Decision Science Letters 3 (2014) 439–444

Contents lists available at GrowingScience

Decision Science Letters

homepage: www.GrowingScience.com/dsl

Identifying spam e-mail messages using an intelligence algorithm

Parichehr Ghaedi[a*] and Ali Harounabadi[b]

[a]*Department of Computer Engineering, Science and Research Damavand Branch, Islamic Azad University, Damavand, Iran*
[b]*Department of Computer, Central Tehran Branch, Islamic Azad University, Tehran, Iran*

C H R O N I C L E

Article history:
Received October 15, 2014
Accepted January 24, 2014
Available online
January 26 2014

Keywords:
Spam
Multiagent filter
Neural Network

A B S T R A C T

During the past few years, there have been growing interests in using email for delivering various types of messages such as social, financial, etc. There are also people who use email messages to promote products and services or even to do criminal activities called Spam email. These unwanted messages are sent to different target population for different purposes and there is a growing interest to develop methods to filter such email messages. This paper presents a method to filter Spam email messages based on the keyword pattern. In this article, a multi-agent filter trade based on the Bayes rule, which has benefit of using the users' interest, keywords and investigation the message content according to its topic, has been used. Then Nested Neural Network has been used to detect the spam messages. To check the authenticity of this proposed method, we test it for a couple of email messages, so that it could determine spams and hams from each other, effectively. The result shows the superiority of this method over the previous ones including filters with Multi-Layer Perceptron that detect spams.

1. Introduction

The fast improvement of Internet technology along with its advantage has created significant opportunities for easier communications, information distribution, etc. Sending/receiving email is one of the most popular Internet services and it has become the primary tool for exchange of information among business owners and other people. However, like other services throughout the world, it has its own problem. However, many email users have been receiving unwanted email messages call Spam email, which are trouble making issue. To solve this problem, to create the sense of security for users and to save users' time, there is a need to develop some methods to block these unwelcome email messages to give better services to the users. The primary aim of filtering methods is to analyze the messages, to select and to extract some features from the header or the body of an email to detect spam email messages from the regular ones. The methods are expected to detect most spam messages as efficiently as possible. This paper presents a method, which could be a solution and method to help

* Corresponding author.
E-mail addresses: parichehr.ghaedi@gmail.com (P. Ghaedi)

doi: 10.5267/j.dsl.2014.1.002

users apply and receive this service, more effectively. In this article, using a multi-agent filtering, which can select a series of features and using the Nested Back-Propagation Neural Network, the proposed model detects the spams. It also determines spams and hams of each other with specific error degree. In the following sections, first we explain the scope of the research, then look at previous researches and then state the proposed method, and apply them for a case study.

2. Scope

There are different types of definitions for spam email messages and one of the most popular ones is "unwanted and unpleasant email which is sent directly or indirectly by a sender who has no relation with the receiver" (Jaffar Gholi Beyk, 2012; Olawale Sulaimon, 2011; Nazirova, 2011). Spam email messages have different forms, which can be classified according to the aims of intruders including business products introductions, financial services, spam email messages about sanitation and frauds (Jaffar Gholi Beyk, 2012; Olawale Sulaimon, 2011). These spam email messages may cause many problems, directly or indirectly, for email system, such as: jam-packed traffic in the network, misusing the saving environment and calculating sources, lacking security, legal affairs resulting from pornography and related advertisement, financial casualty like the pyramid sketches, and economical fraud like phishing, spreading viruses, Trojan horses and worms, wasting the band width and users' money by dial up (Olawale Sulaimon, 2011; Banday & Jan, 2009; Tak & Tapaswi, 2010; Lazzari et al., 2005). Regarding these problems, we need to have a strong anti-spam filtering to fight against it.

3. Related Works

The increase of spam messages in recent years has resulted in delicate filtering methods. Therefore, the researchers have done their best to present efficient and exact methods in detecting spams; one of the mostly used methods is the machine learning. Ayodele et al. (2010) considered the classification of email messages by using Back-Propagation method. First, they use the process of cross validation measurement *n* different times, applying the model, we use it to predict the classification of email messages, and to apply their neural network approach in classification. They reported that if Back-Propagation method were suitable for a few received email messages, it would reach 98% accuracy comparing with human judgment. However, if it is supposed to check more than 6000 email messages, the accuracy of the proposed method decreases and this is regarded as one of the weakest points of this method to check the error compared with few email messages. Ndumiyan et al. (2013) designed a neural network classifier to detect and to classify spam email messages based on descriptive peculiarities from the escaping patterns that spammers use, and explained that their neural network classifier could detect and filter the spam email messages successfully just like the previous ones.

Hameed and Mohammed (2013) introduced Optical Back-Propagation, which is a shape of Back-Propagation algorithm. One of the most important characteristics of this algorithm can escape from the local minimum in the course of training with high speed. Two different structures used for Optical Back-Propagation, depending whether PCA is used or not. The first one is OBP structure-1 and the second one is OBP structure-2. They showed that when the first one yield better results.

Nosseir et al. (2013) classified many email messages from several universities in one section and three lists of tree, four and five character words. These lists have two classifications of words, bad and good, taken out of the emails. To prepare this list, the contents of messages are detected in three levels: stop-words removal, noise removal and stemming. Then they train multi neural network on bad and good words and testing the results. Their method showed low false positive and high true negative, which proved the authenticity of the method.

4. Proposed Method

As the spams have different characteristics, the methods using these characteristics by the name of agent, is named multi-agent filtering. If, we have one agent, we measure the possibility whether the emails are spams or not. If we cannot decide on whether they are spams or not, then we use detecting agents in a group. First, for determining the needed agents for multi-agent filtering method, we need about users' interests. For example, if the user is the sales manager of a company, the emails like goods new prices will be placed in hams, but the same email messages might be considered spams for a school teacher (Jaffar Gholi Beyk, 2012; Androutsopoulos et al., 2000). To filter emails by multi-agent neural network, we need to have spam messages and hams collected and labeled previously in a database from words, phrases and tokens. This database is divided into two parts: hams and spams. It is important to know that the hams database is made based on the needs a person or an organization. It makes the filtering work better and decreases the error. Spam database must have many samples of known spam email messages and be updated. This increases the reliability of filtering and leads to spams with high rate. Also this database is calculated based on the possible of words in our list to get the possible spams or hams according to the following formula (Jaffar Gholi Beyk, 2012; Chakraborty, N., & Patel, A. (2012):

$$\Pr(S|W) = \frac{\Pr(W|S)\,.\,\Pr(s)}{\Pr(W|S)\,.\,\Pr(S) + \Pr(W|H)\,.\,\Pr(H)} \tag{1}$$

Pr(S|W) :The probability that a message is a spam, knowing that the word is in it.

Pr(S) : The overall probability that any given message is spam.

Pr(W|S) : The probability that the word appears in spam messages.

Pr(H) : The overall probability that any given message is not spam (is "ham").

Pr (W|H) : The probability that the word appears in ham messages.

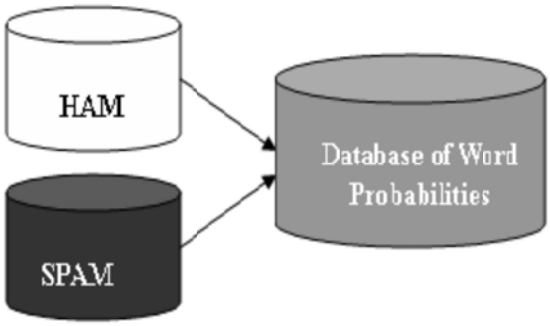

Fig. 1. creating a word database for the filter

For example, if the word "Insurance" appears in 15 samples of 200 spam email messages and 1 samples of 200 hams, then the email is a spam and its probability is as follows,

$$\mathrm{P}(\text{Insurance}|\text{Spam}) = \frac{\frac{15}{200}}{\frac{15}{200} + \frac{1}{200}} = 0.93 \tag{2}$$

After creating a database for multi-agent filter, some of the messages are used as the training set and some of them are considered as the test. In the next stage, the output of the first neural network is

used as the input of the second neural network. In order words, the second neural network has four inputs including the output of the first neural network, the number of links in an email, the number of word with capital letters and the time of sending that email. It must be said that these agents play essential role in detecting spam email messages. During the last stage, the output gained from the second neural network is the final output and determines whether the email is spam or not. We create a rule based trial and error to make these three agents effective: the number of links in an email, the number of words with capital letters and the time of sending that email. We will explain these rules.

For the number of the links, there is a very simple rule: just count the number of existing links in each message. If the number of links is high, the possibility of email being a spam increases since spam email messages have many links. For the number of words with capital letters, first we count the words of all the letters, which are in capital, then based on the following method, we state its possibility. If the number is zero, it means that there are no word with capital letters in the email message, which is the possibility of an email to receive spam message is negligible (the email might be ham). If the number is one, it means that all the words in our email are with capital letters and here the possibility of an email to receive spam is very high (the email might be spam), of course if the spams are all with capital letters.

$$P(w) = \frac{n(w)}{n(S)} \tag{3}$$

P(w) : The possibility of word with capital letters.

n(w) : The number of words with capital letters in an email.

n(S) : The number of all emails.

For the time of sending an email, first, we read the time of sending from the item “Date”, then based on a time classification, we give it a number between zero and one. If the number in question is near one, it means that the email has been sent at night and the possibility of it being a spam is high, of course if the spam message is sent at night. The time classification is as follows:

- If the email is sent between 6 a.m. to 8 p.m., the possibility is α_1.
- If the email is sent between 8 p.m. to 12 midnight, the possibility is α_2.
- If the email is sent between 12 midnight to 6 a.m., the possibility is α_3.

In fact, we use Nested Neural Network to detect the spams. After getting the final output, we calculate the amount of Precision and Recall, which are measuring means:

$$\text{Spam Precision(SP)} = \frac{n_{ss}}{n_{ss} + n_{ls}} \tag{4}$$

$$\text{Spam Recall (SR)} = \frac{n_{ss}}{n_{ss} + n_{sl}} \tag{5}$$

$$\text{Legitimate Precision(LP)} = \frac{n_{ll}}{n_{ll} + n_{sl}} \tag{6}$$

$$\text{Legitimate Recall (LR)} = \frac{n_{ll}}{n_{ll} + n_{ls}} \tag{7}$$

$$\text{Accuracy} = \frac{n_{ll} + n_{ss}}{n_{ll} + n_{ls} + n_{sl} + n_{ss}} \tag{8}$$

n_{ll}: The number of legitimate email messages classified correctly as legitimate email.

n_{ss}: The number of spam messages classified correctly as spam.

n_{sl} : The number of spam messages classified wrongly as legitimate email.

n_{ls} : The number of legitimate email classified wrongly as spam.

5. Case Study

Here 400 short messages have been used to train the network; 200 messages have been labeled spams and 200 ones are considered as legitimate ones. They have been used in equal numbers to prevent the error of network. Then the list of words consisting 261 words are made and we have calculated possibilities based on Bayes theorem, which is used for filters. Then the first neural network is tested with short messages. Then we test the gained output of the first neural network as the input along with three other agents of number of existing links in one email, the number of words with capital letters in one email and the time of sending the email to the second neural network. Then we test the network with giving the characteristics of an email. The number of hidden layers is considered one for both networks by trial and error method. We get 8 neurons of hidden layers. In this layer, in both network, we use Tangent Sigmoid function and in the output layer we use Linear function. We use, also 400 email messages to test the network. Here we state the amounts of the time of sending email.

$\alpha_1 = 0.01$: The time of sending the email between 6 a.m. to 8 p.m.

$\alpha_2 = 0.2$: The time of sending the email between 8 p.m. to 12 midnight.

$\alpha_3 = 0.9$: The time of sending the email between 12 midnight to 6 a.m.

Now after getting the final output, we calculate Precision and Recall and compare then with the previous ones.

Table 1
Comparing Precision and Recall of proposed method using the method by Jaffar Gholi Beyk, (2012)

		Spam		Legitimate email(Ham)	
		Recall	Precision	Recall	Precision
Jaffar Gholi Beyk	Words	94.3%	97.1%	93.4%	87.7%
	Words + Phrases	94.3%	97.6%	94.7%	87.7%
	Phrases +words +Peculiarities related to the scope	98.3%	96%	98.5%	96.2%
Proposed Method		98%	97.5%	97.5%	97.9%

As we can observe from the results of Table 1, the nested neural network, which is Error Back-Propagation with learning supervision, can perfectly detect the spam compared with Multi-Layer Perceptron neural network. In addition, our accuracy, which is 97.77% representing the precision of the proposed method in detecting the spams.

6. Conclusion and Future studies

In this article, a multi-agent filtering method has been used regarding points like users' interest, subject and content. After the preparing the list of keywords, we calculate the possibilities of each item by Bayes theorem. Then we have used nested neural network to detect the spams. To prove its authenticity, we test it on a lot of email messages. The outputs of neural network of spams and hams have been detected by the specific error degree. The results have shown the advantages of the filter of neural network over other filtering method, namely, Multi-Layer Perceptron neural network. For future studies, we can test the Fuzzy algorithms, testing this method of various neural networks with different learning methods, completing the method by increasing and expanding the database and using hybrid methods to detect spam messages. To use the proposed method in particular functions, we need a larger database and updating it.

Acknowledgement

The authors would like to thank the anonymous referees for their comments on earlier version of this paper.

References

Androutsopoulos, I., Paliouras, G., Karkaletsis, V., Sakkis, G., Spyropoulos, C. D., & Stamatopoulos, P. (2000). Learning to filter spam e-mail: A comparison of a naive bayesian and a memory-based approach. *arXiv preprint cs/0009009*.

Ayodele, T., Zhou, S., & Khusaino, R. (2010). Email classification using back propagation technique. *International Journal of Intelligent Computing Research(IJICR),* 1(1/2), 3-9.

Banday, M. T., & Jan, T. R. (2009). Effectiveness and limitations of statistical spam filters. *arXiv preprint arXiv:0910.2540*.

Chakraborty, N., & Patel, A. (2012). Email spam filter using Bayesian neural networks. *International Journal of Advanced Computer Research*, 2(1), 65.

Hameed, S. M., & Mohammed, N. J. (2013). A content based spam filtering using optical back propagation technique. *International Journal of Application or Innovation in Engineering and Management (IJAIEM),* 2(7), 416-421.

Jaffar Gholi Beyk, A. (2012). Machine learning method in detecting spams with content value approach. Master of Science Research, Computer College, Azad University Dezful Branch.

Lazzari, L., Mari, M., & Poggi, A. (2005, June). Cafe-collaborative agents for filtering e-mails. In *Enabling Technologies: Infrastructure for Collaborative Enterprise, 2005. 14th IEEE International Workshops on* (pp. 356-361). IEEE.

Nazirova, S. (2011). Survey on Spam Filtering Techniques. *Communications and Network*, *3*(3), 153-160.

Ndumiyana, D., Magomelo, M., Sakala, L. (2013). Spam detection using a Neural Network classifier. *Online Journal of Physical and Environmental Science Research,* 2(2), 28-37.

Nosseir, A., Nagati, K., & Taj-Eddin, I. (2013). Intelligent word-based spam filter detection using multi-neural networks. *International Journal of Computer Science Issues,* 10(2), 17-21.

Olawale Sulaimon, O. (2011). *E-mail spam: Challenges and filtering techniques*. Bachelor Thesis, Tornio, Kemi-Tornio University of Applied Sciences.

Tak, G. K., & Tapaswi, S. (2010). Query Based approach towards spam attacks using artificial neural network. *International Journal of Artificial Intelligence & Applications*, *1*(4). 82-99.