ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

Using Artificial Neural Network Classification and Invention of Intrusion in Network Intrusion Detection System

Prof.Dighe Mohit S., Kharde Gayatri B., Mahadik Vrushali G., Gade Archana L., Bondre Namrata R.

Dept of Computer Engineering, Savitribai Pule Univercity at Shri chattrapati Shivaji Collage Of Engineering,

Shrishivajinagar, Rahuri, Ahmednagar, Maharashtra, India

ABSTRACT: Network security is become an issue of imperial importance in the information technology field. Now a days with the developement of communication and computer networks, immunity has become a decisive subject for computer network.

In this paper we have to detect attack and classify attack In a NIDS and categorized them, IDS is important for protecting computer system and network from Misuse.IDS is an one type of art of detecting unauthorized used of computer and any attempt to break network. Intrusion detection system is one type of tool that help to prevent unauthorized access to network resources by analyzing access to network traffic. Different algorithm and method and application are created and implemented to solve the problem of discovery of attack in IDS. The experiment and appraisal are experiment by using the set of benchmark data from Knowledge discovery in database. The result show that our implemented and propose system detect the attack and classify them In 10 groups with the approximately 94% accuracy with the two hidden layer of neurons in the neural network. Multilayer perceptron(MLP) and apriori algorithm used for IDS.MLP based improved intrusion detection system to detect and classify all kind of attack using back propagation algorithm.

KEYWORDS: Multilayer perceptron(MLP), Artificial Neural Network(ANN),Intrusion Detection System(IDS),Network Intrusion Detection System(NIDS),Knowledge Discovery in Databases(KDD).

I. INTRODUCTON

Last two decades network and computer protection has becomes and main problem because of increased number of attacker and hackers. therefore system were need to design to detect or/and prevent or visible attacker. attack on the computer or host are major deep problem. Nowadays , therefore several information and data security technique are available today to protect information system against misuse ,duplication ,diversion, damage and viruses attack[1]. information or data security is one of the important part of information society. In this paper the system that is NIDS based on ANN not only detect system is normal or under the attack but it also classify attack into different categories[2]. for these back propagation algorithm is used ,back propagation contain two hidden layer.it not only divide the data in normal or attack but also it classify attack.

Motivation

Attacks on the computer infrastructures are becoming an increasingly serious problem nowadays, therefore several information security techniques are available today to protect information systems against unauthorized use, duplication, alteration, destruction and viruses attacks.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

II. RELATED WORK

The ability of soft computing techniques for dealing with uncertain and partially true data makes them attractive to be applied in intrusion detection. Some studies have used soft computing techniques other than ANNs in intrusion detection .This paper a designed network intrusion detection system based on the artificial neural networks using Multi Layer Perceptron(MLP)[1] and the testing results of the prototype system proved the validity of the method and the advantages over other methods suggested[3]. In many previous studies The ability of soft computing techniques for dealing with uncertain and partially true data makes them attractive to be applied in intrusion detection. Some studies have used soft computing techniques other than ANNs in intrusion detection[4].

III. PR0POSED WORK

ARTIFICIAL NEURAL NETWORK(ANN):

ANN is nothing but the Artificial Neural network.ANN contain many neurons that are linked to each other. The main goal of neural network is to transfer input into output. The result can be calculate by using characteristic of node and weight associated with interconnection among neurons.

INTRUSION DETECTION SYSTEM(IDS):

IDS is nothing but the intrusion detection system. Intrusion is nothing but the attack. IDS is one type of tool that used to detect attack .That means IDS is used to prevent system from unauthorized used.IDS can be classify into two categories. The goal of IDS is to identify entities attempting security control.

An IDS is term which quickly listen to network traffic in order to invention baroque activity.IDS can be classify into following categories

Intrusion Detection Classification:

Intrusion Detection can be divided into two type

.Misuse intrusion detection

.Anomaly intrusion detection

1) Misuse intrusion detection:

Misuse Intrusion Detection System Is Also Called As Signature Based Ids. This Is One Type Of Ids ,It Contain A Database Of Know Exposed .It Observed Traffic And Attempt A Type Or Autograph Match. It Behave Same As, Like Worm, Scanner, By Penetrative For A Known Identity Or Autograph For Each Specific Attack Event. It Can Be Locate On The Network To Perception. The Network Exposed Can Be Locate On A Network.

Autograph Based Ids Observed System Activity And It Gives Alarm Only When Called Match Is Found.

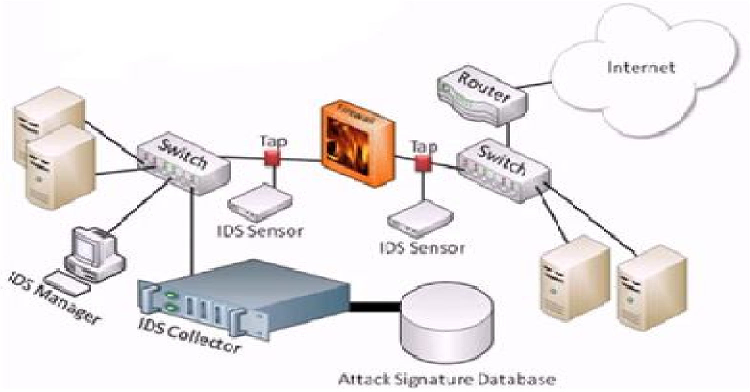

FIG1:Misuse intrusion detection

2) Anomaly intrusion detection:

Anomaly intrusion detection system are also called as behavior based system . Anomaly intrusion detection uses the normal behaviour pattern for identify the intrusion.the user behavior is observed and any deviation from the constructed normal behavior is detected as a attack.

Anomaly intrusion detection method is that they can be very effective in detecting previously unknown threats.

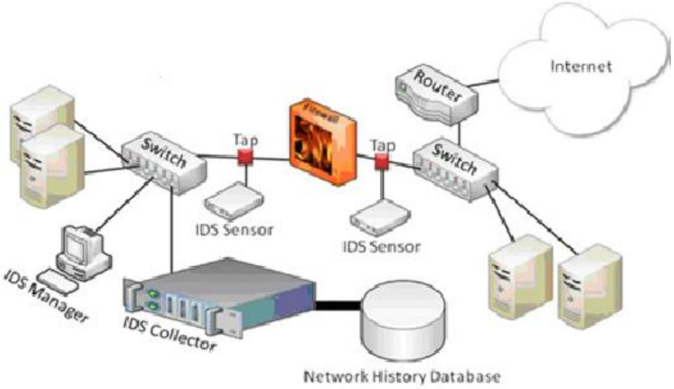

Fig.2 Anomaly Intrusion Detection System

Network Attacks

The main intent of IDS is to invention attack and classify attack in following categories.

1. Denial of Service (DOS) Attacks:

Denial of Service (DOS) Attacks is one type of attack categories .In this class of attack ,attacker makes some computing or resource of memory to engaged or to full to handled appropriate ping or ignored appropriate user access to a machine. Intruder try to prevent appropriate user from using a service

2. User to Root Attacks (U2R)Attack:

User to Root Attacks is one type of attack class .In this class of attack intruder start out with access to normal user account on the system and is able to feat exposed to attain root access to the system .

3.Remote to Local Attacks (R2L)

A remote to local attack is a one type of attacks. In this class of attack intruder pass the packets to a machine over the network. but who does not have an account on that machine. This means that an intruder can not have local account on the victim host and tries to produced it then feat some exposed to attain unauthorized local access as a user of that machine.

4. Probing (Probe)attack:

Probing (Probe)attack is also another type of attack class. In this category of attack in which an intruder scan a n/w of computer to information or find known exposed. An attacker try to get information about goal host, using operating system.

IV.ALGORITHM

Back propagation Learning Algorithm

step 1: Normalize the inputs and outputs with respect to their maximum values. it is proved that the neural networks work better if input and outputs lie between 0-1 for each training pair, assume there are 'l' given by $\{I\}_1$ (l*1) and 'n' outputs $\{O\}_o$ (n*1) in a normalized form.

step 2: Assume the number of neurons in the hidden layer to lie between 1<m<2l.

step 3: [V] Represents the weights of synapses connecting input neurons and hidden neurons and hidden neurons and [w] represents weights of synapses connecting hidden neurons and output neurons. Initialize the weights to small random values usually from -1 to 1. for general problems, λ can be assumed as 1 and the threshold values can be taken as zero.

$[V]^o$ ={random weights}
$[W]^o$ = {random, weights}
$[\Delta V]^o = [\Delta W]^o = [o]$
step 4: for the training data, present one set of inputs and outputs, Present the pattern to the input layer {I}, as inputs to the input layer may be evaluated as

$\{O\}_r = \{I\}_I$ for (l*1)

step 5: Compute the inputs to the hidden layer by multiplying corresponding weights of synapses as
$\{I\}_H = \{V\}^T\{O\}_I$ where I and V sets are m*1 and and o is l*1
step 6 : Let the hidden layer units evaluate the output using the sigmoidal function as

$\{O\}_H = \{- - -1/(1+e^{(-I_{Hi})})- - -\}$

step 7 : Compute the inputs to the output layer by multiplying corresponding weights of synapses as

$\{I\}_o = \{w\}^T\{O\}_H$ where i is set of n*1,w is set of n*m matrix and O is set of m*1 matrix

step 8 : Let the output layer units evaluate the output using sigmoidal function as

$\{O\}_O = \{- - - ((1/ (1+e^{(-I_{Oj})})\}$

the above is the network output.
step 9 : Calculate the error and the difference between the network output and the desired output as for the ith training set as

$$E^P = \sqrt{\sum((Tj - Ooj)2)}/n$$

step 10 : Find {d} as

$\{d\} = \{(T_K-O_{ok})O_{ok}(1-O_{ok})\}$ of matrix n*1

step 11 : Find {Y} matrix as

$[Y] = \{O\}_H<d>$ where Y is matrix of m*n, o is matrix of m*1, d is matrix of 1*n

step 12 : Find $[\Delta W]t+1 = \alpha[\Delta w]t + \eta[Y]$ where each matrix is of m*n
step 13 : Find {e} = [w] {d} where e is matrix of m*1, w is matrix of m*n, and d is matrix of n*1.

$\{d^*\} = \{ei(O_{Hi})(1-O_{Hi})\}$ where d is matrix of m*1

step 14: for finding X matrix as

$[x] = \{O\}_r<d^*> = \{I\}_I<d^*>$ where x = matrix of 1*m, O,I = single value, d =matrix of 1*m

step 15: Find $[\Delta V]^{t+1} = \alpha[\Delta V]^t + \eta[X]$ all matrix of 1*m
step 16: To Find the updated weights and threshold[Θ]

$[V]^{t+1} = [V]t + [\Delta V]^{t+1}$
$[W]^{t+1} = [W]t + [\Delta W]^{t+1}$
$[\Theta]_o^{t+1} = [\Theta]_o^t + [\Delta\Theta]_o^{t+1}$
$[\Theta]_H^{t+1} = [\Theta]_H^t + [\Delta\Theta]_H^{t+1}$

step 17: Find error rate as

Error rate = $((\sum E_P)/nset)$

step 18 : Repeat steps 4-18 untill the convergences in the error rate is less than the tolerance value.

IV. SYSTEM ARCHITECTURE

The system Architecture contain three modules out of these three modules two modules used for intrusion detection with the help of ANN. This is based on back propagation algorithm. Out of these module the first module contain IDS with in Weka Tool. The second module contain back propagation algorithm and finally third module contain online detection if ICMP ping attack. The system that contain the algorithm is divided into five modules. The accumulation of packet , packet processing, extraction of feature, classifier, Training module, KDD dataset, decision module .

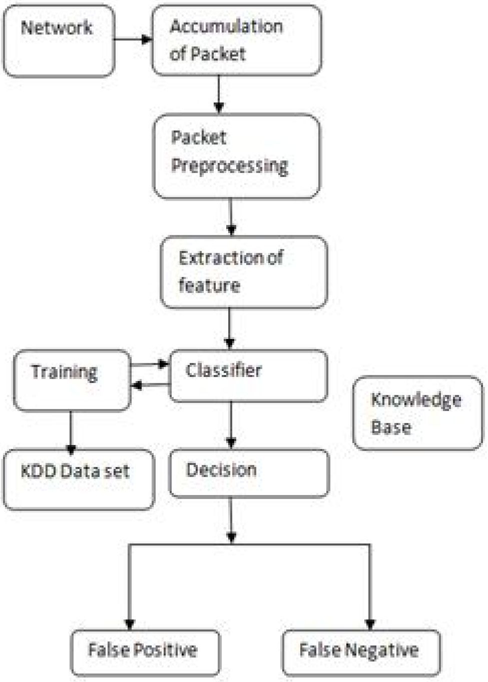

Fig.3 System Architecture

1.Accumulation of packets: Accumulation of packets is nothing but the collection of packet. This phase observe network stream and collect packets for the data source of NIDS. after accumulation of packets there will be preprocessing on packets.

2.Packet Preprocessing: Packet preprocessing means network stream is accumulated and process on these network stream and it is used as input to the system.

3.Extraction of feature: This phase extract feature from the network connection record and send this feature to the classifire phase.

4.Classifire: Classifire is one type of phase, of a system , the main working of this phase is to analyze the network traffic and also main responsibility is to draw a judgement whether attack happens or not.

5.Decision: After detection the instruction happens, this phase submit caution message to the user.

6.Knowledgebase: This phase used for the training. sample of classifire phase. The attack samples can be perfected under user complicity ,so the capacity of the detection can be increased.

DATASET:

Dataset is nothing but the accumulation of network related information or data that was collected under a period of time is called as dataset. The dataset NIDS is collect from UCI KDD archive. The network or computer related information downloaded from the archive UCI KDD. It contain 41 paradigm.

V. RESULT AND DISCUSSION

The output of execution of back propagation algorithm. it provide 94% efficiency of detection rate which is comparison greater. Also it provide the classification of attack in 10 categories .the existing method provide higher detection rate but all they are facing problem while classification of attack but our system is used to provide higher detection rate as well as classification rate with more accuracy

. VII. CONCLUSION

In this paper with the help of artificial neural network based intrusion detection system motivate to detect attack and classify them in various category. Existing system only suggest that where the system under the attack or normal but this paper suggest that it detect attack and also classify them.

The classification result were slightly better in the three layer network. From practical point of view. The experimental result is suggest that there is more to do in the IDS based on ANN. The cause of an intrusion detection system is to invention a potential intruder as possible as. An approach for a neural network based intrusion detection system motivated to classify the normal and attack patterns and the pattern of the attack.

ACKNOWLEDGEMENTS

We would like to express our special thanks of gratitude to our project guide Prof.Dighe M.S. as well as our project coordinator Prof. Dighe M.S who gave us the golden opportunity to do this wonderful project on the topic ,which also helped us in doing a lot of research and we came to know about so many things.We can’t say thanks using artificial neural network classification and invention of intrusion in network intrusion detection system you enough for their tremendous support and help. Without their encouragement and guidance this project would not have materialized.

We would also like to express deepest appreciation towards Dr.Nagraj T.K , Principal of Shri Chhatrapati Shivaji College of Engineering. At last we must express our sincere heartfelt gratitude to all friends and sta? members of Computer Engineering Department who helped us directly or indirectly during this course of work.
We are making this paper not only for marks but to also increase our knowledge.

Miss:Kharde Gayatri B., Misss: Mahadik Vrushali G., Miss:Gade Aarchana L.,Miss:Bondre Namrata R.

REFERENCES

1. Reza Norouzian,sobhan Merati. “Classifiying Attack in a Network Instrusion Detection system Based on Artificial Neural Networks”
2. ” Devikrishna K S*, Ramakrishna B B**“An Artificial Neural Network based Intrusion Detection System and Classification of Attacks”
3. Norouzian M.R., Merati. S., Classifying Attacks in a Network Intrusion Detection System Based on Articial Neural Networks Proceedings of the Advanced Communication Technology (ICACT), 2011 13th International Conference on Publication Year: 2011 , Page(s): 868 873.
4. Srinivas Mukkamala,"Instusion Detection Using Neural Network and Support vector machine,"Proceedings of the 2002 JEEE International Honolulu, HI, 2002.
5. Mukherjee, B., Heberlein, L.T., Levitt, K.N, "Network Intrusion Detection".IEEE Network. pp. 28-42, 1994.
6. Kabiri P, Ghorbani A,"A. Research in intrusion detection and response - a survey". International Journal of Network Security,2005
7. J. Ryan, M. Lin, and R. Miikkulainen,"Instrusion Detection With Neural Network",AI Approaches to Fraud Detection And Risk Management Papers from the 1997 AAAI Workshop, Providence, RI, pp. 72-79, 1997

BIOGRAPHY

Prof:Dighe Mohit S. Assistant professor in the computer department of Shri chattrapati Shivaji Collage Of Engineering,Shrishivajinagar, **Miss:Kharde Gayatri B., Misss: Mahadik Vrushali G., Miss:Gade Aarchana L.,Miss:Bondre Namrata R.,**student of computer dept(B.E.) of Shri chattrapati Shivaji Collage Of Engineering,Shrishivajinagar,Tal:Rahuri,Dist:Ahemednagar ,State:Maharastra,India

Prof.Dighe Mohit S.(Guide), Assistance Professor Bachelors and Master's Degree in the field of Computer science and Engineering. Shri Chhatrapati Shivaji College Of Engineering under Savitribai Phule Pune University, Shrishivajinagar,RahuryFactory,India, Area of Interest:Networking,

Kharde Gayatri B., Bachelor of Engineering, Student,Department Of Computer Engineering, Shri Chhatrapati Shivaji College Of Engineering under Savitribai Phule Pune University, Shrishivajinagar,RahuryFactory,India, Area of Interest:Networking,

Mahadik Vrushali G., Bachelor of Engineering, Student,Department Of Computer Engineering, Shri Chhatrapati Shivaji College Of Engineering under Savitribai Phule Pune University, Shrishivajinagar,RahuryFactory,India Area of Interest: Networking,

Gade Archana L., Bachelor of Engineering, Student,Department Of Computer Engineering, Shri Chhatrapati Shivaji College Of Engineering under Savitribai Phule Pune University, Shrishivajinagar,RahuryFactory,India, Area of Interest: Networking,

Bondre Namrata R., Bachelor of Engineering, Student,Department Of Computer Engineering, Shri Chhatrapati Shivaji College Of Engineering under Savitribai Phule Pune University, Shrishivajinagar,RahuryFactory,India Area of Interest:Networking,