IMPROVEMENT OF ANTI SPAM TECHNOLOGY WITH THE HELP OF AN ESTIMATION OF RELIABILITY OF THE SENDER

Saadat Nazirova

Institute of Information Technologies of ANAS, Baku, Azerbaijan, *saadatn@mail.ru*

There are a lot of technologies to filter spam. Technically the spam can be filtered in two basic ways - formal and linguistic methods.

1. Formal methods
   - List Based Filtration. List (black, white, RBL (Services RBL (Realtime Blackhole List) means of struggle against a spam. RBL service means presence of so-called bad IP addresses list, access to which is carried out in real time under DNS report. Using RBL post servers at the moment of reception of the next message request for service (or some RBL - services) about, whether is IP address of the mail sender bad, and either accept, or reject this mail on the basis of RBL reply;
   - Filtration based on formal attributes of the mail (absence of the address of the sender, absence or too big number of addressees, absence of IP addresses in the Internet DNS addresses system, etc., and also filtration based on a size and a format of the message);
2. Linguistic methods
   - Content Analyses of the mail (a word-combination, heuristics, and statistics).
   - Analyses of mails based on samples (recognition based on signature, voting, and so forth).

Each method has its own integrated parameters of quality. The percent of detected spam is a measure of completeness, a percent of false positives when not spam mails wrongly carry to a spam is a measure of discrepancy. It is possible to offer an integrated estimation of quality. Let's name it as a quality of a filtration. It is obvious, that at the accuracy close to 100%, quality will be approximately equal to completeness. It is impossible completely to be protected from spam while spammers constantly invent new ways of detour an anti spam products of leading manufacturers. On the other hand, at toughening methods of recognition and filtration the spam mails, the threat of false positives grows. Sometimes the portion of spam in mail boxes of users reaches 90 percent of the correspondence; besides by means of a spam dispatches it is distributed not only advertising but also viruses, tojans, worms and etc. Therefore, it is necessary to take into account two criteria choosing an anti spam product: false positives and true negatives. And the criterion of false positives is more important, as destruction of the important mails is much worse, than loss of time for manual sorting of mail.

As till now the ideal filtration method is not created, the decisions constructed on this or that technology cannot be considered effective. Today for achievement of a high level of a filtration and a low level of mistakes it is necessary to use all existing methods (fig. 1) [1, 2]. Quality of a filtration can be increased due to application of complex multilayered systems of the filtration, corresponding configuration of filters on each layer. It is possible to apply consistently the following filters [3, 4, 5]:

- The address of the mail sender is checked on conformity with FQDN (Fully Qualified Domain Name). This filter blocks about 10 - 15% of spam.
- Real time block lists checking: Block lists are DNS based lists. IP address of mail server which tries to send a mail on the specified server under black lists of known spammers is checked out. Such lists are available on www.spamhaus.org or ordb.org. About 1% - 3% of undesirable mails are blocked by these lists.
- The probability of spam is defined with the help of statistical analysis of Bayes.
- Mail sender's IP address comparison with DNS based blacklist. Whether IP address of the sender (mail server) is transformed into a domain name or not. Check the domain names

in the DNS to see if they are likely from dialup users, dynamically assigned addresses, or home-based broadband customers. Since the vast majority, but by no means all, of e-mail that originates from these computers is spam, many mail servers also refuse e-mail with missing or "generic" DNS names. A Forward Confirmed reverse DNS (FCrDNS) verification can create a form of authentication showing a valid relationship between the owner of a domain name and the owner of the server that has been given an IP address. While not very thorough, this validation is strong enough to often be used for white listing purposes, mainly because spammers and phishers usually can't pass verification for it when they use zombie computers to forge domains.

- Checking of HELO command: when two mail servers communicate with each other through Simple Mail Transfer Protocol (SMTP), they represent to each - other (for example, mail.azerın.com). At the start of all SMTP transactions, the calling machine identifies itself, literally by saying "HELO" with its computer name. Some spam distributing software doesn't do that. So this kind of checking blocks 1 - 5% of a spam.
- Detection of unknown servers: the name attribute of HELO command is checked on DNS on a subject is server registered or not. This method is rather effective, cause it blocks 70 - 80% of spam, but sometimes rejects the necessary mail as well.
- The content filtration provides filtration based on the attributes taken from a text part of messages (separate words and/or word-combinations). It analyzes the actual message contents (including the Subject header) and any attached files. With the help of linguistic algorithms based on a comparison with sample messages and a search for typical terms in the message (e.g., words and/or word combinations) characteristics of spam.
- Collective filtration: The work of the collective filter is based on processing of results of a filtration of messages in agents of the system of an adaptive filtration from undesirable dispatch [6].

It is necessary to note also, that the spam constantly varies, therefore it is necessary to use new, various and independent methods of recognition of undesirable mail.

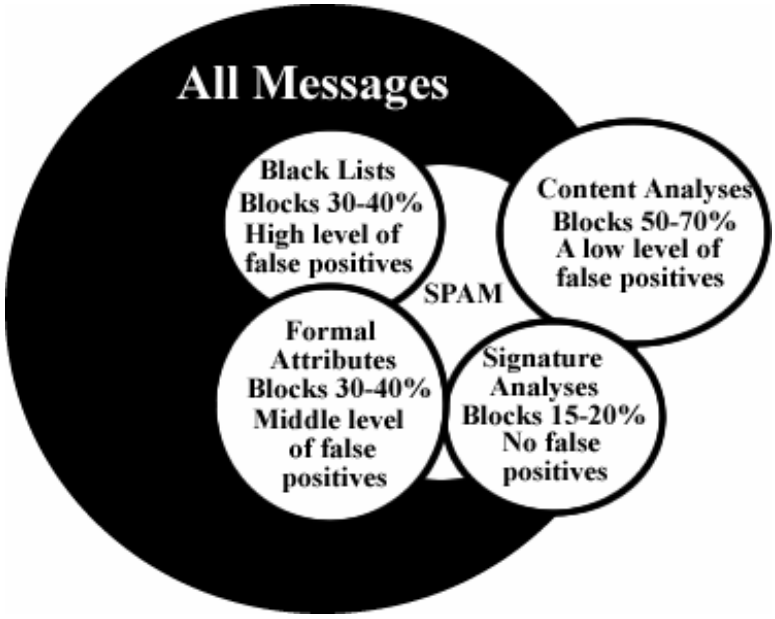

Fig.1. For achievement of a high level filtration and a low level of mistakes it is necessary to use various methods.

Therefore in the given thesis it is considered the decision, using a filtration on the basis of the whole complex of technologies and the constant analysis of a spam.

It is offered new filtration module for existing anti spam systems in order to achieve the best results in spam estimation and not loosing real correspondence along with spam. First of the suggested conditions verifies existence of the sender's mail addresses in Sent Items folder. This parameter will be conditionally named as Check On Sent (COS). The parameter COS receives value "1" or "0". If sender's mail address exists in a sheet of Sent Items folder, then $COS = 1$, hence, this mail automatically moves to Inbox folder, and is not filtered further. Otherwise $COS = 0$ and the mail will be passed to other subsequent of checking. This filtration condition allows minimizing high percent of false positives of anti spam filters.

The second condition is conducted on the basis of sender's mail address age. But before it is necessary to extend SMTP protocol which would allow to add a history of the address in HELO (changes are added in such a manner that the new version is compatible with the old one). Mail Server Providers should make possible to support new extended SMTP protocol that will allow to check the sender's mail address age. At present this parameter is not displayed in the existing protocol [7, 8, 9]. The extended new SMTP protocol will contain new command 250 - BDAY. The format of this command is the following: BDAY date/time

Here the date/time is the sender's mail account registration time. The suggested filter based on the following idea: As spammers automatically create new mail accounts, the age of such mail addresses will be in inverse proportion to probability of undesirable mails from this address. The parameter of the age of sender's mail account conditionally will be named as Age of Mail Account (AMA).

As Internet providers store mails for mail server, then with the command BDAY it is possible to get the age of mail account. There are some ways of realization of such algorithm. One of them is that after setting connection with Internet provider it gives out BDAY command with registration date and time of sender's mail account as an argument. Having received this command, SMTP server of provider calculates AMA:

$$\text{AMA} = \text{Current date/time} - \text{BDAY date/time}$$

After calculation the suggested module compares AMA with variable L. Where L is an average age of mails corresponding to period T_i ($T_i = [t_i, t_{i+1}]$) and $i = [1, m]$. L is defined as a result of training above non requested mails. The high number of non requested mails in Spam folder helps to define the value L more precisely.

Assume the number of non requested mails in Spam folder is N then

$$L = \frac{\sum_{i=1}^{m} T_i / K_i}{N * \sum_{i=1}^{m} K_i}.$$

Where K_i is a spamness coefficient of emails corresponding to the period T_i. K_i is in inverse proportion with T_i and it takes value from the interval $[0,1]$.

If $AMA < L$, then mail moves to folder Newbie. Assume that the folder Newbie is already created. Otherwise, i.e. if $AMA \geq L$ then this e mail passes to other nodes of filtration.

The given technique will allow to detect spam most effectively and to prevent false positives of spam filters. The uniqueness of the given method is provided with that application of conceptually new criteria of identification of a spam which were not used till now because of the existed SMTP protocol did not provide a field which would help with identification of a spam.

The suggested filtration model can be presented as the following:

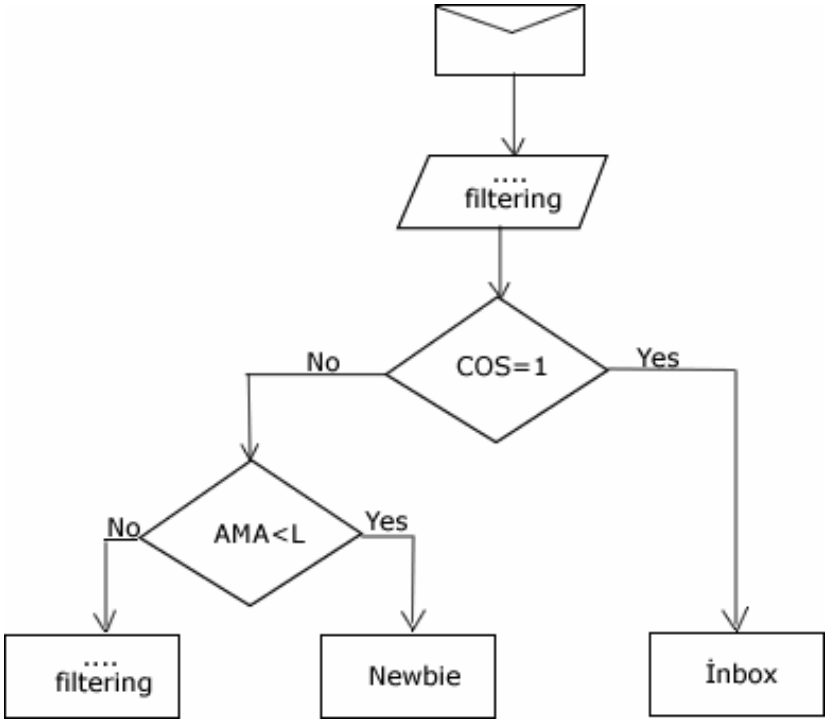

Fig.2. Algorithm of suggested module

Literature

1. Ilya Segalovich, Dmitriy Teyblum, Aleksandr Dilevskiy, "Principles and technical methods of work with the nonrequested correspondence", // Electronic magazine "Spamtest", (In Russian), 31.11.2003 www.spamtest.ru/document.html?context=15932&pubid=28
2. Alexandr Proxorov, "Domestic ant spam for the Domestic spam", // ComputerPress, Moscow, (In Russian), №10, 2005 www.compress.ru/article.aspx?id=14690&iid=696
3. Jhon Rhoton, "Programmer's guide to Internet Mail" / Digital Press, 1999, pg 291
4. Khramcov P. B. "Administration of a network and INTERNET services", (In Russian), http://www.citforum.ru/internet/services/index.shtml.htm
5. Khramcov P. B. "Organization and administration of Internet mail and file servers", (In Russian), http://www.citforum.ru/internet/servers/index.shtml
6. Aliguliyev R.M., Nazirova S.A. "Architecture of hierarchical intellectual nation-wide system of struggle against a spam", // "INFORMATION TECHNOLOGIES", Innovative Technologies, Moscow, (In Russian), №08, 2006, c. 32–36, http://www.informika.ru/text/magaz/it/2006/08/inftech.html#6
7. SMTP Authentication [Tutorial], 26.03.2008, www.fehcom.de/qmail/smtpauth.html
8. Semenov Y. A. "SMTP protocol of E-mail", (In Russian), http://book.itep.ru/4/44/smtp4414.htm
9. Masich G. F. Simple mail transfer protocol (SMTP), (In Russian), www.icmm.ru/~masich/win/lexion/mail/smtp.html