Systems". March 21, 2000.

[3] D. Zamboni, "Using Internal Sensors For Computer Intrusion Detection". Center for Education and Research in Information Assurance and Security, Purdue University. August 2001.

[4] K. Scarfone, P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)". Computer Security Resource Center (National Institute of Standards and Technology). February 2007.

[5] A. Chittur, "Model Generation for an Intrusion Detection System Using Genetic Algorithms". January 2005.

[6] W. Li, "Using Genetic Algorithm for Network Intrusion Detection". "A Genetic Algorithm Approach to Network Intrusion Detection". SANS Institute, USA, 2004.

[7] W. Lu, I. Traore, "Detecting New Forms of Network Intrusion Using Genetic Programming". Computational Intelligence, vol. 20, pp. 3, Blackwell Publishing, Malden, pp. 475-494, 2004.

[8] M. M. Pillai, J. H. P. Eloff, H. S. Venter, "An Approach to Implement a Network Intrusion Detection System using Genetic Algorithms", Proceedings of SAICSIT, pp:221-228, 2004.

[9] S. M. Bridges, R. B. Vaughn, "Fuzzy Data Mining And Genetic Algorithms Applied To Intrusion Detection", Proceedings of 12th Annual Canadian Information Technology Security Symposium, pp. 109-122, 2000.

[10] J. Gomez, D. Dasgupta, "Evolving Fuzzy Classifiers for Intrusion Detection", Proceedings of the IEEE, 2002.

[11] M. Middlemiss, G. Dick, "Feature selection of intrusion detection data using a hybrid genetic algorithm/KNN approach", Design and application of hybrid intelligent systems, IOS Press Amsterdam, pp.519-527, 2003.

[12] Srinivas Mukkamala, Andrew H. Sung, Ajith Abraham, "Intrusion detection using an ensemble of intelligent paradigms", Journal of Network and Computer Applications, Volume 28, Issue 2, April 2005, Pages 167-182

[13] S. Peddabachigari, Ajith Abraham, C. Grosan, J.Thomas, "Modeling intrusion detection system using hybrid intelligent systems", Journal of Network and Computer Applications, Volume 30, Issue 1, January 2007, Pages 114–132

[14] M. Saniee Abadeh, J. Habibi, C. Lucas, "Intrusion detection using a fuzzy genetics-based learning algorithm", Journal of Network and Computer Applications, Volume 30, Issue 1, January 2007,Pages 414-428

[15] Tao Peng, C. Leckie, Kotagiri Ramamohanarao, "Information sharing for distributed intrusion detection systems", Journal of Network and Computer Applications, Volume 30, Issue 3, August 2007, Pages 877–899