Communications and Network, **2011, 3, 153-160**
doi:10.4236/cn.2011.33019 Published Online August 2011 (http://www.SciRP.org/journal/cn)

Survey on Spam Filtering Techniques

Saadat Nazirova
Institute of Information Technology of Azerbaijan National Academy of Sciences, Baku, Azerbaijan
E-mail: *sbunyadova@gmail.com*
Received April 11, 2011; *revised May* 8, 2011; *accepted May* 15, 2011

Abstract

In the recent years spam became as a big problem of Internet and electronic communication. There developed a lot of techniques to fight them. In this paper the overview of existing e-mail spam filtering methods is given. The classification, evaluation, and comparison of traditional and learning-based methods are provided. Some personal anti-spam products are tested and compared. The statement for new approach in spam filtering technique is considered.

Keywords: E-mail Spam, Unsolicited Bulk Messages, Filtering, Traditional Methods, Learning-Based Methods, Classification

1. Introduction

Spam is the use of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately [1]. In this article it is considered the e-mail spam. E-mail spam, also known as junk e-mail or unsolicited bulk e-mail (UBE), is a subset of spam that involves nearly identical messages sent to numerous recipients by e-mail [2]. Day by day the amount of incoming spam increase and, scammer attacks are becoming targeted and consequently more of a threat. When targeted attacks first emerged five years ago, Symantec MessageLabs Intelligence tracked between one or two attacks per week. Subsequently, attacks have increased further from approximately 10 per day to approximately 60 per day in 2010 (**Figure 1**). By the end of 2010 MessageLabs Intelligence identified approximately 77 targeted attacks blocked each day [3].

By the Symantec MessageLab forecast spam will become more culturally and linguistically diverse, in 2011. The amount of spam sent from European countries will increase to 40% - 45% of all spam [3]. These facts state that spam is a big problem for today and for tomorrow and it actually makes sense to investigate new effective methods against spam.

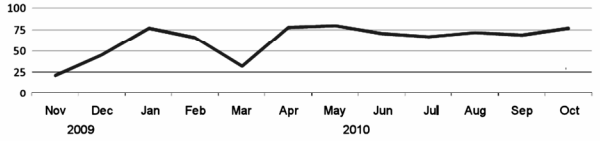

Figure 1. Targeted spam attacks 2009-2010 (Symantec. cloud Message Lab) [3].

2. Historical Review of Spam Filtering Methods

Though the first spam was sent in 1978 it began to be written about it as a problem in scientific literature only from 1982. One of the first papers where this problem is considered is the Peter J. Denning's article [4]. The first mathematical apparatus applied to spam filtering systems is the Bayes' algorithm, which was used first by Sahami et.al in 1996 and then by other researchers [5-8]. Bayes' classifier relies on famous Bayes theorem and the first papers about it could be met as early as 1960 [9]. During more than 40 year history Naive Bayes Classifier (NBC) was used for the solution of very different type of tasks: from classification of texts in news agencies till primary diagnosis of diseases in medicine. For the problems where NBC is applied there is usually selected presence or absence of words in the text as a characteristic, i.e. the set of characteristics T is a set off all words in documents. Hereby, if the word t_i is present, the weight of characteristics $w_i = 1$, otherwise $w_i = 0$. In case of e-mail filters where spam classification is used, there taken into account the area where the word had been met: heading, subject and body of the e-mail.

Beginning from the publication of Gary Robinson [10], in some filters (for example, Spam Assassin) there came to be used the method of overlapping probabilities sug-

gested by R. Fisher in 1950. For spam detection Robinson offered to calculate not only the probability of "spamness" of the document, but also the probability of "legitimness" of email. The next directions were application of Markov chain PageRank and Hidden Markov Model which are met in papers Paolo B., *et al.* [11], and José Gordillo, *et al.* [12]. Kolmogorov complexity estimation is met in papers Spracklin L.M., *et al.* [13]. Absolutely another approach is a new method of digital analysis of textual e-mails for spam detection which can be firstly observed in paper Korelov S. V., *et al.* [14]. Here e-mail is considered as a signal $x(n)$, after the methods of digital processing are applied to signals and the probability of false positives are defined for these methods. Application of methods of clustering analyses to the problem of filtering e-mails to legitimate and spam is considered in papers [15-18]. From 2009 year, beginning from Paulo Cortez's, *et al.* article [19] one can meet the statement as a Symbiotic Data Mining which is a hybrid of Collaborative Filtering (CF) and Content-Based Filtering (CBF).

Considering stunning amount of spam messages coming to e-mail boxes it is possible to assume that spammers operate not alone, there are global, organized, virtual social networks of spammers. They attack e-mails of not only users, eve whole corporations and countries. Spam is of the weapons of information war. In spite of the fact that, the terms spam and war appear in one context [20,21] since 2003 year, only from 2009 the problem of spammers' social networks are considered in scientific papers. Clustering of spammers considering them in groups is offered in paper Fulu Li, *et al.* [22]. In works Xu K.S., *et al.* [23,24] the method of spectral clustering is applied to the set of spam messages collected under project Honey Pot for defining and tracking of social networks of spammers.

They represent a social network of spammers as a graph the nods of which correspond to spammers, and a corner between two junctions of graph as social relations between spammers.

Research and development of spam filtering systems are actively carried all over the world. Along with scientific institutes there are many organizations and corporations investigating and offering different theoretical, practical and juridical approaches to spam filtering. Different organizations as university laboratories (laboratories CSAIL MIT in USA [25], Computer Laboratory Faculty University of Cambridge in UK [26] and etc.); research centers (NCSR Democritos in Greece [27], research centre of IBM [28,29] and etc.); commercial companies (Microsoft [30], Symantec [31], Kaspersky's Laboratory [32] and etc.) had been involved to this process. Many international organizations take great attention to concerned problem. It is created the ASRG (Anti-Spam Research Group) [33] within the organization IETF (Internet Engineering Task Force) [34] in 2003. A lot of international conferences, summits and symposiums dedicated to this topic recently (NIST Spam Technology Workshop USA 2004, ASRG Meeting USA 2003, Cambridge Spam Conference USA 2003-2005, Conference on Email and Anti-Spam (CEAS) Mountain View USA 2004-2005, Spam Forum Paris France 2003, Anti-Spam-Symposium Karlsruh Germany 2003, Spam Summit UK 2003, Conference on "Spam problem and its solution" Moscow and etc.) were held [35].

3. Classification of Spam-Filtering Methods

Depending on used techniques spam filtering methods are generally divided into two categories:

1) Methods to avoid spam distribution in their origins;
2) Methods to avoid spam at destination point.

Let's consider these methods in detailed form

3.1. Methods to Avoid Spam Distribution

Legislative measures limiting spam distribution, development of e-mail protocols using sender authentication, blocking mail servers which distribute spam are the methods which avoid spam distribution in origin.

Using these methods alone doesn't give considerable results. For example, there are many hard legislative restrictions for spam distribution in USA; nevertheless, the greatest amount of spam is distributed from this region. One of the reasons is an existence of high level broadband Internet access in USA. There is a number of the approaches, offering to make spam sending economically unprofitable. One of these statements is to make sending of each e-mail paid. The payment for one e-mail should be the extremely insignificant. In this case for the usual user it will be imperceptible. For spammers who send thousand and millions messages the cost of such mailing becomes considerable that makes it economically unprofitable.

This type of methods avoiding spam in their origins is a subject of author's another papers [36,37]. They should be implemented together with the methods described in the next section, which filter spam at the destination point.

3.2. Methods to Avoid Spam Receiving

Methods which filter spam in destination point can be divided into the following categories:

- Depending on used theoretical approaches: traditional, learning-based and hybrid methods;
- Depending on filtration area: server side, client side

and filtration in public mail-servers.

3.2.1. Classification of Spam Filtering Methods Depending on Theoretical Approaches

As we noted above depending on used theoretical approaches spam filtering methods are divided into traditional, learning-based and hybrid methods. In traditional methods the classification model or the data (rights, patterns, keywords, lists of IP addresses of servers), based on which messages are classified, is defined by expert. The data storage collected by experts is called as the knowledge base. There are also used trusted and mistrusted senders lists, which help to select legal mail. Actually it makes sense only creation of the "white" list, because spammers use fictitious e-mail addresses. This technique can't represent itself as a high-grade anti-spam filter, but can reduce considerably amount of false operations, being a part of e-mail filtration system based on other classification methods.

In learning-based methods the classification model is developed using Data Mining techniques. There are some problems from the point of view of data mining as changing of spam content with time, the proportion of spam to legitimate mail, insufficient amount of training data are characteristic for learning-based methods.

Traditional methods. Traditional methods are divided into the following categories:

1) *Methods based on analysis of messages.* The received e-mail is analyzed for specific signs of spam on the base of:

- formal signs;
- content using signature in updated database;
- content applying statistic methods based on Bayes theorem;
- content by means of use SURBL (Spam URL Real-time Block Lists) [38], when run search for located references in e-mail and their verification under base of SURBL. This method is effective if instead of advertisement, the reference of website with advertisement is located in e-mail.

2) *Detectors of mass distribution.* Their task is to detect distributions of similar e-mails to the bulk of users. The following methods are used for the detection:

- users' voting (Razor / Pyzor) [39,40];
- analysis of e-mails coming through mail system (DCC) [41];
- receipt of e-mail to the spam "trap" and its following analyses (implemented in Symantec Brightmail Anti-Spam) [42].

Independent from a way of bulk detection the idea of a method is that for spam filtration the calculated e-mail signature (the control sum) is used. For the methods based on detection of repetitions two vital issues are characteristic. The first is a spam "personification". This means that each spam e-mail has insignificant differences at the cost of which it is hard to collect steady signatures. To solve this problem the various steady signatures are used. For example, in Yandex Mail System the method of shingles [43] is realized. The second problem is a detection of legitimate bulk mailings.

3) *Methods based on acceptance of sender as a spammer*. These methods relies on different blackhole lists of IP and e-mail addresses. It is possible to apply own blackhole and white lists or to use RBL services (Real-time Blackhole List) and DNSBL (DNS-based Blackhole List) for address verification. Advantage of these methods is detection of spam in early step of mail receiving process. Disadvantage is that the policy of addition and deletion of addresses is not always transparent. Often the whole subnets belonging to providers get to the Black lists. For such systems it is actually impossible to estimate the level of false positives (the legitimate e-mail wrongly classified as spam) on real mail streams.

4) *Methods based on verification of sender's e-mail address and domain name*. This is the simplest method of filtration if DNS request's name is the same with the domain name of sender. But spammers can use real addresses, so that current method is ineffective. In this case it may be verified with possibility of sending the message from current IP address. Firstly, the Sender ID technology [44] can be used where sender's e-mail address is protected from falsification by means of publishing the policy of domain name use in DNS. Secondly, there can be used SPF (Sender Policy Framework) technology [45], where DNS protocol is used for verification of sender's e-mail address. The principle is that if domain's owner wants support SPF verification, then he adds special entry to DNS entry of his domain, where indicates the release of SPF and ranges of IP addresses from where may become an email from users of current domain.

5) *Method based on SMTP server response emulation.* If the real mail delivery systems, which follow the SMTP protocol correctly, observe such error, they get some interval (1 - 2 hours) and repeat attempt again [46]. But the majority of spam-bots has very short time out periods. So filters based on this method slow down the SMTP transaction to the point that some SPAM senders will fail but where real mail delivery systems will still continue and deliver mail successfully.

All above methods are based on some data for analysis collected by experts of third-party suppliers and same for all users. So that traditional method's has the following disadvantages:

- it is necessary to update the knowledge base regularly;

- there is a dependence on update suppliers;
- the security level is low;
- "impersonalized" model of classification doesn't consider individual specifics of user's correspondence;
- dependence on natural language of correspondence;
- low level of detection because of general models of classification.

Learning-based methods. Nowadays there is actively developed trainable or intellectual methods based on Data Mining algorithms for e-mail filtration. These algorithms divide the object to some categories using classification model previously defined on the base precedential information.

Assume spam filtration is defined by the function

$$f(m,\zeta) = \begin{cases} m_{spam}, \text{ if the message } m \text{ is considered as spam} \\ m_{leg}, \text{ if the message } m \text{ is considered as legitimate mail} \end{cases}$$

where m is a classified mail, ζ is a vector of parameters m_{spam} and m_{leg} are spam and legitimate e-mail.

Many spam filters based on classification using machine learning techniques. In learning-based methods the vector of parameters ζ is a result of classification trainings on previously collected e-mails.

$$\zeta = Z(M).$$
$$M = \{(m_1, y_1), (m_2, y_2), \cdots, (m_n, y_n)\},$$
$$y_i \in \{m_{spam}, m_{leg}\},$$

where $m_1, m_2, \cdots, m_n$ are previously collected messages, $y_1, y_2, \cdots, y_n$ are the corresponding labels and Z is the training function.

The following types are belonged to learning-based methods.

1) *Image-based spam filtering.* Image spam has become a new type of e-mail spam. Spammers embed the message into the image and then attach it to the mail. Some traditional methods based on analysis of text-based information do not work in this case. Image filtering process is costly and time-consuming work. In the paper [47] it is proposed three-layer (Mail Header Classifier, the Image Header Classifier and the Visual Feature Classifier) image-spam filtering. In the First layer it is applied Bayesian classifier and SVM classifier in the remaining layers. In paper [48] it is offered statistical feature extraction for classification of image-based spam using artificial neural networks. They consider statistical image feature histogram and mean value of block of image for image classification.

2) *Bag of words Model.* The bag-of-words model is a simplifying assumption used in natural language processing and information retrieval. In this model, a text (such as a sentence or a document) is represented as an unordered collection of words, disregarding grammar and even word order [49]. In spam filtering two bags of words are considered. One bag is filled with word found in spam e-mails, and the other bag is filled with words met in legitimate e-mails. Considering e-mail as a pile of words from one of these bags, there used Bayesian probability to determine to which bag this e-mail belongs. *k*-Nearest neighbor, SVM (Support Vector Mashine), boosting classifiers are also applicable to the bag of words.

3) *Collaborative spam filtering.* This is gathering spam reports between P2P users or from mail server (Google Gmail). The collaborative centralized spam filtration is more economic in comparison with personal approach, but only under condition of presence of adequate procedures of the analysis of false operations and operative reclassification of not correctly classified messages. In the papers [50-54] it is proposed such kind of multi-agent spam filtration and personalized collaborative spam filtering.

4) *Social networking against spam.* This is a one of the latest methods where the information extracted from social networks is used to fight spammers. For example, P.A. Chirita *et al.* [55] estimate the rank of users depending on their social network activities and trustworthy senders are ranked and classified as spam or non-spam. They call this algorithm as MailRank schema and show that it is highly resistant against spammer attacks, which obviously have to be considered right from the beginning in such an application scenario.

So in case of learning-based methods user defines the classification model himself, so that the majority disadvantages of traditional methods are solved successfully; intellectual methods are autonomous, independent on external knowledge base, doesn't require regular update, multilingual, independent of natural language, able to study new types of spam user-aided. There is advantage as construction of personalized mail classification model, where user himself defines which mail is legal or which one is a spam. Therefore learning-based methods have higher rank in spam determination. In many spam filtration systems based on the learning-based methods the Bayes' theorem, Marcov's chain and others are successfully applied. Learning-based methods have also a couple of disadvantages as overfitting, dependence on quality and compound of trainee set, resource-intensivety. Application of statistic algorithms with complicated mathematic calculations led to high loading of computing system's resources. For the spam filtering systems processing fair amount of requests the productivity of algorithm is a main importance, so resource-intensivety

factor is the most important disadvantage of learning-based methods.

Hybrid methods. One of the latest approaches in spam filtering is hybrid filtration system which is a combination of different algorithms, especially if they use unrelated features to produce a solution. In this case it can be applied various filtering techniques and get the advantages of the traditional and learning-based methods [56].

3.2.2. Classification of Spam Filtering Methods Depending on Filtration Scope

Depending on filtration scope spam filtration methods are divided into the following categories.

1) Client side/personal filters. Client side filters works directly on user's computer. In client side filtration e-mail loading to the user's local computer anyway, and only after that classified what leads to additional loading of data transfer in network. Client side spam filtration more accurately due to usage methods of machine learning. In client side filters users' personal information are used, in server side filters the filtration model is defined at once for all users. In spite of the fact that for the majority of users it is obvious what is spam, the concept of spam for each of them is enough personified. The e-mail message marked as spam by someone may be the important information for other one. From filtration quality point of view the personal model is the most preferable as characteristics of user's correspondence are considered. Generally, absence of personification reduces the level of detection and increases quantity of false positives. On the other hand, use of personal model of e-mail classification involves an inevitable overhead cost. Firstly the user should construct his personal model of filtration himself as only he can define what legal e-mail is, and what spam is for him. Secondly, construction, storage and use of personal model demands additional computing resources.

2) Server side/general filters. Server side filters work at mail server level. Generally in server side filtration systems the traditional methods of filtration are applied, but at client level the learning-based or hybrid one. Server side filtration also own priority. As centralized solution reduces expenses, simplifies support and control of this system. User becomes more mobile, so that it is comfortable to store mail centralized in server and to have an access to him from different points, using different devices. Hereby, classification at mail-server level more preferably and development of these methods more actual.

3) Spam filtering in public mail-servers. This solution sometimes is better than client or server solution. In this case users are mobile as in case of server side filtration, and personalized as in case of client side solution. But disadvantage of usage of public mail-servers is that users depend on filtration product installed there. For example, the mail-server of Google.Inc company gmail.com uses its own products against spam [57]. This system considers personal information about user to minimize false positives. The public mail provider Mail.ru uses Kaspersky Anti-Spam product based on "Spamtest" technology, and absolutely based on traditional filtration methods, as well RBL, the base of fuzzy signature of mails with spam, heuristics base. These knowledge bases are maintenanced and updated regularly till 3 times in an hour. Processing of attached files, detection of iterations is supported also. The system as a general model of classification applicable for all users, but at the same time personalization is absent.

4. Software Solutions for Spam Filtering

On basis of suggested theoretical approaches different companies develop hardware software solutions for spam filtering. In this paper it is given the result of testing of personal spam filters. Choosing anti-spam software it is necessary to compare:

- price;
- functionality and user-friendness;
- quality of spam detection.

Estimation of cost and functionality can be made by the company-manufacturer documentation. The quality of spam detection can be defined by the testing these products [58].

In this paper there seven freeware anti-spam software products are chosen for testing. Each soft is installed on Windows XP platform on different personal computers with POP3 mail server. The feature of our test environment was that for tested products the real post traffic was used.

Testing was made 14 days, and during this period 721 messages has been processed, 430 from which were spam. Learning-based filters were previously trained with 33 spam and 33 legitimate e-mails. The spam classification result of each software is represented in **Table 1**. The results of filtration were divided into four categories: false positive, true positive, true negative, false negative. The following parameters were calculated false positive percent (FPP)—the percent of legitimate e-mails detected as spam and the parameter false negative percent (FNP)—the percent of not detected spam e-mails.

It is better to get spam than to lose the legitimate e-mail with important information, so the low level of FPP is important than low level of FNP. The result of experiment shows that the lower values of FNP were in filters Qurb 3.0, Matador 1.0.0 and SpamArrow (**Figure 2**).

Table 1. Testing of different spam filtering software products.

Anti-spam software	FPP	FNP	FP	Detected		FN
				TP	TN	
Matador 1.0.0	4.9%	4.7%	35	410	256	256
SpamBrave	1.1%	7.0%	8	400	283	283
SpamArrow	2.5%	5.8%	18	405	273	273
Espresso 1.06.94	2.9%	20.9%	21	340	270	270
Spam Bully	2.1%	16.3%	15	360	276	276
Spam Fighter	1.9%	19.1%	14	348	277	277
Qurb 2.0	5.8%	2.3%	42	420	249	249

TH-True Negatives, TP-True Positives, FN-False Negatives, FP-False Positives.

And for the FPP the lower value were in filters Spam Brave, Spam Fighter and SpamArrow. The best effective between considered spam filtering software products is SpamArrow. Its efficiency is connected by that it is learning-based and it was trained previously. So for effective spam filtering it is necessary to install traditional filter before learning-based one to collect spam templates for previous training.

5. Conclusions

Summarizing above-listed, we obtain the following conclusions.

So, spammers constantly change external signs of e-mails to skip spam filtering systems, there arises a need for adaptive filtering system, which should have the ability to react quickly to the changes and provide fast and qualitative self-tuning in accordance with a new set of features.

Since the filters are trained on a very limited number of messages that come only to a specific user or a specific mail provider, the quality of filtration in the existing client and server filtering systems is rather low. But it can be improved if to apply the hybrid filtration system in other words the complex hierarchical and multi-agent filtration system that helps users to participate in the identification of the filtering errors and the appropriate setting of filters at each level (user level, organization level, mail provider level).

Therefore it is quite perspective for solving this problem, the combination of two widespread approaches as using the personal e-mail classification model on a server side solution. Development of server side personalized e-mail filtering systems that use the learning-based classification algorithms based on Data Mining methods is a very perspective direction.

This statement is supported by the followings:

- personalized server side filtering systems are preferable than the client side solutions, because provide universal access to an e-mail, reduce expenses, which is very important for corporate users;
- personalized server side filtering systems are more preferably because of greater accuracy and fewer errors in comparison with general model;
- personalized server side filtering system offered in author's another paper [59] bases on the Universal Declaration of Human Rights and has a universal character, can be applied in all countries;

learning-based algorithms used in personalized server side filtering systems exceed traditional ones because of a number of fundamental qualities (quality of filtering, the absence of updates, autonomy, independence from external knowledge bases).

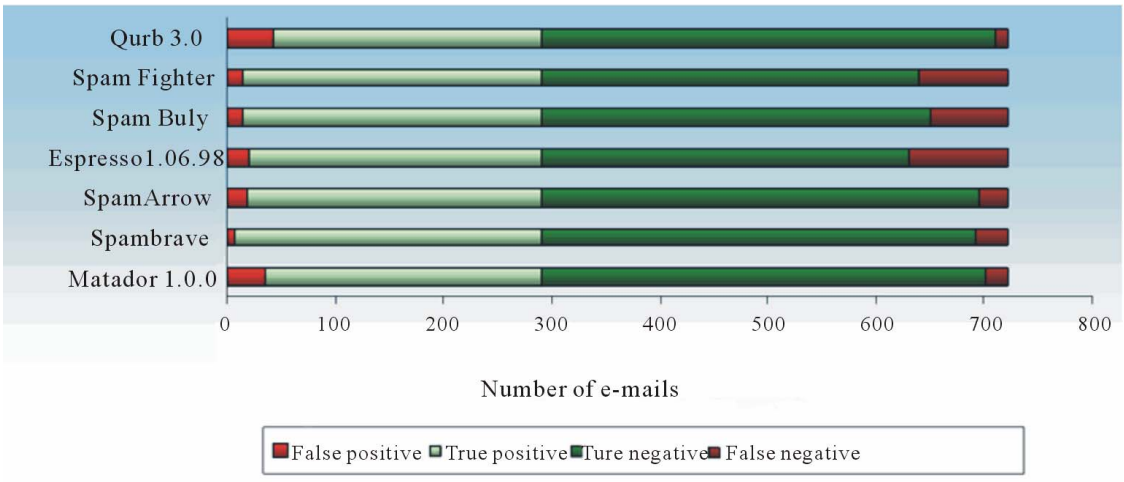

Figure 2. Spam filtering software products testing diagram.

6. Acknowledgements

I would like to give my sincere thanks to Dr. Rasim Alguliev and Dr. Ramiz Aliguliyev for their ideas.

7. References

[1] Wikipedia, "Spam". http://en.wikipedia.org/wiki/Spam_(electronic)

[2] Wikipedia, "E-mail spam". http://en.wikipedia.org/wiki/E-mail_spam

[3] Symantec, "State of Spam and Phishing. A Monthly Report 2010," 2010. http://symantec.com/content/en/us/enterprise/other_rsources/b-state_of_spam_and_phishing_report_09-2010.en-us.pdf.

[4] J. P. Denning, "ACM President's Letter: Electronic Junk," *Communications of the ACM*, Vol. 25, No. 3, March 1982, pp. 163-165. doi:10.1145/358453.358454

[5] M. Sahami, "Learning Limited Dependence Bayesian Classifiers," *Proceedings of the Second International Conference on Knowledge Discovery and Data Mining*, The AAAI Press, Menlo Park, 1996, pp. 334-338.

[6] M. Sahami, S. Dumais, D. Heckerman and E. Horvitz, "A Bayesian Approach to Filtering Junk Email," AAAI Technical Report WS-98-05, AAAI Workshop on Learning for Text Categorization, 1998.

[7] J. R. Hall, "How to Avoid Unwanted Email," *Communications of the ACM*, Vol. 41, No. 3, 1998, pp. 88-95. doi:10.1145/272287.272329

[8] E. Gabber, M. Jakobsson, Y. Matias and A.J. Mayer, "Curbing Junk E-Mail via Secure Classification," *Proceedings of the Second International Conference on Financial Cryptography*, Springer-Verlag London, 23-25 March 1998, pp. 198-213.

[9] R. A. Fisher, "On Some Extensions of Bayesian Inference Proposed by Mr. Lindley," *Journal of the Royal Statistical Society*: *Series B*, Vol. 22, No. 2, 1960, pp. 299-301.

[10] G. Robinson, "A Statistical Approach to the Spam Problem," 2003. http://www.linuxjournal.com/article.php?sid=6467 (accessed March 2011).

[11] P. Boldi, M. Santini and S. Vigna, "PageRank as a Function of the Damping Factor," *Proceedings of the* 14*th International Conference on World Wide Web*, ACM New York, 10-14 May 2005. doi:10.1145/1060745.1060827

[12] J. Gordillo and E. Conde, "An HMM for Detecting Spam Mail," *Expert Systems with Applications*, Vol. 33, No. 3, 2007, pp. 667-682. doi:10.1016/j.eswa.2006.06.016

[13] L. M. Spracklin and L. V. Saxton, "Filtering Spam Using Kolmogorov Complexity Estimates," in Russian, 21*st International Conference on Advanced Information Networking and Applications Workshops* (*Ainaw*'07), Niagara Falls, 21-23 May 2007, pp. 321-328.

[14] S. V. Korelov, A. K. Kryukov and L. U. Rotkov, "Text Messages' Digital Analysis on Spam Identification," in Russian, *Proceedings of Scientific Conference on Radiophysics*, Nizhni Novgorod State University, Nizhny Novgorod Oblast, 2006.

[15] W.-F. Hsiao and T.-M. Chang, "An Incremental Cluster-Based Approach to Spam Filtering," *Expert Systems with Applications*, No. 34, No. 3, 2008, pp. 1599-1608. doi:10.1016/j.eswa.2007.01.018

[16] S. M. Lee, D. S. Kim and J. S. Park, "Spam Detection Using Feature Selection and Parameters Optimization," *IEEE International Conference on Intelligent and Software Intensive Systems*, Krakow, 15-18 February 2010, pp. 883-888. doi:10.1109/CISIS.2010.116

[17] M. F. Saeddian and H. Beigy, "Spam Detection Using Dynamic Weighted Voting Based on Clustering," *Proceedings of the* 2008 *Second International Symposium on Intelligent Information Technology Application*, Vol. 2, pp. 122-126. doi:10.1109/IITA.2008.140

[18] M. Sasaki and H. Shinnou, "Spam Detection Using Text Clustering," *IEEE Proceedings of the 2005 International Conference on Cyberwords*, Singapore, 23-25 November 2005, pp. 316-319. doi:10.1109/CW.2005.83

[19] P. Cortez, C. Lopes, P. Sousa, M. Rocha and M. Rio, "Symbiotic Data Mining for Personalized Spam Filtering," *IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology*, Milan, 15-18 September 2009, pp. 149-156. doi:10.1109/WI-IAT.2009.30

[20] W. Lauren, "Spam Wars," *Communications of the ACM —Program Compaction*, Vol. 46, No. 8, 2003, p. 136.

[21] G. Pawel and M. Jacek, "Fighting the Spam Wars: A Re-Mailer Approach with Restrictive Aliasing," *ACM Transactions on Internet Technology* (*TOIT*), Vol. 4, No. 1, 2004, pp. 1-30.

[22] F. Li, H. Mo-Han and G. Pawel, "The Community Behavior of Spammers" 2011. http://web.media.mit.edu/~fulu/ClusteringSpammers.pdf.

[23] K. S. Xu, M. Kliger, Y. Chen, P. J. Woolf and A. O. Hero, "Revealing Social Networks of Spammers through Spectral Clustering," *IEEE International Conference on Communications*, Dresden, 14-18 June 2009, pp. 1-6. doi:10.1109/ICC.2009.5199418

[24] K. S. Xu, M. Kliger and A. O. Hero, "Tracking Communities of Spammers by Evolutionary Clustering," 2011. http://www.eecs.umich.edu/~xukevin/xu_spam_icml_2010_sna.pdf.

[25] Laboratory CSAIL MIT in USA, 2011. http://projects.csail.mit.edu/spamconf/.

[26] Computer Laboratory Faculty Cambridge University in UK, 2011. http://www.cl.cam.ac.uk/~rnc1/.

[27] National Center for Scientific Research, "Demokritos," 2011. http://www.iit.demokritos.gr/.

[28] D. Mertz, "Spam Filtering Techniques," 2002. http://www.ibm.com/developerworks/linux/library/l-spamf.html.

[29] R. Segal, J. Crawford, J. Kephart and B. Leib, "Spam-

Guru: An Enterprise Anti-Spam Filtering System," IBM Thomas J. Watson Research Center. http://www.research.ibm.com/people/r/rsegal/papers/spamguru-overview.pdf.

[30] Microsoft Antispam Technologies. http://www.microsoft.com/mscorp/safety/technologies/antispam/default.mspx.

[31] Symantec Antispam Protection for E-Mail. http://www.symantec.com/business/premium-antispam,.

[32] Kasperskiy Ant-Spam. http://www.kaspersky.ru/anti-spam.

[33] Anti-Spam Research Group. http://asrg.sp.am/.

[34] The Internet Engineering Task Force. http://www.ietf.org/.

[35] Spam Events. http://spamlinks.net/conf.htm.

[36] S. A. Nazirova, "Anti-Spam Module for Filtering the Outgoing Correspondence," in Russian, *Transactions of ANAS, Informatics and Control Problems*, Vol. XXVIII, No. 3, 2008, pp. 158-162.

[37] S. A. Nazirova, "New Anti Spam Methods," *Proceedings on the Second International Conference on Problems of Cybernetics and Informatics*, Baku, 10-12 September 2008, pp. 89-92.

[38] Spam URL Realtime Block Lists. http://www.surbl.org/.

[39] Razor's homepage. http://razor.sourceforge.net/.

[40] Pyzor's homepage. http://sourceforge.net/apps/trac/pyzor/.

[41] DCC Spam Control Delayed Your E-Mail. http://mail.cc.umanitoba.ca/grey/.

[42] Symantec Brightmail Anti-Spam. http://www.symantec.com/business/premium-antispam.

[43] Yandex, "Some Automatic Spam Detection Methods". http://company.yandex.ru/public/articles/antispam.xml.

[44] Microsoft Sender ID Framework. http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx.

[45] Sender Policy Framework. http://www.openspf.org/Introduction.

[46] J. Klensin, "RFC-2821: Simple Mail Transfer Protocol," April 2001. http://www.rfc-ref.org/RFC-TEXTS/2821/index.html.

[47] T.-J. Liu, W.-L. Tsao and C.-L. Lee, "A High Performance Image-Spam Filtering System," *Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science*, 10-12 August 2010, Hong Kong, pp. 445-449. doi:10.1109/DCABES.2010.97

[48] M. Soranamageswari and C. Meena, "Statistical Feature Extraction for Classification of Image Spam Using Artificial Neural Networks," *Second International Conference on Machine Learning and Computing*, Bangalore, 9-11 February, 2010, pp. 101-105. doi:10.1109/ICMLC.2010.72

[49] Bag of Words Model. http://en.wikipedia.org/wiki/Bag_of_words_model_in_computer_vision.

[50] K. Li, Z. Zhong and L. Ramaswamy, "Privacy-Aware Collaborative Spam Filtering," *IEEE Transactions on Parallel and Distributed Systems*, Vol. 20, No. 5, May 2009, pp. 725-739. doi:10.1109/TPDS.2008.143

[51] F. Weidong and D. Shoubin, "Addressing Interest Diversity in P2P Based Collaborative Spam Filtering," *Fifth International Conference on Grid and Cooperative Computing Workshops*, Hunan, October 2006, pp. 163-169. doi:10.1109/GCCW.2006.16

[52] J. S. Kong, B. A. Rezaei, N. Sarshar, V. P. Roychowdhury and P. O. Boykin, "Collaborative Spam Filtering Using E-Mail Networks," *IEEE Computer Society on Computer*, Vol. 39, No. 8, 2006, pp. 67-73.

[53] A. Gray and M. Haahr, "Personalised, Collaborative Spam Filtering," *Proceedings of the First Conference on Email and Anti-Spam* (*CEAS*), Mountain View, 30-31 July 2004.

[54] R. M. Alguliyev and S. H. Nazirova, "Multilayer and Multiagent Automated Email Filtration System," *Telecommunications and Radioengeneering*, Vol. 67, No. 12, pp. 1089-1095.

[55] P. A. Chirita, J. Diederich and W. Nejdl, "MailRank: Using Ranking for Spam Detection," *Proceedings of the* 14*th ACM International Conference on Information and Knowledge Management*, Bremen, 31 October-5 November 2005.

[56] R. Bhuleskar, A. Sherlekar and A. Pandit, "Hybrid Spam E-Mail Filtering," 2009 *First International Conference on Computational Intelligence, Communication Systems and Networks*, Indore, 23-25 July 2009, pp. 302-307. doi:10.1109/CICSYN.2009.34

[57] Google Message Security Postini Services. http://www.google.com/postini/email.html.

[58] R. M. Alguliyev and S. H. Nazirova, "Architecture of Hierarchical Intellectual Nation-Wide System of Struggle against Spam," in Russian, *Information Technologies*, Moscow, No. 8, 2006, pp. 32-36.

[59] R. M. Alguliyev and S. H. Nazirova, "Mechanism of Formation and Realisation of Anti-Spam Policy," in Russian, *Telecommunications*, Moscow, No. 12, 2009, pp. 6-10.

