Artificial Intelligence Techniques for Network Intrusion Detection

Karan Napanda
Computer Department
Dwarkadas J. Sanghvi COE
Mumbai, India.

Harsh Shah
Computer Department
Dwarkadas J. Sanghvi COE
Mumbai, India.

Prof. Lakshmi Kurup
Computer Department
Dwarkadas J. Sanghvi COE
Mumbai, India.

***Abstract*—Network Intrusion has become the biggest concern of this generation. A lot of data is stored on commercial and personal computers. Protection and confidentiality of such information is very crucial for personnel in organizations which operate on classified data. This paper aims to study the different AI techniques that can be used in support of Intrusion (Anomaly and Misuse) Detection Systems to provide better Intrusion Detection & Prevention. This paper sheds light on techniques like ML, NEURAL NETWORK and Fuzzy Logic and how they can be coupled with INTRUSION DETECTION SYSTEM to detect attacks on private networks. It also provides other techniques which can be used for intrusion detection like Naïve Bayes, Decision Tree, K-nearest neighbors and Support Vector Machine. These techniques were used to classify malicious activity and normal activity and base rules such that necessary actions can be committed to alert and prevent intrusion.**

Keywords—Network Intrusion Detection, Artificial Intelligence, Machine Learning, Neural Networks, Genetic Algorithm, Fuzzy Logic.

I. INTRODUCTION

Communication through the Internet plays a very crucial role in everyone’s daily life. An individual’s life revolves around data, information and everything on the Internet. The Internet holds a lot of crucial information with itself. Crucial information of business organizations, governmental organizations, non-governmental institutions and more are stored online. With such information on the Internet, the world has witnessed a rise in the attempted of information breaches on such crucial information. Access to such information can be very harmful.

The first solution that comes to our mind is an Intrusion Detection System (Intrusion Detection System). Since most of the Intrusion Detection System are signature based, to develop such a sophisticated Intrusion Detection System that can detect and prevent already known and predict unknown attacks is technically unfeasible.[2] It has become mandatory to maintain the confidentiality, availability, and integrity of data. A topic that stands out as a potential solution to this vulnerability is the use of Machine Learning (ML), an Artificial Intelligence (AI) technique of learning..

II. OVERVIEW OF INTRUSION DETECTION SYSTEMS

A. Selecting a Template (Heading 2)

Intrusion Detection, in short can be defined as the detection of action that attempt to compromise the confidentiality, integrity or availability of a resource. Thus, Intrusion Detection System is a device that monitors computer systems and network traffic and analyses that traffic for possible contentious attacks arising from outside the organization and also for system misuse or attacks originating from inside the organization. An Intrusion Detection System can be divided accordingly in different ways.

INTRUSION DETECTION SYSTEM can either be bifurcated as a NIDS (Network IDS) or as a HIDS (Host IDS). Network based Intrusion Detection analyses the network traffic and tries to pinpoint unlicensed, illegitimate and anomalous behavior on the network. The Network Intrusion Detection System captures packets traversing through the network using span port or network taps in order to detect and flag any suspicious activity. It does not block network traffic and works passively. A Host based IDS is device specific and seeks to detect malicious activity or anomalous behavior on the specific device. It usually involves an agent working on each system, observing and alerting on local OS. The Intrusion Detection System uses signatures that were pre-defined depending on attack characteristics to track unauthorized activity. The HIDS also plays a passive role.

An Intrusion Detection System can also be divided as an active or a passive Intrusion Detection System. Passive IDS’ only monitor the network traffic and informs the network administrator of abnormal activity. It is now the responsibility of the administrator to take the necessary actions. Whereas, an active Intrusion Detection System works as an Intrusion Prevention System (IPS). It attempts at preventing and resolving issues caused by intrusion, by taking necessary actions after detection through monitoring.

IDS’ can also be divided according to their detection logic, as signature based or anomaly based intrusion detection.[9] A signature based IDS detects suspicious activity by comparing its attributes against a database of characteristics of known signature attacks. The only drawback is that since the signature based IDS’ rely on previously known information, they are susceptible to newer attacks. Even if the attacks are updated, the delay in updating process will cause malicious software to penetrate the system undetected. An anomaly based IDS checks the characteristics against a baseline. The baseline decides if the activity is suspicious or not & false positives are a big problem.

III. ARTIFICIAL INTELLIGENCE

Artificial Intelligence is the design of intelligent machines through the branch of computer science, where an intelligent machine is a system that perceives its environment and takes actions that maximise its chance of success. It uses computational models to achieve goals and study the mental faculty. In short, AI is the study of how to make computers do things which, at the moment, people do better. These AI learning techniques can be applied for better Intrusion Detection System use. Different Artificial Intelligence techniques can be used for Intrusion Detection System and Intrusion Protection System as well. A current trend in the development is the implementation of Expert Systems. Along with Neural Network, Genetic Algorithm, Fuzzy Logic and others, Expert Intrusion Detection Systems are being developed for recognising and learning through patterns. An expert system consists on a knowledge base where it stores rules and makes inferences for the purpose

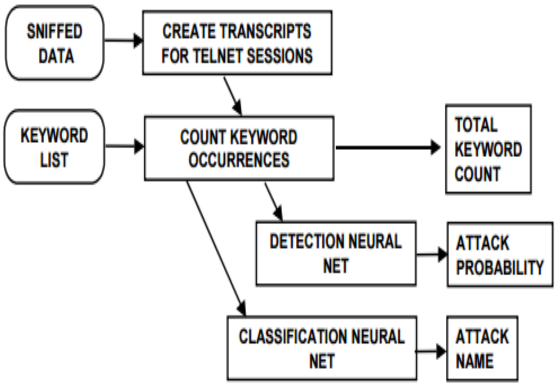
IV. USING AI FOR NID.

A. Machine Learning

Intrusion Detection has been a major research and concern problem in today's world, considering the amount of confidential data that flows through different connections. A number of Machine Learning techniques can be used for anomaly detection. Often only single techniques are used for anomaly detection but the use of a combination of different learning techniques hybrid or ensemble learning techniques are also in use in the recent years. Such techniques are used on the basis of a classifier. The classifier is used to distinguish whether an incoming packet is for a bad connection or a good connection. One of the primary machine learning technique which can be used for anomaly detection is Pattern Classification. Pattern Classification can be implemented using supervised and unsupervised learning as well. In supervised learning, a training data set is trained to create a function which gives an input and output vector. The function creates a classifier and it can classify unknown examples into known class labels. [2]

B. Neural Networks

Neural Networks can be used to build profiles of software behavior and make attempts to distinguish between normal and anomalous/malicious software behavior. The main objective in using Neural Networks is for the Intrusion Detection to be able to generalise from insufficient data and be able to classify between malicious and safe networks. An artificial neural network consists of processing units, or nodes, and connections between them. The connection between any two units has some weight, which is used to determine how much one unit will affect the other. By assigning activation (value) to each input value, and allowing the activations to propagate through the network, a neural network performs a mapping from one set of values (assigned to the input nodes) to another set of values (retrieved from the output nodes). A classical feed-forward multi-layer perceptron rule can be used to create an intrusion detection system as given above. Also, backpropagation network is used successfully in network intrusion detection since backpropagation is used for learning and this will help the Intrusion Detection System to build and learn profiles of anomalous behaviors. [3]



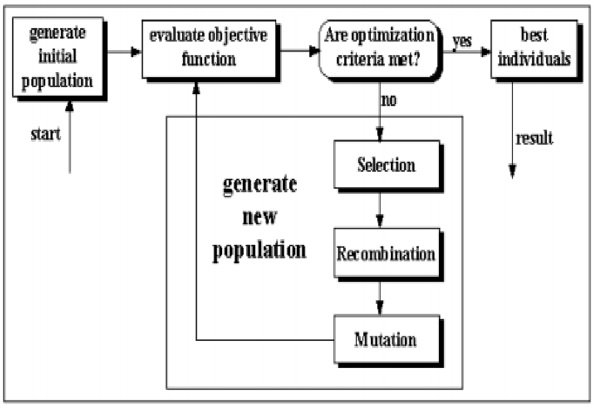
The above is a block diagram of the improved reference intrusion detection system using keyword selection. [7] Network sniffing data is first accessed to convert all data transmitted to and from the victim during telnet sessions. A total number of keyword counts if the first output . Keywords are based on a pre-defined list. Ideally, this count would be directly related to the probability of an attack in a session. These keyword counts are further processed by neural networks in 2 ways. One of the neural networks provides an estimate which gives the improved posterior probability of an attack in a session and the other one tries to classify known attacks to provide an attack name.

Initially 58 keywords were used from a database of keyword-based Intrusion Detection System that detect suspicious actions and well-known attacks. Keyword selection was also done for attack code downloading, attack preparation, the actual break-in where a new root shell was often established, and attacks performed after root-level privilege was obtained. 31 new keywords were added to the existing 58 old keywords. Multilayer perceptron classifier was used for a 10-fold cross validation on the training data to select both keywords and network topology for the detection neural network. For networks with no hidden nodes and feature selection, keywords were selected using weight magnitude pruning. Good detection performance was obtained using 30 keywords and also produced a low false alarm rate but with fewer or more keywords it reduced the detection rate.

Some keyword were classified with strongly positive weights because they were detected often in attacks and some were given negative weights since it was deduced that these were used more often in normal sessions. Thus, this avoids a large amount of false alarms since a lot of these keywords are also used in normal sessions

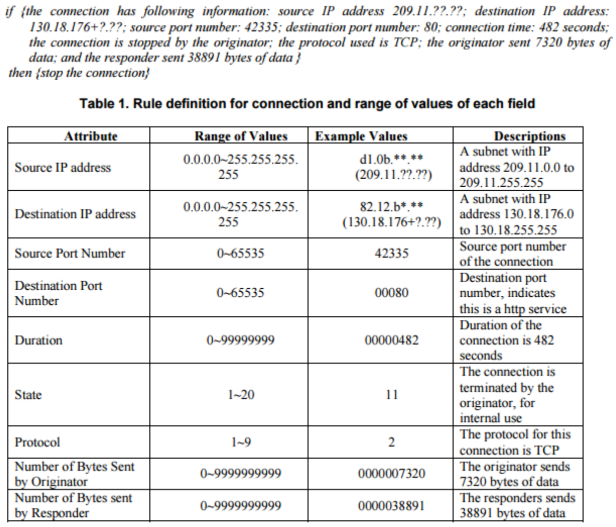
C. Genetic Algorithm

Genetic Algorithm is a class of computational models based on the concepts of natural selection and evolution. Genetic algorithm uses a chromosome like data structure and evolves the chromosome using selection, recombination and mutual operators to convert the problem into a specific domain relating to the model. Genetic algorithm can be used to define simple network access rules. These rules will disallow the passage of already known malicious attacks. These rules are usually stored in the form of if-then rules. These define the genes in the chromosomes, which will be applied previous examples and evaluated accordingly. A correct rule is given importance and an incorrect rule is exempted from selection. This population is then evolved into the optimal set. The evolution takes place using crossover and mutation operators. Because of the efficiency of the evaluation function, the succeeding population are biased towards rules that match intrusion rules. [4]



Thus, in this sense, Genetic Algorithm can be used to simple rules for the network. These rules are basically derived to differentiate between normal and anomalous behavior in the network traffic. These rules are stored in the if {condition} else {action} form such that when the network intercepts any anomalous behavior defined by the if rules, it can perform the action to tackle it. Here, the network traffic used is a pre-classified data set that can differentiate between normal and anomalous behavior. The figure below gives a general idea of how the rules are defined.

[4]

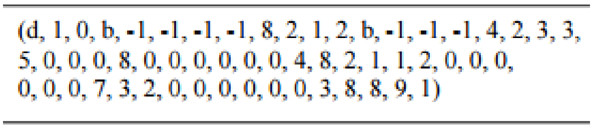


if {the connection has following information: source IP address 209.11.??.??; destination IP address: 130.18.176+?.??; source port number: 42335; destination port number: 80; connection time: 482 seconds; the connection is stopped by the originator; the protocol used is TCP; the originator sent 7320 bytes of data; and the responder sent 38891 bytes of data }
then {stop the connection}

Table 1. Rule definition for connection and range of values of each field

Attribute	Range of Values	Example Values	Descriptions
Source IP address	0.0.0.0~255.255.255.255	d1.0b.**.** (209.11.??.??)	A subnet with IP address 209.11.0.0 to 209.11.255.255
Destination IP address	0.0.0.0~255.255.255.255	82.12.b*.** (130.18.176+?.??)	A subnet with IP address 130.18.176.0 to 130.18.255.255
Source Port Number	0~65535	42335	Source port number of the connection
Destination Port Number	0~65535	00080	Destination port number, indicates this is a http service
Duration	0~99999999	00000482	Duration of the connection is 482 seconds
State	1~20	11	The connection is terminated by the originator, for internal use
Protocol	1~9	2	The protocol for this connection is TCP
Number of Bytes Sent by Originator	0~9999999999	0000007320	The originator sends 7320 bytes of data
Number of Bytes sent by Responder	0~9999999999	0000038891	The responders sends 38891 bytes of data

The above rules form the chromosome base for the Genetic Algorithm. The chromosome form is shown below.



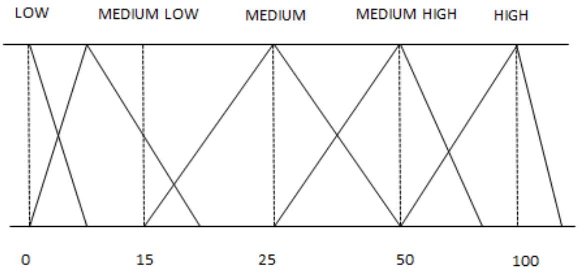
(d, 1, 0, b, -1, -1, -1, -1, 8, 2, 1, 2, b, -1, -1, -1, 4, 2, 3, 3,
5, 0, 0, 0, 8, 0, 0, 0, 0, 0, 0, 4, 8, 2, 1, 1, 2, 0, 0, 0,
0, 0, 0, 7, 3, 2, 0, 0, 0, 0, 0, 0, 3, 8, 8, 9, 1)

Thus, it consists of 57 genes in a chromosome. If a (anomalous behavior) rule is found to be true, a bonus will be given to the respective chromosome and if not (normal behavior), a penalty will be applicable. Also some wild cards are used in the table ('?' and '*'characters) which are given the value of -1. These wild cards represent a specific range of values, which represent a network block in a rule. After this step, the Genetic Algorithm starts with a random population that has randomly selected rules. The population then evolves using crossover and mutation. Ultimately, the processing is stopped and the rules are added to the rule base of the Intrusion Detection System. [4]

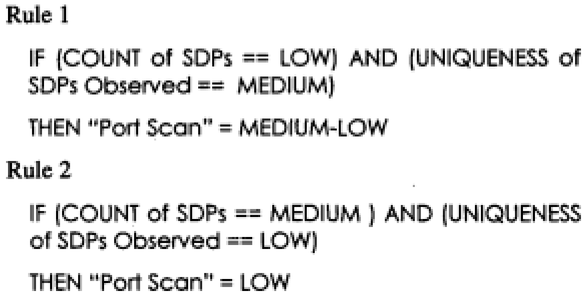
D. Fuzzy Logic

Fuzzy Logic is most effective when solving complex problems. It consists of a fuzzy set of elements where the membership of any element in the fuzzy set can vary from 0 to 1. It does not have a crisp value like in Boolean sets, like 0 & 1. The membership of the elements can be perfectly represented. While Fuzzy c-mean maps an element over 0 to 1, rough c-means classifies the object into lower approximation, boundary and negative region. Now, Fuzzy Rough C-Means will partition the data into 2 classes: lower approximation and boundary. In the first step, we map the symbolic valued attributes to numeric valued attributes (like tcp, udp, icmp, etc.). Then, features were scaled linearly to each range. The testing data is then grouped and fuzzy inference is applied to generate data sets that define rules accurately.[5]

the first step, Data Mining Techniques are applied to a TCP data packet in order to extract parameters which are not obviously mentioned in the packet. These parameters are crucial in the process of segregating normal and anomalous behavior. In short, it is creating parameters which are crucial for giving fuzzy inputs. The source ip address, destination ip address, source & destination port numbers, TCP control bits and other information is extracted. An aggregate key is created composed of the IP source, IP destination and destination port fields. The key is then used to prepare counts and other statistical measures from the mined data. Once the extraction phase is done, it produces fuzzy sets based on the past inputs and a range over which they will vary is calculated. These data feeds are calculated over three characteristics: COUNT, UNIQUENESS and VARIANCE. Also, five fuzzy sets have been chosen to represent the data elements: LOW, MEDIUM-LOW, MEDIUM, MEDIUM-HIGH, HIGH. The fuzzy set inputs for the three domains are shown below:



It might happen that a particular parameter will not be used for a long time. For such parameters, the fuzzy set inputs are defined at LOW and then values vary accordingly. When the fuzzy sets are defined, the rules are defined and that covers as much input as possible. Example of rules are given in the figure below:



Rule 1

IF (COUNT of SDPs == LOW) AND (UNIQUENESS of SDPs Observed == MEDIUM)

THEN "Port Scan" = MEDIUM-LOW

Rule 2

IF (COUNT of SDPs == MEDIUM) AND (UNIQUENESS of SDPs Observed == LOW)

THEN "Port Scan" = LOW

Thus, it was able to detect malicious attackers from outside the network domain. It could also trigger high alerts when anomalous network traffic was observed. [8]

E. Other Methods

i.) K-Nearest Neighbors

A new technique known as the K-nearest neighbor can be used to classify program behavior into normal and intrusive. A separate database of system calls in order to detect anomalous behavior of different programs and learning program profiles invests a lot of time and money. The K-nearest neighbors uses the frequency of system calls to detect malicious activity on the network. Text categorization using K-nearest neighbors is used to categorize texts to convert programs into vectors and use it for comparison and differentiation between two program activities. Text categorization is the process of grouping system call documents into texts of predefined categories. A number of machine learning techniques can be applied to text categorization in a similar manner. Using the vector space model, it is first translated to words. The documents neighbors are then ranked using k-nearest neighbor classifier algorithm. The classes are weighed using the parameter of similarity of the vector to each neighbor. Thus, an analogy is drawn between them for detection. Since, the generation of program profiles is eliminated, the computation complexity is reduced. Also, test results show that the use of K-nearest neighbors produces a very low rate of false positives compared to the other techniques. [6]

ii.) Naïve Bayes

A lot of times we know the statistical dependencies or the casual relationships between the system variables. The basic idea is that there is a chance that some pre-defined variables may influence these system variables. Also, there might be a great difficulty in precisely expressing the relationship between these variables. The statistical, structural and casual relationship between these variables is exploited to form a probabilistic graph model called as the Naïve Bayes network. This model provides answers to questions that can be aroused like, what is the probability that a certain type of an attack can re-occur because of the recording of previous events which give evidence to the same. An answer to the same is provided using a conditional probability formula. A DAG(Direct Acyclic Graph) is used to represent the structure of a Naïve Bayes Network. Here, each of the nodes in the graph represents one of the system variables and the links provide information about the influence on node has on the other.

iii.) Decision Tree

A decision tree is a supervised learning algorithm in which it consists of a flow-graph like structure and each internal node represents a test case for the tree. It classifies a sample such that the current decision helps in making the further decisions which will lead us to a conclusion. Such a sequence of decisions is represented in the form of a decision tree. The traversal from the root to the leaf is such that each leaf represents a certain form of classification. Attributes are labelled to each node and a decision is taken by after computing all the attributes for the particular node. Thus, such a path from the root to the leaf node represents classification rules. These classification rules are defined according to the anomalies recorded by the machine or that have been come across in the history. They are defined according to the behavior and is classified according to the attributes such that when a sample is put through, the decision tree will progress through by making decisions and come to a conclusion which will display is a behavior is malicious or not. A decision tree with a range of discrete (symbolic) class labels is called a classification tree, whereas a decision tree with a range of continuous (numeric) values is called a regression tree. Any tree can be used for Intrusion Detection purposes according to their applications.

iv.) Support Vector Machine

Support Vector Machine is used to solve binary classification problems. It is a supervised learning algorithm that are based on the concept of decision planes that are defined by decision boundaries. It maps a linear algorithm into a non-linear map using a kernel function. Polynomial and radial basis functions are used to for such kind of mapping, which divide the feature space by creating a hyperplane. These kernel functions can be used at the time of training classifiers which chooses support vectors along this function. Thus, these support vectors that outline the hyperplane is used to classify data the Support Vector Machine system. A multiclass Support Vector Machine constructs k phases at the training of the Intrusion Detection System. Thus, multiclass support vector machines can be used for classification in the Intrusion Detection System. The one with the largest margin between classes is the best hyperplane for the Support Vector Machine and this is selected for classification purposes.

V. LITERATURE REVIEW

Among Support Vector Machine, Neural Network, Support Vector Machine had the best performance and K-Nearest Neighbors had the worst. Also, on comparison, it was concluded that Support Vector Machine was better than Neural Network as well. Though Neural Network is the best for generalisation but is poor in the detection of new attacks, DT plays a very efficient role in the generalisation of classes and detection of new attacks. Comparing Naïve Bayes & Decision Tree, Decision Tree has achieved more accuracy that the NB.

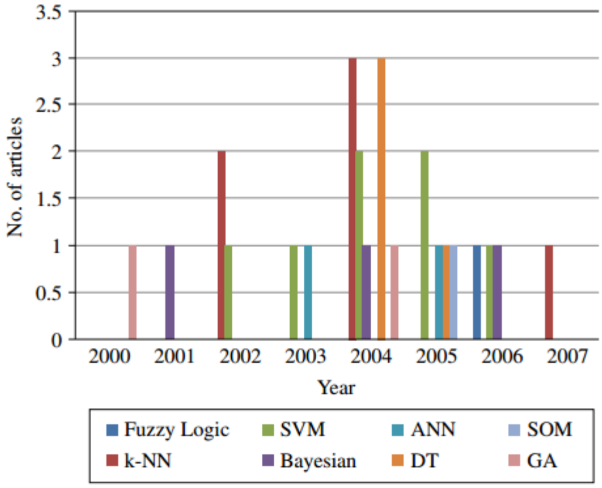


Fig. 1. Example of a figure caption. *(figure caption)*

For literature review, quantitative analysis was done by researching through all websites and scientific forums and publications. Search procedure was conducted using keywords that gave the most results as well. Also, scientific literatures were traversed using Google Scholar mainly because of its simple and open nature. Results showed that ML was the most trending search in terms of Artificial Intelligence. In Artificial Intelligence, Neural Network is the most widely and popularly used algorithm but the popularity decreased in the last couple of years. Also, it was observed that Support Vector Machine was increasing slightly over the past years. Moreover, throughout the years Support Vector Machine was concluded to be the least popular methodology to be used for Intrusion Detection

VI. CONCLUSION

Thus, the paper has discussed different techniques which can be used to improve Intrusion Detection System. It briefly describes four major techniques of Machine Learning, Neural Network, Genetic Algorithm and Fuzzy Logic. How these techniques can be integrated with Intrusion Detection Systems to improvise anomalous and malicious activity, how rules are generated to classify network behaviour and how these classifications are based on is elaborated efficiently

VII. REFERENCES

[1] https://www.sans.org/security-resources/idfaq/what_is_id.php

[2] C. F. Tsai, Y. F. Hsu, C. Y. Lin, and W. Y. Lin, "Intrusion detection by machine learning: A review," *Expert Systems with Applications* 36, no. 10, pp. 11994-12000, 2009.

[3]] A. K. Ghosh, and A. Schwartzbard, "A Study in Using Neural Networks for Anomaly and Misuse Detection," in Proc. USENIX Security, 1999.

[4] W. Li, "Using genetic algorithm for network intrusion detection," in *Proc. of the United States Department of Energy Cyber Security Group*, pp. 1-8, 2004.

[5] W. Chimphlee, A. H. Abdullah, M. N. M. Sap, S. Srinoy, and S. Chimphlee, "Anomaly-based intrusion detection using fuzzy rough clustering," in *Proc. ICHIT'06*, pp. 329-334, IEEE, 2006.

[6] Y. Liao, and V. R. Vemuri, "Use of k-nearest neighbor classifier for intrusion detection,“ *Computers & Security*, 21.5, pp: 439-448, 2002.

[7] R. P. Lippmann, and R. K. Cunningham, "Improving intrusion detection performance using keyword selection and neural networks," *Computer Networks* 34, no. 4, pp. 597-603, 2000.

[8] J. E. Dickerson, and J. A. Dickerson, "Fuzzy network profiling for intrusion detection," in *Proc. NAFIPS'00*, pp. 301-306, IEEE, 2000.

[9] Norbik Bashah Idris and Bharanidlran Shanmugam, "Artificial Intelligence Techniques Applied To Intrusion Detection" in IEEE Indicon 2005 Conference, Chennai, India, 11 - 13 Dec. 2005.