International Journal of Future Innovative Science and Engineering Research
Volume-1, Issue-I ISSN (Online): 2454- 1966

Research Manuscript Title

A HYBRID APPROACH FOR ANALYZING AND DISCOVERING SERVICE ATTACK IN NETWORK

Website: www.istpublications.com

S.Muthamil Selvi[1], B.Kiranbala,[2]
Assistant professor
M.E-computer science and engineering
K.Ramakrishnan College of Engineering

E-Mail: muthamilpriya11@gmail.com, kiranit2010@gmail.com

MARCH - 2015

A HYBRID APPROACH FOR ANALYZING AND DISCOVERING SERVICE ATTACK IN NETWORK

S.Muthamil selvi[1], MrsB.Kiranbala ME MBA[2]
Assistant professor
M.E-computer science and engineering
K.Ramakrishnan College of Engineering
E-Mail: muthamilpriya11@gmail.com, kiranit2010@gmail.com

Abstract

The security plays important role in neural networks due to the population of internet and the communication. One of the ways to find the attacker or illegal user's from the network means analyze their packets. The number of methods, techniques, and the algorithms are used to find and detect the attack present in the intrusion detection system. Most methods are used to find the attacks in the system and then they are categorized into two such as the normal and threat. to propose the efficient approach of intruder detection system in the artificial neural network. to implement the MLP (Multilayer Perceptron) in intruder detection system. The experimental results shows our proposed system categorize the attacks in six groups based upon four categories such as the DOS, U2R, R2L and probing attacks. Our concept provides the 90.78% accuracy with the two hidden layers of neurons in the neural network.

Key-words Attackers, triangle area, KDD cup

1.Introduction:

Nemours advances have been made in developing intelligent storage systems are some inspired by neural networks systems.. scientists from many scientific ideas are designing artificial neural networks to solve a variety of problems in identification patterns recognition, prediction, optimization, associative memory, and control (the"Challenging problems" slides in process). Conventional approaches have been proposed for solving these defects and causes. Although conventional applications features can be found in certain well-constrained environments, none is scalable enough to perform well outside its domain. Areas ANNs provide exciting alternatives, and features applications are could benefit from using them. perform well domain areas features. ANNs provide exciting alternatives, and applications many could benefit from using them .Artificial Neural Networks are relatively crude electronic methods based on the neural structure of the brain area. The brain basically learns from experience scientific value. It is actual proof that some problems that are beyond the scope of current computers are indeed solvable by small gain energy efficient packets This brain modeling also promises a high synthetic technical way to develop machine and human solutions. This new approach to computing also provides a more degradation graceful during system overload than its more traditional counter parts. These biologically inspired methods of computing are thought to be the next major advancement in the computing industry approaches. Even simple animal brains are capable of functions that are currently impossible for computers. Computers do role well thimgs, like keeping scientific ledgers or performing complex mathmatical values But computers have trouble recognizing even simple patterns much less generalizing those patterns of the past into actions of the future.Now, advances in biological research values promise an initial understanding of the natural thinking mechanism. This research shows that brains information store as patterns. Some of these informations are very complicated to identifying values and allow us the ability to recognize individual faces from many different angles and features. This process of storing information as patterns, utilizing those patterns, and then solving problems encompasses a new field in computing.

This field, as mentioned before, does not utilize programming tradional but involves the creation of massively parallel networks and the training of those networks to solve specific problems. This field also utilizes words very different from traditional computing resources, words like behave, react, self-special value organize , learn, generalize, and forget. The most popular class of multilayer connecting with many layers approaches feed-forward networks is multilayer perceptions in which each computational unit employs either the thresholding function or the sigmoid function and generated.

2.Existing methods:

In existing system the more number of methods and techniques are discussed for detect the attacks in intruder detection system. One of the methods is that the rule based analysis. Rule based analysis sets of rules features are defined that are provided by an administrator or created by the source detections. Expert systems are the most common form of rule-based intrusion detection approaches. The use of system expert techniques in unauthorized user acess in detection mechanisms was a significant milestone in the development of effective and practical detection-based information security systems. An expert system consists of a set of ideas that encode the knowledge of a human "expert". These rules are used by the system to make conclusions about the security-related data from the intrusion detection system. The problem may arise that the intruder or hacker is an intelligent and flexible agent while the rule-based IDSs obey fixed rules. In fact systems expert suffer from the updating trends, the searching and the matching of the rule sets fortunately, systems experts require frequent updates to current. Remains values,

This design approach usually results in an inflexible detection system is unable to detect an attack if the sequence of events is even slightly different from the profile. defined While increasing the level of abstraction of the rule-base does provide a partial solution to this weakness, it also reduces the granularity of the intrusion detection device. Generally network based detection systems can be classified in to two main categories namely misuse based detection system and anomaly based detection system detect attackers by monitoring network activities and looking for matches with existing signatures .namely based anomaly detection. owing to the principle of detection which monitors and flags any network activities presenting significant deviation from legitimate traffic profiles objects, anomaly based detection techniques show more promising in detecting zero day intrusions that exploit previous unknown system vulnerabilities. this approach also successfully avoids the above problems, but it works with network packet payload's furthermore it is complicated and labor intensive task to keep signature database updated because signature generation is a manual process and heavily involves network security expertise. it is vulnerable attack that linearly changed all monitored features un addition this approach can only label to entire group of observed samples to legitimate or attack traffic but not indivuals in the group. Traffic classification techniques such as dynamic port numbers and user privacy protection. may rely on the port numbers specified by different applications or the signature strings in the payload of IP packets..Modern techniques normally utilize host/network behavior analysis or flow level statistical features by taking emerging and encrypted applications into account. In the state-of the-art traffic classification methods, Internet traffic is characterized by a set flow statistical properties and machine learning techniques are applied to automatically search for the structural patterns .It found that the main reason for the underperformance of number of traditional classifiers including NB is the lack of the feature discretization process.. A big challenge for current network management is to handle a large number of emerging applications, where it is almost possible to collect sufficient training samples in a limited time..to only manually label very few samples as supervised training data since traffic labeling is time-consuming.The unsupervised classification traffic methods analyze the super data, training data and produce an inferred function which can predict the output class for any testing flow..In supervised traffic ideas to, sufficient supervised training data is a general assumption.To address the problems suffered by payload-based traffic classification. the correlation between features attributes are intrinsically replaced neglected or the manages or the techniques do not manage to fully exploit these correlations. to support using the scalar vector machine. The timely and accurate detection of computer and network system intrusions has always been an elusive goal for system administrators and informationss security scientist.While the complexities of computers in host location already made intrusion detection a endeavor difficult, the prevalence increasing of distributed network-based systems and insecure networks such as the Internet has greatly increased the need for intrusion detection, The neural network gains the experience initially by training the system to correctly preselected to idendify. examples of the problem. The response of the neural network is reviewed and the configuration of the system is refined until the neural network's analysis of the training data reaches a satisfied. In addition to the initial period trainining, the neural network also gains experience over time as it conducts analyses on data related to the problem. A limited amount of research has been conducted on the application of neural networks to detecting intrusions defects. Artificial neural networks offer the potential to resolve a number of the problems encountered by the other current approaches to intrusion Statistical Analysis involves statistical comparison of current events to a predetermined set of criteria baseline. The technique is most often employed in the detection of deviations from typical behavior and determination of the similarly of events to those which are indicative of an attack .Neural networks were specifically proposed to identify the typical characteristics of system users and identify statistically significant variations from the user's established behavior.dtection. Artificial neural networks have been proposed as alternatives to the statistical analysis component of anomaly detection systems.

3. Proposed architecture

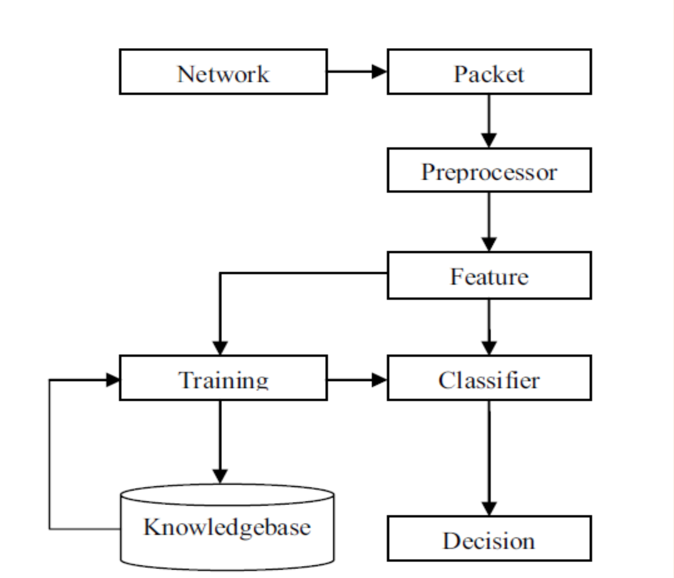


Fig 1.proposed structure

To overcome the problems presented in an existing concept in our proposed system we implement the one efficient method in an intruder detection system such as the MLP (Multi Layered Perceptron).. In our proposed work we use the KDD cup data set as the input data set for detect the attack present in the network.. There are two different learning methods are used. They are supervised and unsupervised. In supervised learning technique we use the MLP for pattern recognition problem. and in unsupervised learning anomaly detection to use the SOM (Self Organizing Mapping) for find a topological mapping from the input space to clusters. to first of all connect with the main server.. The two or more clients connect with the main server. Through the network .to detect if any attack are present in the network and also we trace the location of the network. And also we compare the training and test datasets to find the number of attacks with the help of the back propagation algorithm.

To trace the location of lan.shutdown the client system with the help of the server. This means we are controlling the system with the help of server..MCA-based detection mechanism\ evaluates the performance of our proposed detection system usimg KDD cup 99 data sets. Show the systematic analysis on the computational complexityand the time cost of the proposed system.

4. Framework:

The whole detection process consists of three maampljor steps .the sample-by-sample detection mechanism.connectionestablishment,loaddataset,classification of attacks,scanning processssystem control

In step 1. In this module we establish the connection between the server and client. For made the connection establishment process first run the server program after specify the client port number.. In our concept to made the establishment between the one server and more than one client at a time. After specifying the port number the connection will be successfully established.. After establishment the established message is shown server machine.

Step 2 To use the KDD cup99 data set as the input dataset. For identification of attack in the network we first load the data set into the system. Our system contains both the normal and attack information's. From that data set we find out or classify the attacks into 6 groups based upon the 4 different categories.

Step 3 After loading the data set into the system next stage is to the classification. In this stage we classify the attack into six different groups based upon the four different categories. The categories are,DOS (Denial Of Service),U2R,R2L and Probe attack.. These attacks are classified from the whole data set. To detect the normal and threat data's are separated from the list. Each of which can be handled in separate and efficient manner.. And also we list out the amount of attack and normal data details.

Step 4 In this stage we apply the real time implementation. Here we first scan the client system with the help of different scanners. Such as the port scanner, traceroute tool, Host locator tool and ping tool. For LAN scanning we use the ping tool. In our project we can saw what are the process are running in client system.. It's just look like a task manager. With the help of the SOM we trace the location of the LAN The back propagation algorithm is used to compare the train and test data sets and find out the attacks.. The loaded dataset is first classified after that detect the attack.

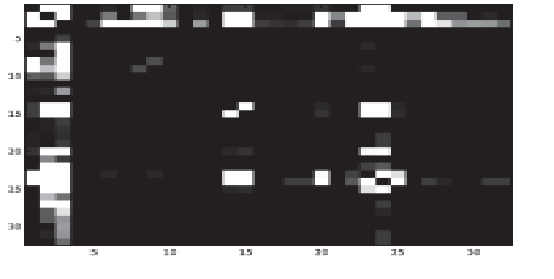
Step 5 This is our final stage. In this stage we are going to control the client system with the server.. In client the running process are listed out.. If the list contain any attack means for example Wscript. We can end the process using endprocess option.. And also another one thing is that we can shutdown the client system in our concept.

5 Detection of attack

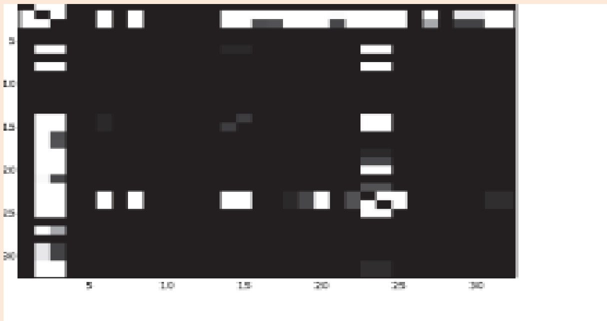
To detect attacks the lower triangle the TAM of an observed record are generated using(TAB) Triangle area based approaches and normal profile generation is generated.

6 Dection system based on (MCA)and evaluation:

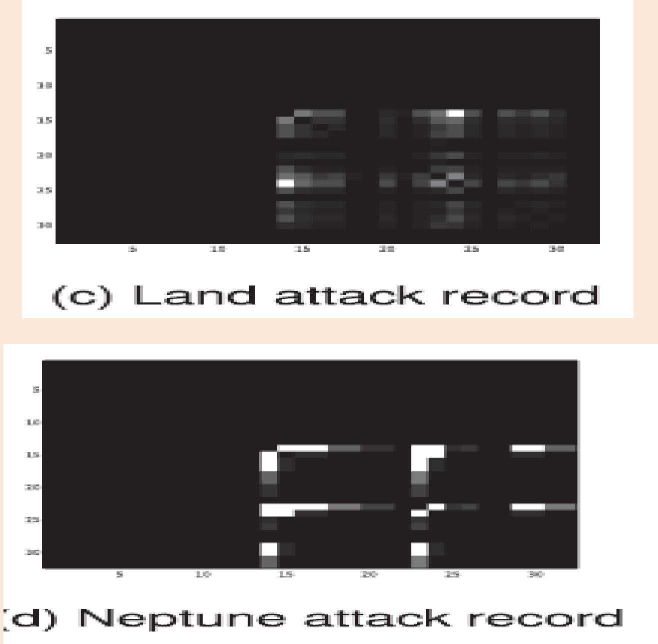
Despite the data set is criticized for reduant records that preventing algorithms.from learning infrequent harmful records.the additionally detection system innately withstands the negatively impact introduced by the data set.Triangle-area based on MCA approach assessed for its capability of network traffic characterization



(a) Normal TCP record



(b) Back attack record



(c) Land attack record

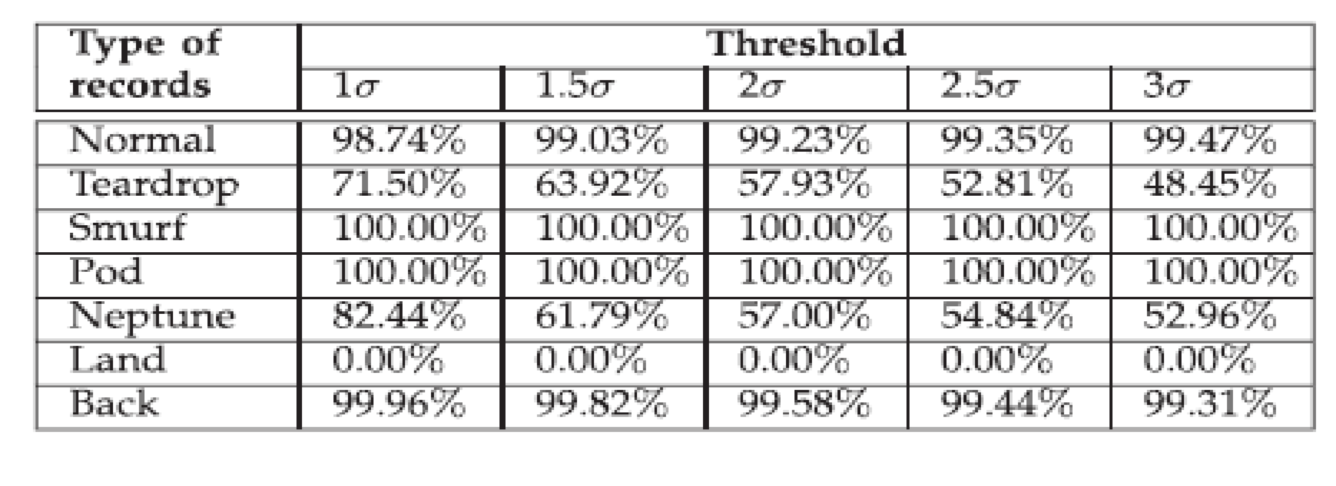
(d) Neptune attack record

Fig 2 Images of TAMS of normal TCP traffic, Back ,Land and Neptune attacks generated using original data

During the evaluation the 10 percent labeled data of KDD cup 99 data set is used, three types of legitimate traffic controls.(TCP,UDP,and ICMP Traffic)and six different types of dos attack are available such that(Teardrop,smuri,pod,neptune,land and back attacks) Triangle-area based on MCA approach assessed for its capability of network traffic characterization another technique can be used. tenfold cross validation is conducted to evaluate the accuracy detection and performance. It can be works on transport layer some metrics are based such that true-negative rate detection, false positive rate detection and accuracy used to evaluate the proposed MCA based detection system. is required to achieve a high good performance and accurate detection. it has been widely used in the domain of intrusion detection research.

TABLE 1

Average Detection Performance of the Proposed System on Original Data against Different Thresholds



Type of records	Threshold				
	1σ	1.5σ	2σ	2.5σ	3σ
Normal	98.74%	99.03%	99.23%	99.35%	99.47%
Teardrop	71.50%	63.92%	57.93%	52.81%	48.45%
Smurf	100.00%	100.00%	100.00%	100.00%	100.00%
Pod	100.00%	100.00%	100.00%	100.00%	100.00%
Neptune	82.44%	61.79%	57.00%	54.84%	52.96%
Land	0.00%	0.00%	0.00%	0.00%	0.00%
Back	99.96%	99.82%	99.58%	99.44%	99.31%

The different types of traffic records are generated using 32 continuous features. The images for the TAM'S of normal TCP record ,back attack record,land attack record,and Neptune record are presented. The brighttness of an element ia an image represents its value in the corresponding TAM. The images also demonstrate that our proposed MCA approach fulfills the antipaction of generation features.

6. Conclusion

The security is a most important thing in intrusion detection systems are used to detecting the attacks.. In we use the two different learning schemes in the neural network. First one is that the supervised learning and another one that the unsupervised learning. In supervised learning we use the MLP algorithm to find out the attacks and in unsupervised learning method. To use the SOM to trace the locations. For detection purpose we use the KDD cup99 data sets. In our proposed work we classify the attacks six different groups based upon the four different categories. The attacks are the DOS, U2R, R2L, and Probe. Evaluation has been conducted using KDD CUP 99data set to verify the effectiveness and performance of the proposed DOS attack detection system. The problem however can be solved by utiliziningl normalization stastical. Technique to eliminate the bias from the datasource. the results of evaluating with the data normalize items

Encouraging detection accuracy of 99,95 percent and nearly 100.00 percent DRs for the various detection DOS attacks. Besides the comparison results has proven that our detection system. The proposed system achieves equal or better performance in comparisons with two state-of-the—art approaches. To be part of the work future to will further test the DOS attack detection system using real- world data and employ more sophisticated classification techniques.

References

[1] K. Lee, J. Kim, K.H. Kwon, Y. Han, and S. Kim, "DDoS Attack Detection Method Using Cluster Analysis," Expert Systems with Applications, vol. 34, no. 3, pp. 1659-1665, 2008

[2] J. Yu, H. Lee, M.-S. Kim, and D. Park, "Traffic Flooding Attack Detection with SNMP MIB Using SVM," Computer Comm., vol. 31, no. 17, pp. 4212-4219, 2008.

[3]S. Jin, D.S. Yeung, and X. Wang, "Network Intrusion Detection in Covariance Feature Space," Pattern Recognition, vol. 40, pp. 2185- 2197, 2007

[4]P. Garca-Teodoro, J. Daz-Verdejo, G. Maci-Fernndez, and E.Vzquez, "Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges," Computers and Security, vol. 28, pp. 18-28, 2009

[5] S. Jin, D.S. Yeung, and X. Wang, "Network Intrusion Detection in Covariance Feature Space," Pattern Recognition, vol. 40, pp. 2185-2197, 2007.

[6] C.F. Tsai and C.Y. Lin, "A Triangle Area Based Nearest Neighbors Approach to Intrusion Detection," Pattern Recognition, vol. 43, pp. 222-229, 2010.