International Journal of Scientific and Innovative Research 2017; 5(1) : 99-102
P-ISSN 2347-2189, E- ISSN 2347-4971

AN APPROACH BASED ON BAYESIAN METHOD IN COMBINATION WITH BLACKLIST AND WHITELIST FILTERS

*** Devesh Katiyar**

Department of Computer Science, Dr. Shakuntala Misra National Rehabilitation University, Lucknow, Uttar Pradesh, India

*Address for correspondence: Dr. Devesh Katiyar, Assistant Professor, Department of Computer Science, Dr. Shakuntala Misra National Rehabilitation University, Lucknow, Uttar Pradesh, India

ABSTRACT

Spam is more often regarded as junk mail or junk newsgroup electronic publications. Some people describe the spam even more generally as any unsolicited e-mail. Real spam is generally e-mail advertising for some product sent to a mailing list or newsgroup. Most spam is commercial advertising, often for dubious products, get-rich-quick schemes, or quasi-legal services. Spam costs the sender very little to send -- most of the costs are paid for by the recipient or the carriers rather than by the sender.

Keywords: SPAM; HAM; Blacklist; White list; Bayesian

INTRODUCTION

Electronic mail is presently the most familiar, cheapest and expedient technique of daily communication between individuals and organizations. A spam filter is a program that is utilized to distinguish unsolicited and unnecessary emails and foil those messages from getting to a user's inbox. Similar to other varieties of filtering programs, a spam filter seems for definite criterion on which it bases judgments. Spam can also be defined as junk mail, but it involves the question: what is spam? Although most users know what email is spam, but it is not obvious how to define spam. Spam is more often regarded as junk mail or junk newsgroup electronic publications. Some people describe the spam even more generally as any unsolicited e-mail. However, if a long-lost brother, the email is time - and sends you a message, this could hardly be called spam, even though it has been requested. Real spam is generally e-mail advertising for some product sent to a mailing list or newsgroup.

The network-level blacklisting is based on creating intentional network outages. The method has the ability the detect spam letters based on its origin rather than its content. Unfortunately new spam hosts can pop up instantly and the propagation time could be a significant weakness. Moreover if a legitimate user was accidentally blacklisted, there is no way, to get off the blacklist, hence all mails ware rejected from the blacklisted part of the network. Spammers have learnt quickly how they can get around blacklisted networks.

White listing is the opposite of blacklisting. Content filtering identifies spam, while white listing requires identifying users. A white list is a collection of reliable contacts. If e-mail comes from the members of this list, it should be marked automatically as legitimate letter what is also called ham. Just as the blacklisting, the white list also needs a continuous upgrade and refreshment.

LITERATURE REVIEW

Spam has caused some serious problems that alert email user nowadays. Firstly, it wastes a lot of network resources that are very important for network users. It may fill up the user's email mailbox and therefore causing insufficient space for legitimate email to pass through. Secondly, it greatly influences the daily work of many users by require users to spend a lot of time to deal with spam every day. Beside, many current spam mails bring users unexpected wicked attachments that would seriously crack the user's system.

According to the report published by FTC (Federal Trade Commission), there are several types of offers made via spam e-mails. The spam e-mails fell into eight general categories with catch-all category included for types of offers that appeared infrequently as shown in Table

Type of Offer	Description
Investment/Business Opportunity	Work-at-home, franchise, chain letters, etc.
Adult	Pornography, dating services, etc.
Finance	Credit cards, refinancing, insurance, foreign money offers, etc.
Products/Services	Products and services, other than those coded with greater specificity.
Health	Dietary supplements, disease prevention, organ enlargement, etc.
Computers/Internet	Web hosting, domain name registration, email marketing, etc.
Leisure/Travel	Vacation properties, etc.
Education	Diplomas, job training, etc.
Other	Catch-all for types of offers not captured by specific categories listed above.

The simplest definition of SPAM is that it is any received email message that is unwelcome by the recipient. SPAM has been identified as the most widespread problem facing email users. The mainstream of SPAM is sent to attain a profit, through the sale of goods or services. The major problem with SPAM is that it is the receiver that is paying for the SPAM in terms of spending their time to check and clean their inboxes. The flexibility of a SPAM filter depends on the filtering software. SPAM filter analysis may be directed at the following:

Header analysis: Here the SPAM filter will check the header of the incoming email, if the header is defined as a SPAM (for example: free gifts for you, you are the winner…etc) the SPAM filter will prevent the message from passing through to the recipient.

Address lists analysis: If the incoming email is from any unknown sender, the SPAM filter will check the email address of the sender against the address list that the recipient allows receiving messages from, then the message will be blocked or passed through to the user.

Keyword lists analysis: The SPAM filter will check the contents of the incoming message if it has any words that could be suspicious (like: Viagra, Sex…etc), then the message will be blocked [Allman, 2003b].

Bayesian Filtering

Bayesian filtering is an extension of the text classification technology. This filter is a computer program used to recognize the words in a document, and can be implemented in a SPAM filter to search the textual content of an email. Bayesian filtering method uses text categorization algorithms to determine the probability that a certain email is SPAM [Didsbury, 2003]. The algorithms are capable of categorizing the occurrence of certain words or phrases in terms of how and where they appear in the email message, but not by their existence alone. The challenge with content filtering is that SPAM emails often contain simply image links (e.g. photographs), which download image-based content to the receiver [Androutsopoulos *et al.*, 2000a]. Bayesian SPAM

filters are capable of analysing text, but are not capable of analysing images. To carry out the analysis of images requires pattern matching techniques which is another area of research in itself. This analysis is beyond the scope of this study.

Although the Bayesian filter is quite effective, it needs to be updated regularly. The reason for this is that it divides the incoming email messages into two classes, legitimate or illegitimate. Following this, each email is split into tokens (words, html codes, etc.) so their occurrence in the body of the messages can be computed. Based on this occurrence and using a specific mathematical formula, the probability that an email is SPAM or not can be calculated [Pelletier *et al.*, 2004].

Bayesian Filter subject to HAM or SPAM

If the filter has not recognized the incoming message as a whitelist or a blacklist, the Bayesian filter will be applied on <SUBJECT> field and the content <BODY> of the message. The filter scans through the message, and creates a probability of every word (spamicity). This spamicity value is assigned to each word, and ranges from 0.0 to 1.0. [Process, 2005]. If the spamicity value is greater than or equal to 0.5 then the message containing the word is likely to be SPAM. The filtering process checks (using Bayesian method) the incoming email message against the SPAM words text file which is called (defaultStopWords.txt). The content of this file will be similar to (Vi ag r a, ¾«Æ·Í¼Êé1ÕÛ-5ÕÛ…etc). Furthermore, the users may include their own custom SPAM phrases. The content of this text file is updated manually at this stage, but it may also be updated (in future work) form the web as an automated update. The filter will decide if the incoming email is a SPAM email. Then the filter will prompt the user (the incoming message is subject to SPAM do you want to add to blacklist "Y/N"). If the user entered Y, the message will be blocked, and the email address will be added to the blacklist file. When another email is received from the same sender, the email message will be blocked. If the user entered N, then the message will pass through to the INBOX, and the email address will be added to the whitelist file.

If the spamicity value is less than 0.5, the message containing the word is likely to be HAM. This is achieved by checking the words against a text file of HAM words (non- suspicious words) called (ham.txt), which is customized by the user. Thus, the user will be prompted with the message (the incoming message is subject to HAM do you want to add to whitelist "Y/N"). If the user entered Y, then the message will pass through to the INBOX, and the email address will be added to the whitelist. The whitelist is a text file for the legitimate email addresses called (whitelist.txt), and it will store the incoming legitimate email addresses. If another email is received from the same email address, it will go directly to the inbox.

CONCLUSION

SPAM is not an easy problem to solve. SPAM has become very popular due to a variety of reasons. Unscrupulous companies and individuals can reap high rewards from unsuspecting victims without having a high ingoing and ongoing investment cost. The most commonly used method for stopping SPAM in use today is the deployment of SPAM filters [Le Zhang, 2004]. SPAM filters use a variety of methods to detect SPAM. However, this research has shown that the Bayesian method, in combination with blacklist and whitelist filters, is most effective in dealing with SPAM. The other two commercial SPAM filters (*EmailProtect© and SpamEater©*) are not based on the Bayesian method; however they do incorporate black or white filters and a number of other methods.

REFERENCE

1. ACMA (2005a). "MULTILATERAL MEMORANDUM OF UNDERSTANDING ON COOPERATION IN COUNTERING SPAM". Retrieved 6 March 2006, from http://www.acma.gov.au/acmainterwr/consumer_info/spam/spam- multilateral mouseoul. melbourne-finalwebversion.rtf.
2. ACMA (2005b). "Recent ACMA Compliance Activities". Retrieved 3 Febuary 2006, from. http://www.acma.gov.au/ACMAINTER.65640: STANDARD:: pc=PC_2974.
3. ACMA (2005c). "Racing tips company fined for breach of Spam Act". Retrieved 2 Febuary 2006, from http://www.acma.gov.au/ACMAINTER.131174: STANDARD::pc=PC_100121.

4. January 2004, from http://media.aoltimewarner.com/media/newmedia /cb_press_view.cfm?release_num=55253692.
5. APEC (2004). "Australia's Role in Combating SPAM". Retrieved 13 July 2005, from http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN 016410.pdf
6. ARPANET (2006). "Online Encyclopedia". Retrieved 5 January 2006, from http://www.webopedia.com/TERM/A/ARPANET.html.
7. ContentWatch (2005). "ContentWatch™ Products". Retrieved 21 November 2005, from http://www.contentwatch.com/products/emailprotect.php.
8. COTSE (2004). "Email Filters: Overview". Retrieved 20 February 2005, from http://www.cotse.net/emailfilters.html.
9. DCITA (2005). "Spam Act Review". Retrieved 11 April 2005, from http://www.dcita.gov.au/ie/spam_home/spam_act_review.
10. Emailuniverse (2004). "Drugs, Degrees and Smut Top AOL Spam List". Retrieved 31 July 2005, from http://emailuniverse.com/list-news/?id=973.
11. ExpressionEngine (2005). "Blacklist/Whitelist Module". Retrieved 31 Decmber 2005, from http://eedocs.pmachine.com/modules/blacklist/#whitelist.
12. Falk, E. (2000). "Spam glossary". Retrieved 10 March 2004, from http://www. rahul.net/falk/glossary.html#spam.