I.J. Education and Management Engineering, **2013, 2, 66-71**
Published Online February 2013 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijeme.2013.02.11

Available online at http://www.mecs-press.net/ijeme

Collaborative Spam Mail Filtering Model Design

Zhiyi Liu[a1], Rui Chang[a]

[a] *School of Information & Engineering, Changzhou Institute of Technology CZU Changzhou, China*

Abstract

This thesis analyzes the characteristic and regulation of anti-spam technologies. Based of these facts, this paper brings forward a collaborative anti-spam filtering model for E-mail. Our system not only defends the repeated spam mails at the router layer but also has a higher accuracy than Spam Assassin. Presents the structure of the model and give some necessary sketch maps. Explicates carefully our idea of the design and many technologies related to the model and discusses especially many key-points too. Finally, we give the experiment results.

Index Terms: Spam; intelligent detection; multiplayer filter; mail digest

1. INTRODUCTION

The proliferation of spam has become a major threat to the Internet, in addition to commercial messages, some malicious information such as phishing, online fraud, pornography and malicious programs are spread through spam. Spam for individuals, organizations and society has a significant impact, so intelligent analysis of spam and automatic filtering system of network security have become a hot research field, it has very important significance.

2. Status of spam filtering technology

Filtering spam is the imitation of human beings to judge the logic of thinking, usually aimed at the characteristics of the message or content analysis, combined with statistical or machine learning mechanism to determine whether the message is spam. There are many spam filtering techniques are proposed, a common spam filtering mechanisms can be classified Rule Base, Heuristic analysis, Context Base, etc. These class methods usually take e-mail headers, subject, content, style and features as a basis for filtering.

* Corresponding author.
E-mail address: [1]liuzy@czu.cn

A. Rule base

Such methods are simple rule conditions through the mail filtering, common methods are: White-lists/Black-lists, Basic Structured Text Filter and so on. Black and white list filtering uses in the case of already known sender's email address or domains, and later by this mechanism system, various security vendors gradually evolved into real-time updates to the blacklist mechanism (RBL). Basic structure text filter is similar with black and white list filtering, the difference is black and white judgments based on the list of e-mail address and domain, and the basic structure text filtering method is based on message content to determine, if the message content is same with user settings the key word, the letters will be filtered out. Most of the current e-mail software, such as: Outlook, FoxMail or the network e-mail (WebMail) offer this feature, which is the most easy filtering to use. Unfortunately, message rules must be manually set, can not be automatically updated, difficult to modify, spam is usually just change the message or change the header text, you can easily break through the filter block, it is the biggest drawback of this approach.

B. Heuristic analysis

To solve the shortcomings that the e-mail rules can not automatically update, scholars have proposed heuristic rules analysis, can automatically summarize the apparent regularity of spam and automatically generated e-mail rules. Doing mail filtering, the system will check the message contains the number of compliance with the rules of the project, and according to the way of mail rules, system score points, at last account the mount of the points. If the score exceeds the threshold, is to determine the message as spam. Heuristic analysis common methods include: Ripper, Boosting, the other also with the decision tree method of automatically generated e-mail rules. The most famous heuristic analysis filter is the SpamAssassin. In the past studies, the accuracy of heuristic rules is up to 98%, but its main drawback as the training is too slow, the average training time is the Bayesian classifier 15 to 20 times which is the obvious problem of the poor efficiency.

C. Context Base

Filtration method of content analysis is derived from the document classification technology; the goal is to divide e-mail spam messages into two categories. The method takes use of email context as characteristic value source, firstly extract the independent words, with a variety of statistical methods and document classify techniques to filter characteristic values, such as: TF-IDF and Mutual Information, Information Gain or Chi-squared etc. to select the higher identification degree independence words as the important characteristics, at last take the important feature of these values into the classifier training, the new classifier learn how to judge whether the message is spam.

There are some common classifiers such as Bayesian Filter, Support Vector Machines, SVM, and Clustering as the classifier approach. In the current use of classifier with filtration, Bayesian classifier is the most widely used with easy and good efficiency filtration.

3. CSFS

A. Module main structure

Collaborative spam filtering system (CSFS) designed to run on the gateway location is a system working in the routing level. CSFS received the mail from honey pots and Internet mail, using filters to remove spam, and then forwarded legitimate e-mail to the internal mail server. CSFS has four major spam filtering module, followed by e-mail honey pot, policy filtering module, the message digests match module, Spam Assassin filter. Fig. 1 shows the overall structure of the CSFS.

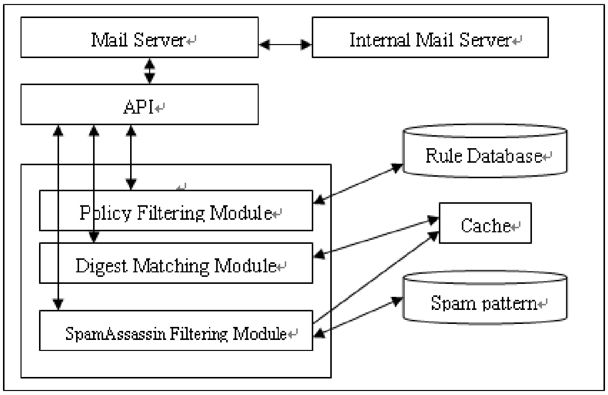

Figure 1. CSFS

When the message first arrived CSFS system, it will first be handled by the policy filter module, and then followed by the message digests match module and SpamAssassin filter. If the message in the white list, it will immediately be forwarded to the internal mail server. Other mail must be filtered through these three modules analysis. If there is a module to determine the message spam, it will make its marked on the subject line, and the remaining filtering module does not require treatment. Fig. 2 shows the message in the CSFS processes within the system.

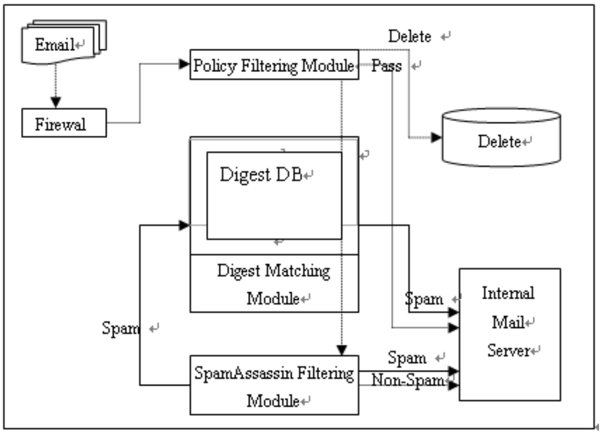

Figure 2. CSFS processes

B. Mail Honey Pot

Mail honey pot is a specialized collection of spam e-mail server. According to Dr. Guido Schryen study, know that spammers more concerned area, thus creating a group dedicated account to receiving junk e-mail and publish them to a specific page. These accounts just used to receive spam, never to contact others. Therefore, normal users e-mail will not be sent to the mailbox.

Overall, e-mail honey pot received e-mail from the Internet will be in different folders based on the message destination address. Mail honey pot only has two folders: "Spam" folder and the "unknown type" folder. Fig. 2 illustrates the process of the module how to handle mail. At the beginning when design account, we will take part of the account for the collection of pornography, mail fraud and gambling. Destination addresses same as these accounts will directly be identified as spam into "spam" folder, rather than go through manual or machine verification. The types of messages need to determine by hand or machine that are stored in "unknown type" folder. Eventually, the junk mail folder contains only spam, but "unknown type" folder contains spam and non-spam.

In the virtual account created, there are two special e-mail accounts, are called "EH.spam" and "EH.unknown". Mail honey pot will use them to forward "spam" folder and the "unknown type" folder e-mail to CSFS system for further processing. If you send a "spam" mail folder, use "EH.spam", the opposite is to use "EH.unknown". When the CSFS receive mail, policy filtering module will examine the message source address. If it is "EH.spam", summary of the message is calculated and stored in the database. If it is "EH.unknown", the message will be forwarded to the SpamAssassin filtering module.

C. Policy module

Policy filtering module is the first line of CSFS defense system, which work according to the information provided in SMTP session. The module has the following tasks:

- According to the white and black lists information, compare e-mail address: policy filtering module will first see the sender's IP address and the sender and the recipient's email address. Because CSFS will also receive the message forwarded from the honey pot system, it is very important to decide email the source. If the message is from the e-mail honey pot, then the CSFS system will not waste any time to check the relevant content. Match the white list messages will be forwarded to internal mail server, and match the blacklist matching messages will be deleted.
- Confirm the IP address: Policy filter module is also checking the DNS where it is connected from, and compare with real-time blacklist. If the record does not exist or are listed on the RBL, CSFS system will end the connection and sends a wrong message to the sender.
- Confirm the HELO | EHLO parameters: also verified HELO | EHLO parameter. If the argument is not correct, CSFS system will send an error report to the sending machine and close the connection.
- Confirm the identity of the letter sender: Policy filtering module to check the DNS MX records or A records, then it will connect the original mail server in order to check the validity of the sender mailbox. Secondly, it also checks whether the sender with a false name. Once there is a problem, CSFS system will stop processing and send a wrong message to the sender.

If a message has no problem in the IP address, email address, SMTP protocol parameters and the message envelope, then the message will be sent to CSFS system of digest match module for further processing.

D. Digest Match module

Digests match module system will process the spam which is submitted by trap module and spamAssassin filter module to calculate the message digest and stored in the database. Comparing suspicious mail digests and spam e-mail database can determine whether the message is spam.

To ensure the CSFS system can identify spam variant, using a local sensitive digest generated algorithms, message digest generation algorithm that should be able to guarantee the same or similar messages can produce the same or similar digest. Nilsimsa digest generation algorithm is a kind of local sensitive generation algorithm; it takes a document or a string as input and generates a text digest of n bits. E. Damiani in the article discussed Nilsimsa digest generation algorithm robustness issues. Article classified four kind of senders who attack against Nilsimsa algorithm, namely ① random increase (in the original message to add a random string); ② Dictionary replaced (in the original message some words are replaced by synonyms); ③ the same meaning replaced (without changing the meaning of the premise of the message, replace some words); ④ algorithm attacks (by increasing the message behind the characters change some particular barrel values). For these 4 attacks, E. Damiani tested Nilsimsa digest generation algorithm by experiment, get a satisfactory conclusion, Nilsimsa algorithm has better anti-attack.

Over time, new spam will continue to appear, CSFS system stored and managed spam Nilsimsa digest will continue to increase, leading to take up a lot of storage space and impact the matching digest time. If you do not use Nilsimsa digest elimination mechanism, CSFS system will too large and collapse because of too heavy storage and management for the Nilsimsa digest. Here we use literature [2,4] proposed the time-out mechanism, specific practices are as follows: Suppose spam Nilsimsa digest life cycle is T0-day. Meanwhile, in order to deal with spam which life cycle is greater than T0, CSFS system uses life cycle growth strategy in the life. Under this program, the minimum life cycle of spam Nilsimsa digest is T0-day, when a new message Nilsimsa digest is matching with spam Nilsimsa digest database, it will increase ∆T days in the life cycle to the corresponding to digest of spam Nilsimsa life cycle. If the spam Nilsimsa digest has not been hit on the last day, then the Nilsimsa digest will be eliminated from the CSFS system.

E. SpamAssassin

SpamAssassin is a mail server installed on Bayesian filtering technology-based mail filter. It is using a large number of the default rule to check spam; these rules will check all the messages header, text, and the sender which are sent to the serve. It takes the point's filtration that will give point according to the standard of the system, if the point is more than the threshold, it will be spam. Spam Assassin filtering module process is in Table 1.

TABLE I. SPAMASSASSIN PROCESS

Event	**Process**
Spam	Mark the subject
	Send mail to internal sever
	copy the mail and send it to digest match module
Non-spam	Send mail to internal sever

We used SpamAssassin as a spam filter in CSFS system, because SpamAssassin has the following advantages: (a) SpamAssassin uses a lot of different types of rules and weight to determine the spam, the rules have already been proven will be given higher weight to distinguish spam and non-spam. (b) In addition SpamAssassin own rules, it also allows the user to modify the weights of existing rules or define your own decision rules. (c) SpamAssassin is suitable for a variety of e-mail system environments, to quickly identify messages sources, or identify new spam categories. (d) SpamAssassin is a free software, which is based on GNU Public License or Perl AL for distribution. Both licenses allow users to freely distribute the software to modify and enforce the same distribution of its license to distribute the changes again.

4. Experimental results analysis

Experimental samples are the collections of 1000 mail; consist of 300 spam and legitimate e-mail 400, 300 copies of the original spam. Purpose of the experiment is to compare system accuracy and time-consuming with spamAssassin and the CSFS filtering on the mail server. Experimental results show the spam filtering system to achieve high accuracy, mainly due to systems integrate a variety of spam filtering technology.

TABLE II. RESULTS WITH SPAMASSASSIN

Training data	**500non-spam，800 spam**
Testing data	1000 mail
Accuracy	89.67%
Run time	396s

TABLE III. RESULTS WITH（CSFS）

Testing data	**1000 mails**
Run time	396+12s
Accuracy	94.57%

5. Conclusions

Currently, the high volume of spam, and the trend is increasing year by year. This takes significant loss for the e-mail user, mail service providers and the community, also contributed to the spam filtering technology to appear and continue to develop. Based on the study a variety of spam filtering technology, single spam filter is mostly only for certain aspect of e-mail filter, resulting in one-sidedness mail filtering in existence. This paper presents a model of collaborative spam filtering CSFS, the model used in combination with a variety of filtering techniques to detect spam, which is a manifestation of knowledge sharing thoughts, and the system model has an open framework for the continued phase-out outdate e-mail filtering technology and the introduction of new, excellent spam filtering technology.

Each module of CSFS filtration systems completes independently a specific function, they communicate with each other, collaborate with each other, at all levels take use of the advantages of technology spam filtering, but there is still some need for improvement, such as (1) It can be add an anti-virus module for CSFS system to detect virus-infected e-mail, so CSFS system can not only filter spam but also to detect the infected mail. (2) The current CSFS system filter mails in English, it can consider increasing the ability to filter messages in Chinese in future.

References

[1] J.jun, E.si. An Empirical Study of Spam Traffic and the Use of DNS Black Lists. Proceeding of the 4th ACM SIGCOMM Conference on Internet Measurement, Tarmina, Italy,2004, pp. 370-375.

[2] Androutsopoulos, I., G. Paliouras and E. Michelakis, “Learning to Filter Unsolicited Commercial E-Mail,” Technical report of National Centre for Sensor Research, 2004.

[3] SpamAssassin, “Tests Performed: v3.2.x,” The Apache SpamAssassin Project, 2008.

[4] http://spamassassin.apache.org/tests_3_2_x.html.

[5] Tran, Q. A., H. Duan and X. Li, “Real-time statistical rules for spam detection,” International Journal of Computer Science and Network Security (IJCSNS), Vol. 6, No.2, pp.178-184, 2006.

[6] Lai, C., “ An Empirical Study of Three Machine Learning Methods for Spam Filtering,” Knowledge-Based System, Vol. 20, No. 3, pp. 249-254, 2007.

[7] Blanzieri, E. and A. Bryl, “Evaluation of the Highest Probability SVM Nearest Neighbor Classifier with Variable Relative Error Cost,” Proceedings of Conference on Email and Anti-Spam (CEAS), 2007.

[8] Nilsimsa． http://ixazon.dynip.corn/~cmeclax/nilsimsa.html.

[9] E Damiani,S De Capitani di Vimercati, S Paraboschi et a1. An open digest-based technique for spam detection. In proceedings of the 2004 International Workshop on Security in Parallel and Distributed Systems. San Francisco, CA, USA, September 2004.

How to cite this paper: hiyi Liu,Rui Chang,"Collaborative Spam Mail Filtering Model Design", IJEME, vol.3, no.2, pp.66-71, 2013.