An Efficient Network Intrusion Detection System using Multilayer Perceptron

R. Roshini[1] L. Sankara Maheswari[2]
[1]Student [2]Assistant Professor
[1]Department of Computer Science [2]Department of Information Technology
[1,2]Sri GVG Visalakshi College for Women

Abstract— Presently, the growth of internet has given rise to increasingly utilize internet for public and commercial services. As a result malicious activities are on the rise to exploit users to steal information related to credit card details, passwords, sensitive information etc. It has become a major concern in the society to protect data shared across networks and stored in computer. At the same time attackers use many techniques to gain advantage of breaking firewalls and security measures. The attacker use techniques to steal the data such as malware, viruses, Trojans etc. An intrusion detection system is used to detect and block malicious traffic originating from attackers. Traditional Intrusion detection systems are becoming less effective to capture the malicious traffic. Combining data mining techniques into intrusion detection system offer more security than traditional methods. Since data mining can use vast number of data, detecting a tiny variation in the network traffic is possible leading to detect and block unwanted traffic in the network. In the present study multi layer perceptron classifier is used to classify the network attack types. MLP based intrusion detection system is designed to support network administrators to find signature based attacks and anomaly of the network traffic. The IDS is trained on the traffic data using MLP to capture the known attack types and differentiate traffic as intrusion and normal traffic.

Key words: MLP, IDS, Malicious Traffic

I. Introduction

In recent years, with the tremendous growth in networked computer resources, a variety of network-based applications have been developed to provide services in different areas such as ecommerce services, social media services, banking services, government services, etc. The increase within the variety of networked machines has result in a rise in unauthorized activity, not solely from external attacks, however conjointly from internal attacks, like folks gaining unprivileged access for personal gain. Intrusion detection system (IDS) detects unauthorized intrusions into computer systems and networks. Incidents may be malware attacks (such as worms, virus), attackers gaining unauthorized access to system through Internet or user of the system gaining unprivileged root access of the system for which they are not authorized.

An IDS monitors network traffic of an information processing system sort of a network human and collects network log data. The collected network knowledge is analyzed by intrusion detection model or technique for rule violations. Intrusions are the activities that violate the safety norms of the system.

An Intrusion Detection system is a mechanism used to identify, monitor network or system actions for malicious activities and produces reports to a management departments. The development of IDS is for two reasons i) Most existing systems have security was that render them susceptible to intrusions, and finding and fixing all these deficiencies are not feasible. ii) Prevention techniques cannot be sufficient. It is virtually not possible to possess associate degree fully secure system. Even the foremost secure systems are liable to business executive attacks. New intrusions frequently emerge and new techniques are required to defend against them.

A. Intrusion Detection System:

It is an automated system that screens system activities for malicious activities or any abnormal activity which is against the policy and produces reports to an administration station. There are 2 IDS systems; one within the network and also the different outside. The IDS devise continuously check the systems in the network and monitor servers and send the report of any abnormal activity to the network administration.

B. Network Based:

Network Intrusion Detection Systems are placed at a vital point or indicates inside of the network monitor activity to and from all gadgets on the network. It performs Associate in Nursing examination of passing movement on the entire subnet, and matches the activity that's gone on the subnets to the library of famous attacks.

C. Host Based:

Host based mostly Intrusion detection system keeps running on individual hosts or gadgets on the network. In the event that the fundamental system files were adjusted or erased, An alert is shipped to the pinnacle to research.

D. Data Mining:

Data Mining refers to the method of extracting effective, updated, latent, useful, and therefore the comprehensible pattern from an outsized incomplete, noise, non-stable and random information. In intrusion detection system, the data deals from multiple sources like network traffic or logs, system logs, application logs, alarm messages, etc. Due to varied information supply and format, the complexity increased in auditing and analysis of data. Data Mining has large advantage in information extraction from giant volumes of knowledge that square measure screaming and dynamic, thus it is of great importance in intrusion detection system.

Data mining based IDS can efficiently identify these data of user interest and also predicts the results that can be utilized in the future. Data mining or data discovery in databases has gained a good deal of attention in IT trade yet as within the society. Data mining has been concerned to investigate the helpful data from giant volumes of knowledge that square measure screaming, fuzzy and dynamic.

II. LITERATURE SURVEY

(Belouch, 2017) carried out studying machine learning methods on intrusion detection system and proposed an ensemble method to improve its performance. The study involved ensemble methods to minimize the false rate using boosting, bagging and stacking learning methods. Using decision tree, Naive Bayes, neural network and REPTree the ensemble involving boosting, bagging and stacking accuracies were compared and the study concluded that the ensemble method produced higher accuracy in detecting intrusions with low false alarm rate. An accuracy of 87.92% is achieved using ANN and stacking.

(Idhammad, Afdel, &amp; Belouch, 2018) presented semi-supervised method using entropy estimation, co-clustering, information gain ratio and extra tree algorithms for detecting DDos and target to reduce the false alarm rate and improve classification. These machine learning algorithms on the traffic data is trained on three data sets. The proposed machine learning algorithm produced 98.33% accuracy and FP rate of 0.33% on NSL-KDD dataset, 99.88% and 0.35% on UNB ISCX 12 and 93.71% and 0.46% on UNSW-NB15.

(Azab, Alazab, &amp; Aiash, 2016) investigated on predicting newer bots that are yet to demonstrate an attack. The study involved capturing deep network flow features using CONIFA framework targeting harmful traffic. Using machine learning method, the study distinguishes the C&amp;C flows and classification algorithms are trained on these abnormal flows using statistical features. The network flow data was collected for Zeus botnet and three data sets were extracted and using CFS filtered the features with statistical significance and the classifier is trained on C4.5 algorithm with 10 fold cross validation. The framework efficiently detected Zeus botnet and non-Zeus botnet using network flow characteristics using different combinations of features and using cost sensitive analysis.

(Terzi et al, 2017) retrospected intrusion detection on network anomaly attacks and proposed a new technique for Bigdata using unsupervised machine learning techniques. The proposed method uses PCA for dimensionality reduction of netflow features and using kmeans algorithm, the features are clustered using the Euclidian distance measure. The proposed approach achieved 96% of accuracy and able to detect malicious traffic flows, outliers, and infected IP.

(Li et al 2015) proposed a mechanism to detect botnet using PSO and Kmeans clustering using real world network behaviour data. The proposed study targets the abnormal behaviour on each client machine for its network behaviour with respect to scanning behaviour, communication behaviour and connection failure behaviour. The experimental study shows a high detection rate and low false alarm rate. The study also finds that the change in the network flow properties does not affect the botnet behaviour in the network.

III. PROBLEM STATEMENT

In the past, rule based analysis relies on sets of predefined rules that are provided by an administrator. Rule based systems cannot adapt with the evolving nature of attacks resulting in an inflexible detection system. Attacks are continuously increasing and evolving. Detection methods should have the same nature to be able to detect new attacks. Data mining techniques have the ability to deal with evolving and changing attacks. IDS is a way to distinguish malicious and benign intrusions and it is done by monitoring a network for such behaviors. This technique detects attacks after they have already entered the network and caused damage.

The goal of Intrusion Detection Systems (IDS) is to detect an intrusion as it happens and be able to respond to it in a timely manner. A false positive is a situation where something abnormal happens, but it is not an intrusion. Too many false positives affects the quality of genuine traffic and a false negative is a situation where an intrusion is really happening, but IDS doesn't detect it. To detect the intrusion effectively, the IDS should be capable of producing low false positive rate and to detect normal traffic as normal. The problem becomes evident to develop a data mining model that can detect intrusions effectively with low false negative and false positives and the accuracy of the detection intrusions can be improved.

IV. METHODOLOGY

Traditional Intrusion detection systems are becoming less effective to capture the malicious traffic. Combining data mining techniques into intrusion detection system offer more security than traditional methods. Since data mining can use vast number of data, detecting a tiny variation in the network traffic is possible leading to detect and block unwanted traffic in the network. In the present study multi layer perceptron classifier is used to classify the network attack types. MLP based intrusion detection system is designed to support network administrators to find signature based attacks and anomaly of the network traffic. The IDS is trained on the traffic data using MLP to capture the known attack types and differentiate traffic as intrusion and normal traffic.

Multilayer perceptron neural network (MLPNN) is that the commonest and standard sort of neural networks in use these days. MLPNN represents a generic function approximator and classifier. It’s capable to approximate generic classes of functions, including continuous and discrete functions.

Also it will distinguish information that don't seem to be linearly divisible. MLPNN could be a feed forward network with one or additional layers (hidden layers) of units (hidden neurons) between the input and output layers. The neurons of the previous layer square measure perpetually connected with those of subsequent one whereas the neurons within the same layer don't seem to be interconnected.

The number of hidden layers and hidden neurons are generated randomly. Many efforts are employed to look for the optimal parameters of this layout of neurons grouped in layers. The number of neurons in the input layer equals the dimension of observations while the number of neurons in the output layer is fixed a priori according to the purpose of the problem at hand. The input layer is reserved to present the features to the fist hidden layer of the perceptron model. Hidden layers propagate the knowledge from the inputs to the outputs (outputs of every hidden layer) on the network. The neurons of the output layer represent a hyper plane in the space of the input patterns.

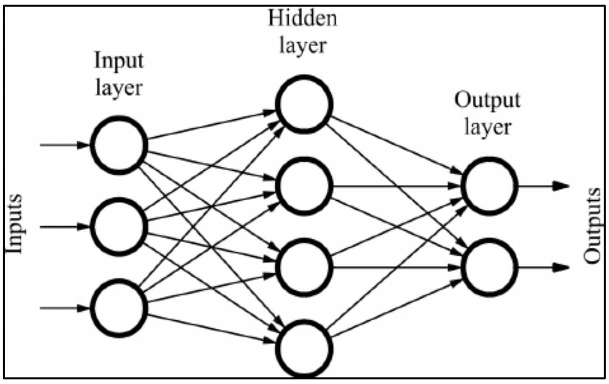


Fig. 4.1: MLP Architecture

A. Data Set:

The dataset used for the study which is generated by Cyber Range Lab from ACCS, they recently introduced the dataset for studying attacks and attack based behaviors in the network flow. The dataset has nine attacks types which are commonly labeled as attacks. The dataset has a total of 44 features and class labels as attack and normal. The training set contains about 17 thousand instances of traffic flow. For this study only 1500 instances and two classes, attack and normal are used. The features include Source IP address, Source port number, Destination IP address, Destination port number, Transaction protocol, Record total duration, Source to destination transaction bytes, Destination to source transaction bytes, Source to destination time to live value, Destination to source time to live value, Source packets retransmitted or dropped, Destination packets retransmitted or dropped, http, ftp, smtp, ssh, dns, ftp-data ,irc Source bits per second, Destination bits per second, Source to destination packet count, Destination to source packet count, Represents the pipelined depth into the connection, data transferred from the server's http service, Source jitter (mSec), Destination jitter (mSec), record start time, record last time, Source interpacket arrival time (mSec), Destination interpacket arrival time (mSec), TCP connection setup round-trip time, TCP connection setup time, TCP connection setup time, If source (1) and destination (3)IP address, No. for each state (6) according to specific range of value, No. of flows that has methods such as Get and Post in http service, If the ftp session is accessed by user and password then 1 else 0, No of flows that has a command in ftp session, No.of connections that contain the same service (14), No. of connections that contain the same service (14), No. of connections of the same destination address (3), No. of connections of the same source address (1), No of connections of the same source address (1), No of connections of the same destination address (3) and the source, No of connections of the same source (1) and the destination (3) and the name of each attack category, 0 for normal and 1 for attack records.

B. Evaluation Metrics:

The performance of any classifier is measured through confusion matrix. Using confusion matrix the classification results are visualized. It contains row and columns where each row represents the actual class and each column represent predicted class. From the confusion matrix different metrics such as sensitivity, specificity, and accuracy are calculated. In classification, the classification results between predicted and actual instances are tabulated. The classification matrix contains positive and negative conditions where positives are interpreted as classifier's ability and negative conditions are classifiers errors. The errors are of two type's, error type one which accounts for the false positive and error type two are false negative.

True Positive: True positives are the instances that are positive and the classifier predicted as positive

True Negative: True negatives are the instances that are negatives and the classifier predicted as negative.

False Positive: False positives are the instances that are positive and the classifier predicted as negative

False Negative: False negatives are the instances that are negative and the classifier predicted as positive

		PREDICTED	
ACTUAL		Positive	Negative
	Positive	TP	FP
	Negative	FN	TN

Table 4.1: Confusion Matrix

C. Experiments:

Combining data mining techniques into intrusion detection system offer more security than traditional methods. Since data mining can use vast number of data, detecting a tiny variation in the network traffic is possible leading to detect and block unwanted traffic in the network. In the present study multi layer perceptron classifier is used to classify the network attack types. MLP based intrusion detection system is designed to support network administrators to find signature based attacks and anomaly of the network traffic. The IDS is trained on the traffic data using MLP to capture the known attack types and differentiate traffic as intrusion and normal traffic.

D. Feature Selection:

The traffic data set has 43 different features that belong to a particular behaviour group and the data set has dimensionality problem. In order to select the best features and to reduce the data dimensions that can represent the malicious traffic, the feature selection algorithm information gain is chosen to rank the features. The data set is applied to the feature selection algorithm. Based on the flow features all the features are found to important as flow features are the primary characteristics that describe the network and its behaviour. To reduce the data dimension features that are top ranked are chosen for classification. The selected features include id, ct_state_ttl, sbytes, sttl, dttl, rate, smean, dur, sinpkt, sload.

V. CLASSIFICATION RESULTS

The classification results for the selected features shows an accuracy of 98%. The confusion matrix shows true positives of 384 instances, false positive of 29 instances, true negatives of 1089 instances and false negative of 1 instance. 98% of precision, 98% of recall and f-score of 98 is achieved when reducing the number of features. The reduced number of features and their importance in traffic classification is evaluated using the feature characteristics.

	Actual	Predicted
Actual	384	29

Predicted	1	1089

Table 5.1: Confusion Matrix

Accuracy	Precision	Recall	f-Score
98%	98%	98%	98%

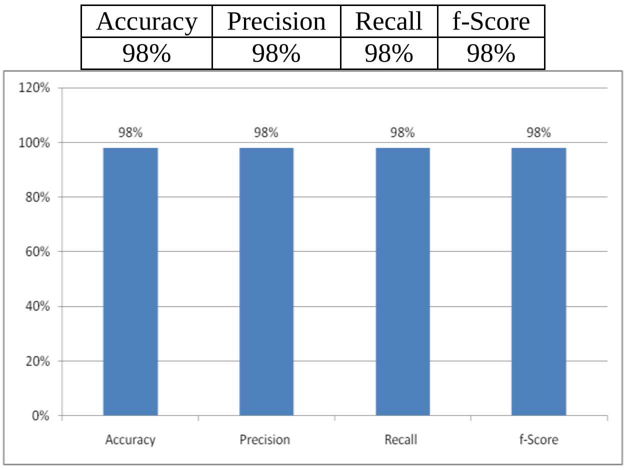
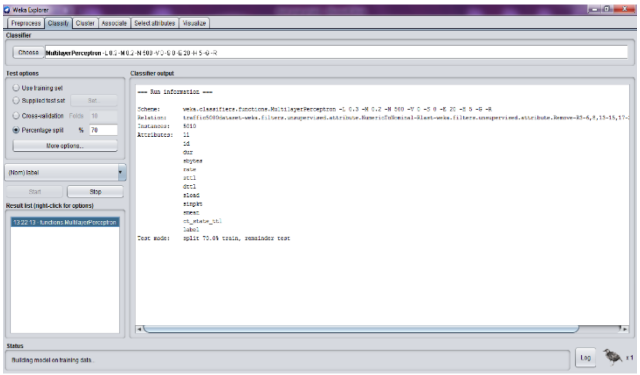


Fig. 5.1: Accuracy metrics

VI. DISCUSSION

sttl ,dttl, sload, smean belong to general features, while sinpkt, sload, dur belong to time features, while ct_state_ttl, smean belong to extra general features. Spkts, dpkts, sbytes, dbytes, dttl refers to the payload of the network transaction, where the user data is usually transmitted from source to destinations. Infected program uses these packet headers to hide their message or communication to their master which disguises their additional packet load in the traffic data. The payload based features differ with respect to protocol and the difference between normal and infected can be differentiated through the packet size sent and received. The difference between packets sent and the received varies, and then there are chances that the traffic can be infected, since the packets never get altered in the middle of a normal traffic flow. Also, extra general features count for the malicious behavior on the time to live and method used to transmit data between source and destination with respect to specific protocols. This study demonstrated detection of malicious traffic from HTTP network data using feature selection and machine learning techniques. The study showed that classification performance can be improved through selecting important features by feature selection method.



MultilayerPerceptron -L 0.3 -M 0.2 -N 500 -V 0 -S 0 -E 20 -H 5 -G -R

○ Use training set
○ Supplied test set
○ Cross-validation Folds 10
● Percentage split % 70

(Nom) label

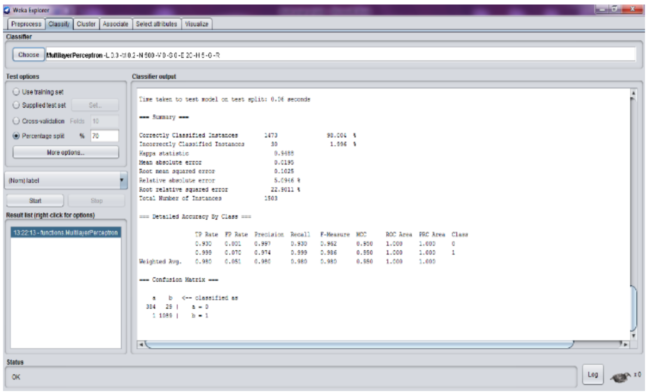
13:22:13 - functions.MultilayerPerceptron

```
=== Run information ===

Scheme:       weka.classifiers.functions.MultilayerPerceptron -L 0.3 -M 0.2 -N 500 -V 0 -S 0 -E 20 -H 5 -G -R
Relation:     traffic5000dataset-weka.filters.unsupervised.attribute.NumericToNominal-Rlast-weka.filters.unsupervised.attribute.Remove-R3-6,8,13-15,17-
Instances:    5010
Attributes:   11
              id
              dur
              sbytes
              rate
              sttl
              dttl
              sload
              sinpkt
              smean
              ct_state_ttl
              label
Test mode:    split 70.0% train, remainder test
```

Status
Building model on training data

Fig. 6.1: Data Partitioning for Training as 70%



MultilayerPerceptron -L 0.3 -M 0.2 -N 500 -V 0 -S 0 -E 20 -H 5 -G -R

○ Use training set
○ Supplied test set
○ Cross-validation Folds 10
● Percentage split % 70

(Nom) label

13:22:13 - functions.MultilayerPerceptron

```
Time taken to test model on test split: 0.06 seconds

=== Summary ===

Correctly Classified Instances        1473               98.004 %
Incorrectly Classified Instances        30                1.996 %
Kappa statistic                          0.9488
Mean absolute error                      0.0195
Root mean squared error                  0.1025
Relative absolute error                  5.0946 %
Root relative squared error             22.9011 %
Total Number of Instances             1503

=== Detailed Accuracy By Class ===

                 TP Rate  FP Rate  Precision  Recall   F-Measure  MCC      ROC Area  PRC Area  Class
                 0.930    0.001    0.997      0.930    0.962      0.950    1.000     1.000     0
                 0.999    0.070    0.974      0.999    0.986      0.950    1.000     1.000     1
Weighted Avg.    0.980    0.051    0.980      0.980    0.980      0.950    1.000     1.000

=== Confusion Matrix ===

    a    b   <-- classified as
  384   29 |    a = 0
    1 1089 |    b = 1
```

Status
OK

Fig. 6.2: Classified Instances Result

VII. CONCLUSION

In this study classification of normal and infected HTTP network data using traffic dataset is done. The traffic dataset consist of about 43 features with two class labels, normal and infected. The information gain feature selection is used to reduce the data dimensions. The selected features are applied to the classification, where the network flow is classified into normal and infected using Machine learning algorithm MLP. The classification result shows an accuracy of only 98% for selected features.

VIII. FUTURE WORK

As newer types of traffic infections are and characteristics are being introduced daily. The growing amount of newer malicious traffics demands a rich detection capabilities and also, quicker in response with low computational time. Although the network traffic data is huge for any traffic behaviour study, the computational problems and costs are limiting, newer methods addressing these limitations are in need. The features selected in the present study are with respect to the normal and infected pattern where as specific to different variants of malicious activities are to be included in the future work. With growing capabilities of machine learning algorithm and their usage, more number of algorithms are being introduced and studied extensively. As a future work, more algorithms and data mining techniques will be employed to improve the detection rate of infected traffic data. Also, this study utilized only HTTP network, other network and traffic data could help improve the classification and detection of infections actively.

REFERENCES

[1] Belouch, M. (2017, March). Comparison of ensemble learning methods applied to network intrusion detection. In Proceedings of the Second International Conference on Internet of things and Cloud Computing (p. 194). ACM.

[2] Idhammad, M., Afdel, K., & Belouch, M. (2018). Semi-supervised machine learning approach for DDoS detection. Applied Intelligence, 1-16.

[3] Azab, A., Alazab, M., & Aiash, M. (2016, August). Machine learning based botnet identification traffic. In Trustcom/BigDataSE/I? SPA, 2016 IEEE (pp. 1788-1794). IEEE.

[4] Terzi, D. S., Terzi, R., & Sagiroglu, S. (2017, October). Big data analytics for network anomaly detection from netflow data. In Computer Science and Engineering (UBMK), 2017 International Conference on (pp. 592-597). IEEE.

[5] Li, S. H., Kao, Y. C., Zhang, Z. C., Chuang, Y. P., & Yen, D. C. (2015). A network behavior-based botnet detection mechanism using PSO and K-means. ACM Transactions on Management Information Systems (TMIS), 6(1), 3.