ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

A survey on spam detection techniques

Anjali Sharma[1], Manisha [2], Dr.Manisha [3], Dr.Rekha Jain [4]

Bansthali Vidyapith, Jaipur Campus, India[1,2,3,4]

Abstract: Today e-mails have become one of the most popular and economical forms of communication for Internet users. Thus due to its popularity, the e-mail is going to be misused. One such misuse is the posting of unwelcome, unwanted e-mails known as spam or junk e-mails [1]. E-mail spam has various consequences. It reduces productivity, takes extra space in mail boxes, extra time, extend software damaging viruses, and materials that contains potentially harmful information for Internet users, destroy stability of mail servers, and as a result users spend lots of time for sorting incoming mail and deleting unwanted correspondence. So there is a need of spam detection so that its consequences can be reduced [2]. In this paper, we present various spam detection techniques.

Keywords: Spam, Spam detection techniques, Email classification

I. INTRODUCTION

Spam refers to unsolicited commercial email. Also known as junk mail, spam floods Internet users' electronic mailboxes. These junk mails can contain various types of messages such as pornography, commercial advertising, doubtful product, viruses or quasi legal services [3].

II. TYPES OF SPAM

Basically, spam can be categorized into the following four types:

1. Usenet Spam
2. Instant messaging Spam
3. Mobile Spam
4. E-mail Spam

Usenet Spam: **USE**r **NET**work is an open access network on the Internet that provides group talks and group email messaging. All the information that travels over the Internet is called "NetNews" and a running collection of messages about a particular topic is called a "newsgroup". Usenet spam is posting of some advertisement to the newsgroups. Spammers target the users those read news from these newsgroups. Spammers post advertisement to large amount of newsgroups at a time. Usenet spam rob users of the utility of the newsgroups by overpowering them with a barrage of marketing or other unrelated posts.

Instant Messaging Spam: Instant messaging systems, such as Yahoo Messenger, AOL Instant Messenger (AIM), Windows Live Messenger, Facebook Messenger, XMPP, Tencent QQ, Instant Messaging Client (ICQ), and MySpace chat rooms are all targets for spammers. Several IM systems provide a directory of users, including demographic information such as date of birth and gender. Advertisers can collect this information, sign on to the system, and send unwanted messages, which could include commercial malware, viruses, and associates to paid sites [8]. As instant messaging tends to not be jammed by firewalls; therefore, it is an especially useful way for spammers. It targets the users when they join any chat room to find new friends. It spoils enjoy of people and waste their time also.

Mobile Phone Spam: Mobile phone spam is focussed at the text messaging service of a mobile phone. This can be especially annoying to customers not only for the inconvenience but also because of the cost they may be charged per text message received in some markets. This kind of spam usually contains some schemes and offers on various products. Sometimes service providers also make use of this to trap the user for activation of some paid service.

E-mail Spam: Email spam is the most familiar form of spam. E-mail spam targets the individual users with direct mails. Spammers create a list of e-mail users by inspecting Usenet postings, stealing lists of internet mail, search web for e-mail addresses. E-mail spam costs money to user of e-mail because while user is reading the e-mails meter is running. E-mail spam also costs the ISPs because when a bulk of spam mails are sent to the e-mail users its wastes the band width of the service providers these costs are transmitted to users. All unwanted e-mails are not spam e-mails.

III. NEED FOR SPAM DETECTION

All Spam detection is becoming a big challenge for network resources and users because of their following negative effects:

- Spam causes annoyance and wastes users' time to regularly check and delete this large number of unwanted messages [4].

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

- Flooding of mailboxes with spam e-mails waste storage space and overload the server; thus it may lead to losing legitimate e-mails, delaying the server response, or even make it totally unavailable. Hence, spam consumes network bandwidth and server storage space.
- Spam has ethical issues like advertising fraudulent ads (for example make-money quick), offensive and immoral content (such as pornographic images and adult material) that are detrimental to the young generations [5].
- Sometimes spam even containing explicit content or malicious code including viruses, rootkits, worms, trojans or other kind of damaging software *etc.*
- Spam has become the key to carry out "phishing" damages, where a bank or another association is replaced in order to get valid user identification, and steal his banking data leading to scam [7].
- Receiving unsolicited messages is a privacy violation.

As an ultimate observation, spam is not simply hazardous or a misuse of time, but it can be quite troubling. Also, network and email supervisors need to utilize considerable time and effort in deploying systems to fight spam. There is not a way to measure this damage regarding money, but undoubtedly it is far from minor .Hence, it has become an important and indispensable aspect of any recent e-mail system to incorporate a spam filtering subsystem that detect spam.

IV. SPAM DETECTION TECHNIQUES

There are lots of existing techniques which try to prevent or reduce the expansion of huge amount of spam or junk e-mail. The available techniques usually move around using of spam filters. Generally, spam detection techniques or Spam filters inspect different sections of an email message to determine if it is spam or not.

On the basis of different sections of email messages; Spam detection techniques can be classified as Origin based spam detection techniques and Content based spam detection techniques [6]. Generally, most of the techniques applied to the issue of spam detection are effective but the important role in minimizing spam email is the content-based filtering. Its positive outcome has forced spammers to regularly change their methods, behaviours, and to scam their messages, in order to avoid these kinds of filters.

Spam detection techniques are discussed below:

Origin-Based Technique:

Origin or address based filters are techniques which based on using network information to detect whether a email message is spam or not. the email address and the IP address are the most important parts of network information used.

There are few main categories of origin-Based filters like Blacklists; Whitelists based systems [6].

1) Blaclists: Blacklists are records of email addresses or IP addresses that have been earlier used to send spam [9]. In creating a filter; if the sender of mail has its entry in the black list then that mail is undesirable and will be considered as spam [10]. For example those websites can be put in blacklist which have a past record of fraudulent or which exploits browser's vulnerabilities.

The main problem of a blacklist is maintaining its content to be accurate and up-to-date.

2) WhiteLists: It is opposite to the black list concept. It consists of the list of entries which can penetrate through and are authorized. These mails are considered as ham mails and can be accepted by the user. It has a set of URLs and domain names that are legitimate [10]. Spam is blocked by a white list with a system which is exactly opposite to existing blacklist. Rather than define which senders to block mail from, a white list define which senders to permit mail from; these addresses are placed on a trusted-users list [9].

The main difficulty of white listings is the assumption that trustworthy contacts do not send junk, for a while this theory could be invalid. Great number of spammers uses PCs that have been harmed using viruses and trojans for sending spam, to every single one contacts of address book, thus we could receive a spam message from a recognized sender if a virus has infected his computer.

seeing as these contacts are present in the white list, all messages arriving from them are labelled as secure [7].

3) Realtime Blackhole List (RBL): This spam-filtering method acts something like the same to a accepted blacklist on the converse less hands-on maintenance is required, and the Mail Abuse Prevention System and System administrators (third-party) operate it using spam detection tools [7]. This filter basically needs to connect to the third-party system whenever an email comes in, to authenticate the sender's IP address against the list. As the list is probably to be preserved by a third party, we don't have as much of control on what addresses are there on the list [9].

Content Based Spam Detection Techniques:

Content based filters are based on examining the content of emails. These content based filters are based on manually made rules, also called as heuristic filters, or these filters are learned by machine learning algorithms [7].These filters try to interpret the text in respect of examine its content and make decisions on that basis have spread among the Internet users, ranging from individual

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

users at their personal computers, to big commercial networks. The success of content-based filters for spam detection is so large that spammers have performed more and more complex attacks intended to avoid them and to reach the users mailbox.

There are various popular content based filters such as: Rule Based Filters, Bayesian filters, Support Vector Machines (SVM) and Artificial Neural Network (ANN) [11].

1) Rule- Based Filters: The Rule-Based Filters use a set of rules on the words incorporated in the whole message to find out whether the message is spam or not. In this approach, a comparison is done between each email message and a set of rules to find out whether a message is spam or ham. A set of rules contains rules with a variety of weights assigned to each rule. In the beginning, each received email message has a zero score. Then email is parsed to detect the existence of any rule, if it exists. If the rule is found in the message, then the weight of the rule is added to the final score of the email. At the end, if the final score is found to be exceeding some threshold value, then the email is declared as spam [12].

The drawback of Rule-Based Spam Detection Technique is that it is a set of rules that is very huge and static that causes less performance [6]. The spammers can effortlessly surmount these filters by simple word obfuscation, for example, the word "SALE" could be changed to S*A*L*E so it will bypass the filters.

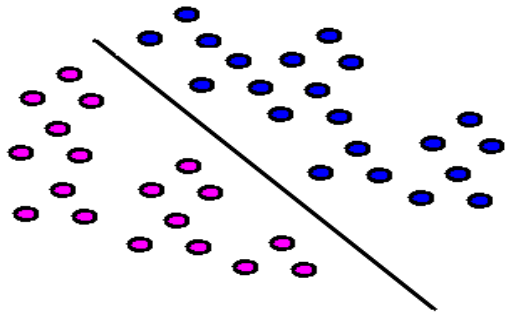
The inflexibility of the rule-based approach is it's another major disadvantage. The rule based spam filter is not intelligent as there is no self-learning ability available in the filter.

2) Bayesian filters: The Bayesian filters are most advanced form of content-based filtering, these filters uses the laws of probability to find out which messages are legitimate and which are spam. Bayesian Filters are also the well known machine learning approaches [11]. In order to identifying each message as either junk or legitimate, initially the end user must "train" the Bayesian filter manually for efficiently block the spam messages. Eventually, the filter takes words and phrases found in legitimate emails and adds them to a list; it also applied the same method with words found in spam. To decide which received messages are classified as spam emails, the content of the email are scan by the Bayesian filter and then compare the text against its two-word lists to calculate the probability that the message is spam.

For example, if the occurrences of word "free" is 62 times in a list of spam messages but only 3 times in ham(legitimate) emails, then there is a 95% possibility that an arriving email containing the word "free" is spam or junk email. Because a Bayesian filter is continuously building its list of word based on the messages that an individual user receives, it theoretically becomes more efficient the longer it's used.

However, since the Bayesian filter method requires a training before it starts working well, we will require to exercise patience and will probably have to delete few junk messages manually, at least at first time [9].

3) Support Vector Machines: The Support Vector Machines (SVM) has successes at using as classifying text documents. SVM has encouraged important researches into applying them to spam filtering. SVMs are kernel methods whose vital idea is to embed the data indicating the text documents into a vector space where geometry and linear algebra can be performed [11]. SVMs try to create a linear separation between the two classes in the vector space [6].



Support Vector Machine

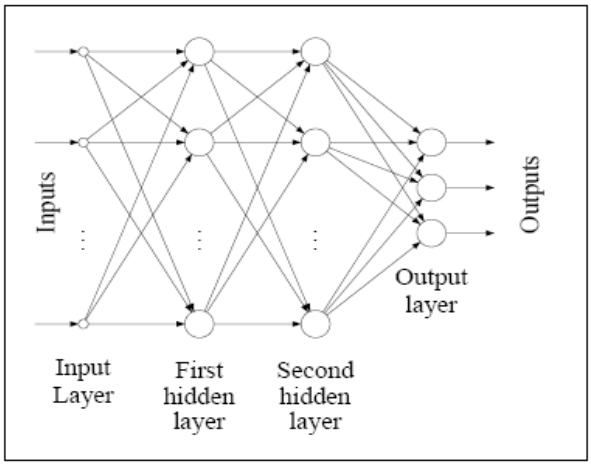
An example is shown above. In this example, the objects belong either to BLUE (ham) class or PINK (spam) class. The separating line defines a boundary on the left side of which all objects are PINK and to the right of which all objects are BLUE. Any new object (white circle) falling to the right is labelled, i.e., classified, as BLUE (or classified as PINK should it fall to the left of the separating line).

4) Artificial Neural Network An artificial neural network is a group of interconnected nodes these nodes are called as neurons. The well known example of artificial neural network is the human brain.

The term artificial neural network has moved around a huge class of models and machine learning methods. The central idea is to extract linear combinations of the inputs and derived features from input and then model the target as a nonlinear function of these features [6].

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014



Artificial Neural Network as an interconnected collection of nodes

ANN is an adaptational system that changes its structure based on internal or external information that flows through the network during the learning phase. They are generally familiar with model complex relationships between inputs and outputs or to find patterns in data. The neural network must first be "trained" to categorize emails into spam or non spam starting from the particular data sets. This training includes a computational analysis of message content using huge representative samples of both spam and non-spam messages [11]. To generate training sets of spam and non-spam emails, each email is attentively reviewed according to this simple, yet limited definition of spam.

V. CONCLUSIONS

The Spam is one of the most annoying and malicious additions to global computer world. In this paper, we have presented different spam detection techniques that have been used or projected for use to detect spam. We have required to arrange these techniques in a systematic and instructive manner, expecting that the result will prove beneficial in the progressing fight against spam, by allowing intelligent selection of spam filters by practitioners, and informed treatment and more reliable of spam filters in the academic literature equated with the earlier situation. Content based filters are more effective than origin based filters because learning facility available in content based filters.

REFERENCES

[1] S. Abduelbaset M. Goweder, Tarik Rashed, Ali S. Elbekaie, and Husien A. Alhammi, "An Anti-Spam System Using Artificial Neural Networks And Genetic Algorithms" (A Neural Model In Anti Spam).

[2] Er. Seema Rani, Er. Sugandha Sharma, "Survey on E-mail Spam Detection Using NLP", International Journal of Advanced Research in Computer Science and Software Engineering, India, Volume 4, Issue 5, May 2014.

[3] Masurah Mohamad, Khairulliza Ahmad Salleh, "Independent Feature Selection as Spam-Filtering Technique: An Evaluation of Neural Network", Malaysia.

[4] El-Sayed M. El-Alfy, "Learning Methods For Spam Filtering", College of Computer Sciences and Engineering King Fahd University of Petroleum and Minerals, Saudi Arabia.

[5] Upasna Attri & Harpreet Kaur, "Comparative Study of Gaussian and Nearest Mean Classifiers for Filtering Spam E-mails", Global Journal of Computer Science and Technology Network, Web & Security, USA, Volume 12 Issue 11 Version June 2012.

[6] Alia Taha Sabri, Adel Hamdan Mohammads, Bassam Al-Shargabi, Maher Abu Hamdeh, "Developing New Continuous Learning Approach for Spam Detection using Artificial Neural Network (CLA_ANN)", European Journal of Scientific Research, ISSN 1450-216X Vol.42 No.3 (2010), pp.511-521.

[7] Enrique Puertas Sanz, José María Gómez Hidalgo,José Carlos Cortizo Pérez, "Email Spam Filtering", Universidad Europea de Madrid Villaviciosa de Odón, 28670 Madrid, SPAIN.

[8] Ravinder Kamboj, "A rule based approach for spam detection" , Computer Science and Engineering Department, Thapar University, India, July 2010.

[9] Vandana Jaswal, Nidhi Sood, "Spam Detection System Using Hidden Markov Model", International Journal of Advanced Research in Computer Science and Software Engineering, India, Volume 3, Issue 7, July 2013.

[10] Sahil Puri, Dishant Gosain, Mehak Ahuja, Ishita Kathuria, Nishtha Jatana, "Comparison And Analysis Of Spam Detection Algorithms", International Journal of Application or Innovation in Engineering & Management (IJAIEM), India, Volume 2, Issue 4, April 2013.

[11] Ann Nosseir , Khaled Nagati and Islam Taj-Eddin, **"**Intelligent Word-Based Spam Filter Detection Using Multi-Neural Networks" , IJCSI International Journal of Computer Science Issues, Egypt**,** Vol. 10, Issue 2, No 1, March 2013.

[12] Jitendra Nath Shrivastava, Maringanti Hima Bindu, " E-mail Spam Filtering Using Adaptive Genetic Algorithm", I.J. Intelligent Systems and Applications,MECS, India, January 2014.