An Anti-Spam Engine using Fuzzy Logic with Enhanced Performance Tuning

Vijayan R
Assistant Professor (Senior),
School of Information
Technology and Engineering,
VIT University, Vellore 632014,
Tamil Nadu, India

Viknesh S T G M
M.S. in Software Engineering,
School of Information
Technology and Engineering,
VIT University, Vellore 632014,
Tamil Nadu, India

Subhashini S
M.S. in Software Engineering,
School of Information
Technology and Engineering,
VIT University, Vellore 632014,
Tamil Nadu, India

ABSTRACT

E-mail has been considered as one of the most primary communication channels among the users with the rapid extension of internet. Unfortunately e-mail is also one of those tools, if not used properly could bring in irreparable consequences.

But, recently the increasing popularity and fewer cost of sending an email makes it very easy to send unsolicited messages blindly to thousands of people at no cost at all by using easily available bulk mailing software and large lists of e-mail addresses typically harvested, even purchased or rented from web pages and news group archives.

The Anti-Spam SMTP Proxy (ASSP) mail server engine is preferred one of the best from all the existing Mail filters as it is a platform independent open source-filtering engine and its file size is 565.5KB, which much less compared to other mail filters.

General Terms

Spam, Web security, Mail Filtering engine, Threshold analysis, Fuzzy logic, MTA

Keywords

fuzzy spam filter, fuzzy logic spam engine, assp with fuzzy, anti-spam engine, spam engine performance tuning, MTA comparison

1. INTRODUCTION

E-mail has been considered as one of the most primary communication channels among the users with the rapid extension of internet. Unfortunately e-mail is also one of those tools, if not used properly could bring in irreparable consequences.

But, recently the increasing popularity and fewer cost of sending an email makes it very easy to send unsolicited messages blindly to thousands of people at no cost at all by using easily available bulk mailing software and large lists of e-mail addresses typically harvested, even purchased or rented from web pages and news group archives.

The Anti-Spam SMTP Proxy (ASSP) mail server engine is preferred one of the best from all the existing Mail filters as it is a platform independent open source-filtering engine and its file size is 565.5KB, which much less compared to other mail filters.

2. CURRENT SCENARIO

A multiple mail filtering engines are available worldwide at heavy cost and most are apt for a particular platform. Mail filtering engines like SPAMfighter, Cloudmark DesktopOne, MailWasher, ChoiceMailOne are noteworthy and efficient. But, they are available at greater prices. The features [11] that each engine provides vary accordingly. But, the world is moving to open source and people rely on it.

The Anti-Spam SMTP Proxy is a mail-filtering engine invented by John Hanna and developed by Fritz Borgstedt that works in the server side keeping track of the incoming mail and the mails are transferred towards the recipient via internet. It blocks the spam that passes via the engine and protects the user, free from spam and virus mails flooding into the inboxes and prevents the wastage of bandwidth.

It is an Open Source platform independent SMTP Proxy server, which was developed in PERL script and with an ease GUI monitoring and reporting tools [10] to the user. It can integrate with any kind of MTA that are available based on the user's preference. It starts with network setup proceeding to address segregation and finally detects the presence of spam and processes the ham mails to the client.

3. EXISTING METHODOLOGY: BAYESIAN FILTERING ALGORITHM

The Anti-Spam SMTP Proxy server uses three complementary strategies [10] to allow good mail and to block unsolicited email. They are:

- Whitelisting
- Spam Buckets
- Bayesian Filtering

Addresses listed in the Whitelist are readily granted access. Addresses listed in Spam Buckets are denied access. The Anti-Spam SMTP Proxy uses the Bayesian filtering technique, considered the most advanced form of content-based filtering, employ the laws of mathematical probability to determine which messages are legitimate and which are spam. In Bayesian filtering technique to effectively block spam, the end user must initially "train" it by manually flagging each message as either junk or legitimate. Overtime, the filter takes words and phrases found in legitimate emails and adds them to a list; it does the same with terms present in spam. To determine which incoming messages are classified as spam, the Bayesian filtering technique scans the contents of the email and then compares text against its two-word lists to calculate the probability that the message is spam.

3.1 Abbreviations and Acronyms

Term	Definition
ASSP	Anti-Spam SMTP Proxy
MTA	Mail Transfer Agent
DNS	Domain Name Server

3.2 Drawbacks in Existing Engine

- The existing engine does not support better attachment spam identification.
- No image, audio or video spam [3, 4] detection.
- The Bayesian Algorithm analysis needs to be more accurate.

Drawbacks in Bayesian Filtering

- Does not analyze a single line that would redirect to another URL.
- Delay in initial training and responding to messages built on unknown vocabularies.
- Does not analyze noise and image content.
- Bayesian poisoning.

4. ENGINE ARCHITECTURE

The architecture preferred for this engine is Client-Server architecture.

4.1 Server Side

The filtering engine retrieves the incoming mail from the internet. An incoming mail need to undergo various analysis steps to identify itself as a ham as shown in Fig 1.

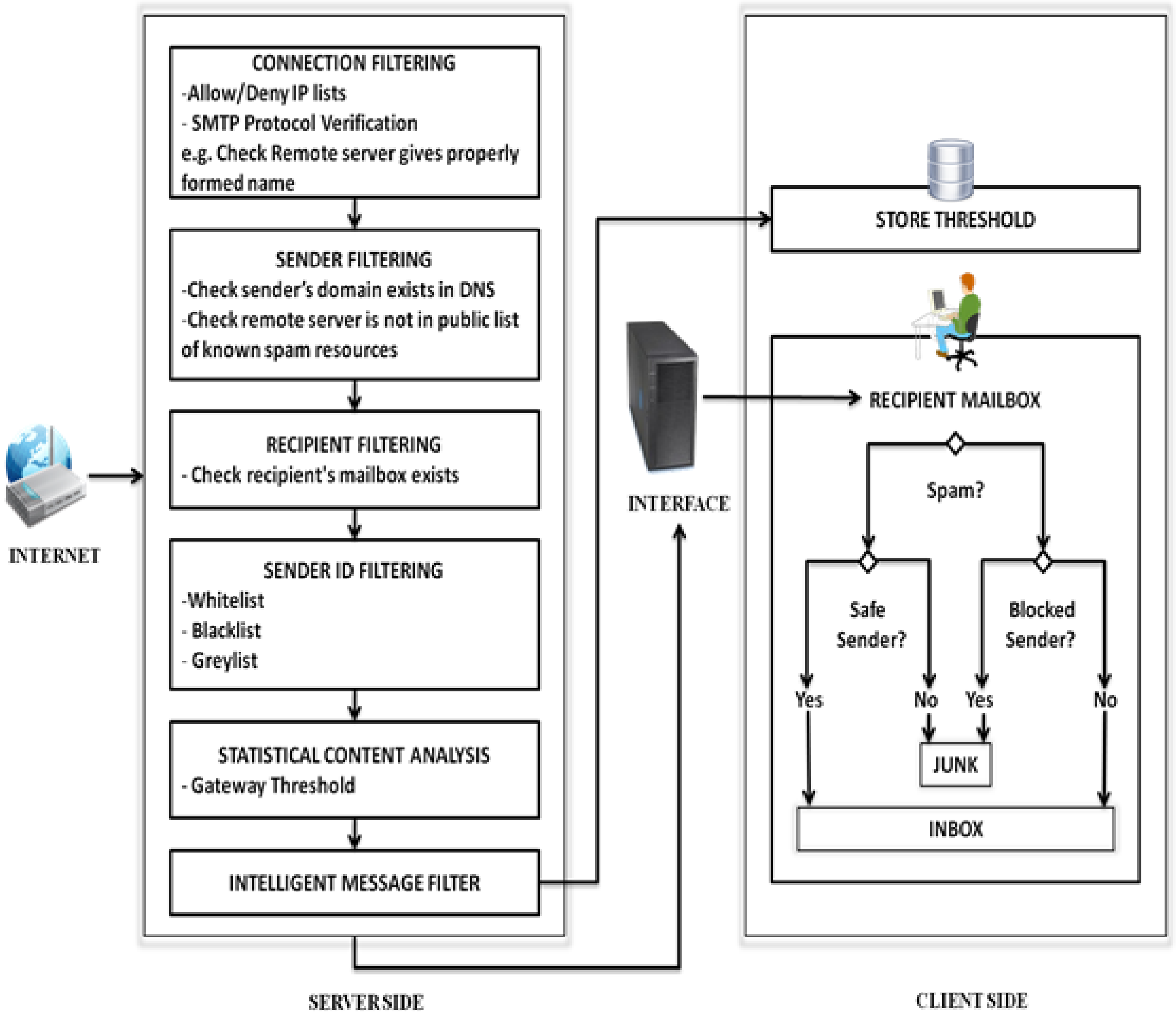
CONNECTION FILTERING
-Allow/Deny IP lists
- SMTP Protocol Verification
e.g. Check Remote server gives properly formed name
SENDER FILTERING
-Check sender's domain exists in DNS
-Check remote server is not in public list of known spam resources
RECIPIENT FILTERING
- Check recipient's mailbox exists
SENDER ID FILTERING
-Whitelist
- Blacklist
- Greylist
STATISTICAL CONTENT ANALYSIS
- Gateway Threshold
INTELLIGENT MESSAGE FILTER
INTERNET
INTERFACE
STORE THRESHOLD
RECIPIENT MAILBOX
Spam?
Safe Sender?
Blocked Sender?
Yes
No
Yes
No
JUNK
INBOX
SERVER SIDE
CLIENT SIDE

Fig 1: System Architecture

Firstly, the incoming mail connection is verified for its validity against various IP lists, Protocol verifications. Secondly, the incoming mail's sender is verified with the DNS. Thirdly the mail is checked with the validity of the recipient i.e. whether the recipient exists in the domain or not. Fourthly, the blacklisting, whitelisting and greylisting of the mail with the corresponding recipient is verified. Fifthly, the content of the mail is read and a threshold value is set for each token identified. Finally the tokens are verified using various statistical techniques using Bayesian mail filtering algorithm and Fuzzy logic algorithm and the mail is declared to be a spam or not and are stored in the spam database of the client.

4.2 Interface

The mails are then transferred through a mail server to the corresponding domain and route them to the correct domain with a relay server.

4.3 Client Side

The intelligent filter will transfer the threshold values to the spam database of the client. In addition, the incoming mails from the MTA or the relay server are then transferred to the corresponding user and check for the user's database to separate the mail as spam and ham. The mails are verified against the sender's address and finally classified as spam and ham in the user's mailbox.

5. PROPOSED ENHANCEMENT OF ASSP

The new engine was implemented using the following strategies:

- Whitelisting
- Spam Buckets
- Attachment Scanning
- Fuzzy Logic Technique

The whitelisted addresses are readily granted access. Spam Bucket addresses are denied access. In addition to this, the proposed engine also uses a concept called Greylisting, which is the technique for temporarily rejecting messages from unknown sender mail server. If it is legitimate, the originating sender will try again after a delay, if sufficient time has elapsed, the email is accepted for processing.

The attachments that come with the mail is checked whether it comes under blocked extensions or allowed extensions. The allowed extensions are then verified for spam in images [3,4] by analyzing the features of the image i.e. size, aspect ratio, pixels and comparing them with the test spam instances, comparing the histogram of the image with the test histograms and also using OCR which is ineffective and time consuming. The video spam is detected by taking frames of video at certain time intervals and analyzing them with the same way as image spam.

In this instance of junk mails, since the mail body has little text information, [9] it provides insufficient hints to distinguish spam mails from legitimate mails. To address this problem, Fuzzy inference [7] method follow hyperlinks contained in the email body, fetch contents of a remote webpage and extract hints from both original email body and fetched web pages.

5.1 Fuzzy Evaluation

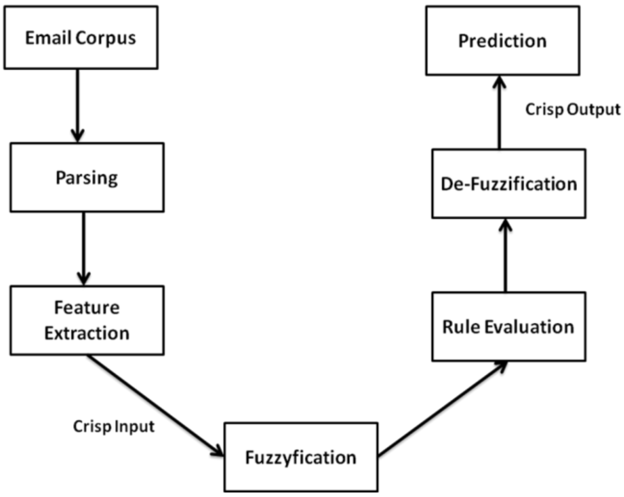

Fig. 2 Fuzzy Evaluation Process

- The message from the corpus is parsed and important features are extracted.
- The feature values are passed to the respective fuzzy sets for Fuzzyfication as shown in Fig 2.
- Based on the fuzzified input signals, a number of fuzzy rules are triggered in parallel with various values of firing strength.
- The rule outcomes are then aggregated, defuzzified, and based on the output a prediction was done.

In this instance of junk mails, since the mail body has little text information, it provides insufficient hints to distinguish spam mails from legitimate ones.

To address this problem, the fuzzy inference methods follow hyperlinks contained in the email body, fetch contents of a remote web page, and extract hints from both original email body and fetched web pages.

A two-phase approach is applied to filter spam in which definite hint is used first, and then less definite textual information is used.

5.2 Fuzzy Rule

IF A1 is Low AND A2 is Mid AND A3 is High AND A4 is High THEN B is Spam (1)

Where A1 to A5 are crisp inputs representing feature values then AND represents the fuzzy AND operation. All the outputs of the fuzzy rules are then combined with fuzzy OR operation which would be the input for Defuzzification.

6. IMPLEMENTATION

6.1 Algorithm for Identification of Image spam

```
Read file properties (image size, width, height, bit depth, aspect ratio)
Compare suspected file property with ham and spam feature database
Retrieve result
IF (result > threshold value)
    Declare spam
    Reject mail
    Notify database
ELSE
    Send to fuzzy filtering
ENDIF
```

6.2 Algorithm for Identification of Video spam

```
Collect multiple frames at various intervals randomly as images
Read each image property
Compare suspected file property with ham and spam feature database
Retrieve result
IF (result > threshold value)
    Declare spam
    Reject mail
    Notify database
ELSE
    Send to fuzzy filtering
ENDIF
```

6.3 Fuzzy clustering algorithm

```
Reads the content
Splits into definite (subject, address) hint and less definite (textual) hint
Reads subject and compare with existing database
Extracts feature
    Separate as tokens
    Forms fuzzy sets
    Applies fuzzy rule
    Declare spam or ham
    Notify database
```

7. RESULTS AND DISCUSSION

The initial ASSP engine is verified against the strategies that were to be implemented in the new engine. But the engine failed in all circumstances stating its insufficiency towards the dynamic changing criteria of spam behavior. Then the stable version of ASSP is taken and is modified based on the latest requirements that are needed in today's environment.

This engine was developed and implemented in an organization with users to check its working and performance. The engine was trained with the previously received mails and the features were extracted. Then the engine was made to analyze the inbound and outbound mails towards and from the organization for more than a month and finally a report was generated.

Table 1. Engine Performance Analysis

Summary	Today	Last Week	Last Month
Total Mails Received	1048	9692	37959
Total Mails Allowed	179 (17.08%)	3728 (38.46%)	10585 (27.89%)
Total Mails Blocked	869 (82.92%)	5964 (61.54%)	27374 (72.11%)

It was felt that the engine learns the behavior of the incoming mails and adapts itself to the new false positives and reduces the forwarding of spam mails accordingly. In addition, the incoming spam mails are much reduced than the existing engine.

The engine is then verified with invalid port numbers, invalid user name and invalid domain. The engine rejects them and displayed invalidity report accordingly.

Table 2. MTA Performance Analysis

Test Instance	Postfix (secs)	Qmail (secs)	Sendmail (secs)
30 recipients without attachment	0.03	0.03	0.03
30 recipients with attachment of size 5MB	0.32	0.33	0.35
30 recipients with attachment of size 10MB	2.25	2.47	2.92
10 recipients of mail size 15MB	3.12	3.18	3.23
20 recipients of mail size 15MB	4.57	4.61	4.7
30 recipients of mail size 15MB	5.25	5.3	5.38

By the analysis that was undergone with the MTAs listed, the paper suggests using Postfix as the best MTA among others and strongly recommends it to the users of ASSP. By using the best MTA, the performance of the engine will also increase as a whole.

8. CONCLUSION AND FUTURE WORK

The image and video spam are well detected and the existing Bayesian algorithm was replaced with a trainable fuzzy filtering mechanism for better attachment scanning and reduces Bayesian poisoning. From the analysis done based on the three MTA's namely Sendmail, Postfix and Qmail, it was felt that Postfix suits better with ASSP compared with any other MTAs to increase the performance of the server engine.

The ASSP Mailfilter engine is platform independent, free software licensed under the GPL. Since the entire paper completely relies on open source, future enhancements can be done easily with almost no cost except a little for maintenance.

The paper is successfully completed and implemented with all the basic needs and requirements that are described. In this paper, the proposed engine performs better functionality and a well-improved engine when compared to the existing engine. The engine described in the paper can further be enhanced in the future by adding a more additional features like audio spam detection, mails with only HTML in its body, multiple language detection, preventing spoofing and detecting spam in punycode.

9. REFERENCES

[1] Courname, A. and Hunt, R., "An Analysis of the Tools used for Generation and Prevention of Spam", Computer and Security, Vol.23, 2004, pp 154-166.

[2] "State of Spam", "A monthly Report", Report #33, September 2009.

[3] Peizhou He, Xiangming Wen and Wei Zheng, "A Simple Method for Filtering Image Spam", Eighth IEEE/ACIS International Conference on Computer and Information Science, 2009.

[4] Zhaoyang Qu, Yingjin Zhang "Filtering Image Spam using Image Semantics and Near-Duplicate Detection", Second International Conference Technology and Automation, 2009.

[5] Jong-Wan Kim, Sin-Jae Kang and Byeong Man Kim "A Fuzzy Inference Method for Spam-Mail Filtering", Springer-Verlag Berlin Heideberg 2005, LNAI 3809, pp 1112-1115.

[6] M. Muztaba Fuad, Debzani Deb, M. Shahriar Hossain "A Trainable Fuzzy Spam Detection System.

[7] Nozaki, K., Ishibushi, H. and Tanaka, H., "Trainable Fuzzy Classification Systems Based on Fuzzy If-Then-Else Rules", Proc IEEE vol-1, pp.498-502, 1994.

[8] Cox, E., "The Fuzzy System Handbook", Academic Press, 2nd Edition, 1999.

[9] Anti-Spam SMTP Proxy, http://assp.sourceforge.net

[10] Spam Filter Review http://spam-filter-review-toptenreviews.com.