NavaJyoti, International Journal of Multi-Disciplinary
Research Volume 2, Issue 1, August 2017

Neural Network Model for Email-Spam Detection

[1]Shama.N, [2]Thanfiya

[1]*Department of Master of Computer Science, Jyoti Nivas College Post Graduate Centre, Bangalore*
[2]*Department of Master of Computer Science, Jyoti Nivas College Post Graduate Centre, Bangalore*

ABSTRACT

Email spam is a word that we come across in our daily life. The word spam means junk mails. The unsolicited emails that are received by any person in his/her mailbox are called spam. These junk mails are usually sent in bulk for advertising and marketing some products. This work presents a neural network approach to intrusion detection. A Multi-Layer Perceptron using Back Propagation Algorithm is used to classify the emails as a spam or normal mail in an email spam application.

Keywords: Email Spam, Classification, Back Propagation Algorithm

1. INTRODUCTION

An Intrusion detection system monitors network traffic and monitors for suspicious activity and alerts the system or network administrator. In some cases the IDS may also respond to anomalous of malicious traffic by taking action such as blocking the user or source IP address from accessing the network.IDS come in a variety of flavors and approach the goal of detecting suspicious traffic in different ways. One such flavor is detection of Email-spam. Internet poses serious concerns on the security of computer infrastructures and the integrity of sensitive data. Intrusion detection is the art of detecting computer abuse and any attempt to break the networks.

IDS are designed to identify unauthorized use, misuse and attacks on information system. Soft-computing based methods have been proposed for the development of Intrusion detection system. The costs of temporary or permanent damages caused by unauthorized access of the intruders to computer systems have urged different organizations. ANN is an information processing model that is inspired by biological nervous systems, such as brain. It is the network of individual neurons. Each neuron in a neural networks acts as individual processing element. Each neuron is fundamentally a summing element followed by an activation function. The output of each neuron is fed as input to all of the neurons in the next layer.

As we know that Email spam is one of the major problems of the today's internet, bringing financial damage to companies and annoying individual users. Among the approaches developed to spam, filtering is an important and popular one. As it effects the email communication in a wider range that is spam puts unnecessary load on the network traffic. It takes lot of time to clear those junk emails.
Most modern email-spam software packages provide some form of programmable filtering, typically in the form of rules that organize mail into folders or dispose of spam mail based on keywords detected in the header or body. However, most users avoid customizing software.

In addition, manually constructing robust rules is difficult as users are constantly creating, deleting and recognizing their folders. Even if the folders remain the same, the nature of emails within in the folder may well drift over time. The characteristics of the spam email(Eg:-topics, frequent terms) also change over time. Hence, the rules must be constantly tuned by the user, that is time consuming and error-prone. A system that can automatically learn how to classify emails

into a set of folders and filter spam emails is highly desirable. Several systems for automatic email classification based on Text Categorization have been developed.

Therefore a fully connected multilayer perceptron trained with back propagation algorithm is used as a classifier. For each user, it learns from a set of emails with assigned mailboxes. The current assumption is that each email is only assigned to one mailbox. The NN classifier is a multi-class one ie, there is one output neuron for each mailbox

2. LITERATURE STUDY

Previous studies have focused on classification of records in one of the two general classes: Normal, Attack.
Features to identify that the mail is spam or a normal mail:
1. Words that are found in Header of the email
2. Text that is found in the content of the mail.
3. From address of the mail. (From address can be any malicious text)
4. Frequent occurrence of word in body of the message.

The above classification will decide the spam words will fall under which category. The signature based techniques for spam detection is the most widely used method.The purpose of this report is to introduce the user to Intrusion Detect Systems and give a deep understanding of some sophisticated techniques for intrusion detection.Intrusion Detection is an important component of infrastructure protection mechanisms. Given the increasing complexities of today's network environments, more and more system s are becoming vulnerable to attacks and hence it is important to look at systematic, efficient and automated approaches for Intrusion Detection.

3. IMPLEMENTATION USING BACK PROPAGATION ALGORITHM

This work has gone through all the previously implemented research papers in which it was found to implement a Multi-Layer Perceptron model using back propagation algorithm to classify e mails as normal or -spam mails. Multi-Layer perceptron model where the inputs are provided in order to gain the desired output out of which if any intruder or spam message is encountered then it is reported to the user.
The Multi-layer perceptron is one of the most widely used types of neural networks. It is simple and based on solid mathematical grounds. Input quantities are processed through successive layers of "neurons".

There is always an input layer, with a number of neurons equal to the number of variables of the problem, and an output layer, where the perceptron response is made available, with a number of neurons equal to the desired number of quantities computed from the inputs (very often only one).

The layers in between are called "hidden" layers. With no hidden layer, the perceptron can only perform linear tasks (for example a linear discriminant analysis, which is already useful). All problems which can be solved by a perceptron can be solved with only one hidden layer, but it is sometimes more efficient to use 2 hidden layers.

Each neuron of a layer other than the input layer computes first a linear combination of the outputs of the neurons of the previous layer, plus a bias. The coefficients of the linear combinations plus the biases are called the weights. They are usually determined from examples to minimize, on the set of examples, the (Euclidian) norm of the desired output - net output vector. Neurons in the hidden layer then compute a non-linear function of their input. Usually, the non-linear function is the sigmoid function,

Y(x) = 1/ (1+exp (-x))).

The output neuron(s) has its output equal to the linear combination. Thus, a Multi-Layer Perceptron with 1 hidden layer basically performs a linear combination of sigmoid function of the inputs. A linear combination of sigmoid is useful because of 2 theorems:

- A linear function of sigmoid can approximate any continuous function of 1 or more variable(s). This is useful to obtain a continuous function fitting a finite set of points when no underlying model is available.
- Trained with a desired answer = 1 for signal and 0 for background, the approximated function is the probability of signal knowing the input values.

This work attempts to apply a MLP to the problem of email spam detection. It is based on content filtering and is a method that is getting popular these days. It is can be a very
Accurate and efficient method for text classification. It is an extension of text classification technology, which searches the textual content of an email and employs algorithms to classify an Email as spam or not-spam (1 or 0).

The MLP is used to classify the occurrence of certain words and phrases in terms of how and where they appear in the email message. Thus the spam filtering problem can be broken down into a simple classification Problem.

"The Multi-layer perceptron is one of the most widely used types of neural networks. It is simple and based on solid mathematical grounds. Input quantities are processed through successive layers of "neurons". There is always an input layer, with a number of neurons equal to the number of variables of the problem, and an output layer, where the perceptron response is made available, with a number of neurons equal to the desired number of quantities computed from the inputs (very often only one). The layers in between are called "hidden" layers.

Text categorization that says the mail is spam or normal mail from the sender it is categorized into a positive class (relevant to the user) or a negative class (irrelevant to the user).Text Classification is the task of automatically sorting a set of documents into categories such as topics from a predefined set.
Hence the proposed work to implement is that categorizing what kind of a text it is, and then solve the problem of email spam.

1. Perform a feedforward pass, computing the activations for layers L_2, L_3, and so on up to the output layer L_{n_l}.
2. For each output unit i in layer n_l (the output layer), set

$$\delta_i^{(n_l)} = \frac{\partial}{\partial z_i^{(n_l)}} \frac{1}{2} \|y - h_{W,b}(x)\|^2 = -(y_i - a_i^{(n_l)}) \cdot f'(z_i^{(n_l)})$$

3. For $l = n_l - 1, n_l - 2, n_l - 3, \ldots, 2$

For each node i in layer l, set

$$\delta_i^{(l)} = \left(\sum_{j=1}^{s_{l+1}} W_{ji}^{(l)} \delta_j^{(l+1)} \right) f'(z_i^{(l)})$$

4. Compute the desired partial derivatives, which are given as:

$$\frac{\partial}{\partial W_{ij}^{(l)}} J(W,b;x,y) = a_j^{(l)} \delta_i^{(l+1)}$$

$$\frac{\partial}{\partial b_i^{(l)}} J(W,b;x,y) = \delta_i^{(l+1)}.$$

CONCLUSION

In this paper an email spam detection method is implemented to efficiently detect the spam mails to justify and classify as normal and attack and also mainly focusing on the identification of what kind of text can make the mail spam mail or a normal mail. So the text can be encountered in the Header of the mails, in the body of the mail, and also from address of the mail as well the popup windows that the user is not interested in can also be said as the spam messages.
Hence to overcome all this, the proposed work is first categorizing the problem to be an attack or a normal that is implemented with multilayer perceptron using back propagation algorithm. The work presented here can be further extended and can be tested with different algorithms. One such algorithm implemented is back propagation algorithm.

References

[1]. Ismaila Idris, "E-mail Spam Classification with Artificial Neural Network and Negative Selection Algorithm", Ismaila Idris, December 2011.
[2]. SivanadyanThiagarajan, "Detecting Spam emails using neural networks November 2012.
[3]. Mohammed Awad and MonirFoqaha, "Email spam classification using Hybrid approach of RBF Neural Network", July 2016.
[4]. Ganesh Kumar Devaraj,"Intrusion Detection Using Artificial Neural Network With Reduced Input Features",July 2010.
[5]. G Wang, "Intrusion Detection Using Artificial Neural Networks", February 2010.
[6]. SK.Jonnalagadda, "Comprehensive Analysis on Intrusion Detection Using Neural Network", January 2011.
[7]. P.Kabiri, "Research on Intrusion Detection and Response", 2005
[8]. Mukkamalla, "Apllications of Neural Networks To Intrusion Detection", November 2009.
[9]. SM ELseuofi, "Enhancing E-mail Filtering Based on GRF", March 2014.
[10]. I Idris, "Improved Negative Selection Algorithm for Email Spam Detection Application", 2014.
[11]. Devaraj, "Detection of Accuracy for Intrusion Detection System using Neural Network Classifier", January 2013.