The Current State of Battle against Spam

Rochak Gupta, K Vinay Kumar

Department of Computer Science and Engineering, National Institute of Technology Karnataka
Surathkal, India

***Abstract*— the growth of Spam over the years suggests that Spam is no longer simply a threat but a large scale network problem today. The battle between spammers and anti-spamming techniques has been going on for many years. Many anti-spam techniques are currently employed to filter spam e-mails, however spam is still able to attack many email users. This paper provides an overview of available spam filtering approaches and their drawbacks. We also describe the common spammers' tricks that spammers use to bypass the currently available spam filters. The paper primarily focuses to throw some light on root causes of the spam growth.**

***Keywords*— Spam, Tricks, Spam filter, Email, Email server, Network bandwidth**

I. INTRODUCTION

1.1. Categories of Spam

E-mail has become an easy means to distribute a huge amount of unsolicited mails to a large of users with very low cost. These unwanted bulk mails or unsolicited mails are called Spam mails. As shown in Table 1, the majority of Spam messages that has been reported recently are unsolicited commercials including pharmaceutical, newsletters, gambling, watches, jobs, sexual/dating, softwares etc [12].

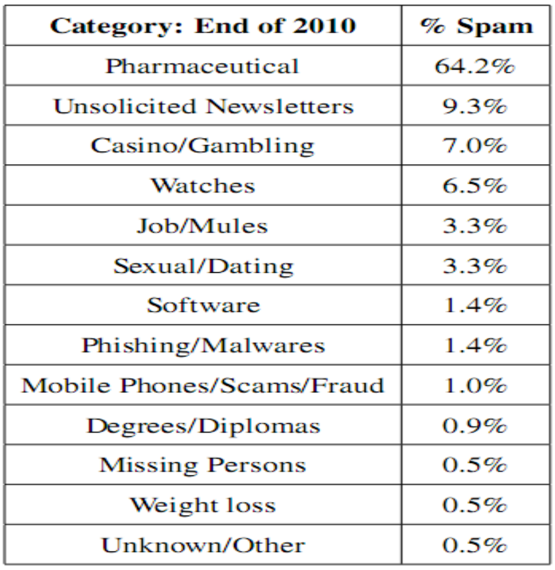
They also include annoying content such pornographic images and can be used as well for spreading rumours and other fraudulent advertisements. Spam software can also be used to distribute harmful content such as viruses, Trojan horses, malwares, worms and other malicious codes. It can be a means for phishing attacks as well.

1.2. Why Spam is a problem?

Spam has been growing rapidly over the years. As shown in Figure 1, in 2010, the average global Spam rate for the year was 89.1%, an increase of 1.4% compared with 2009 [12]. The growth of Spam over the years suggests that Spam is no longer simply a threat but a large scale network problem today.

The key reason for the growth of spam is the fact that it costs nothing to send an email; since all of the costs are paid by the carriers and the email servers. Furthermore there is a level of annoyance at receiving a lot of Spam. Email Spam affects the recipient; their time and resources are wasted dealing with Spam emails. It also affects the performance of email servers which process huge amount of emails sent by the Spammers.

Table 1:
CATEGORIES OF SPAM



Category: End of 2010	% Spam
Pharmaceutical	64.2%
Unsolicited Newsletters	9.3%
Casino/Gambling	7.0%
Watches	6.5%
Job/Mules	3.3%
Sexual/Dating	3.3%
Software	1.4%
Phishing/Malwares	1.4%
Mobile Phones/Scams/Fraud	1.0%
Degrees/Diplomas	0.9%
Missing Persons	0.5%
Weight loss	0.5%
Unknown/Other	0.5%

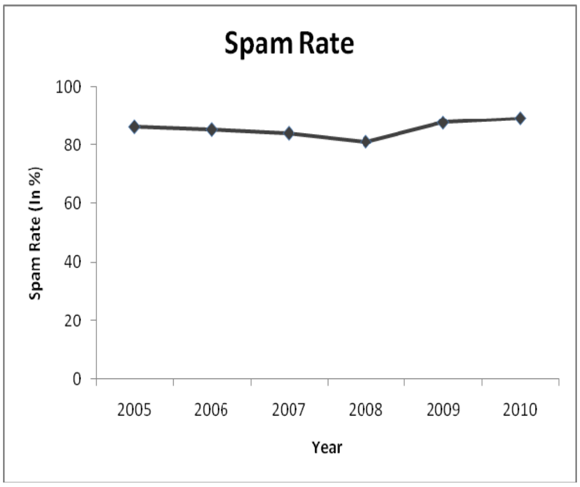


Figure 1: Rate of Spam

II. THE SOURCE OF SPAM

There are three primary sources of Spam in service provider networks:

2.1. Botnets

A botnet is a network of infected computers that have been taken over by Spammers and are used to send bulk Spam E-mails. The number of bots in botnets depends on profit desired by the spammer. Botnets might have a few thousand computers, but others might have lacks of infected computers. In most of the cases even owner of computers does not know that their computers are infected.

The proportion of Spam sent by botnets was much higher for 2010, approximately 88.2% of all Spam. However, the average number of Spam emails sent from each bot fell at the end of 2010 [12]. This led to a decrease in the total amount of global Spam in circulation toward the end of 2010. But many of the experts predict that e-mail will remain the primary, preferred medium for sending Spam. As the year progresses, researchers expect Spam volumes to match or exceed previous levels.

Following botnets were the active Spam botnets of 2010:

2.1.1. Rustock

Rustock was the one of the most dominant botnet in last few years. Rustock has been an important member of the botnets since January 2006. It was responsible for massive amount of Spam production worldwide. It was capable of sending up to 25,000 Spam messages per hour from an infected computer. It was a botnet of around 2 million bots capable of sending out 30 billion Spam emails per day. Microsoft's Digital Crimes Unit, working with federal law enforcement agents, has brought down the world's largest Spam network, Rustock in March 2011. Global Spam drops by huge amount as Rustock Botnet is Dismantled [1].

2.1.2. Grum

Grum is the future for Spam botnets. It's a kernel-mode rootkit and hence it is difficult to detect and remove it. Grum is mainly involved in sending pharmaceutical Spam e-mails. It consists of around 560,000 - 840,000 Grum root-kit infected computers. It was one of the most active Spam-sending botnets at the end of 2010 and was responsible for approximately 9% of botnet Spam. [12].

2.1.3. Cutwail

The Cutwail botnet has been active since 2007. It is mainly involved in DDoS attacks and sending Spam e-mails. It was responsible for approximately 6% of global Spam in year 2010. The number of active bots has increased by approximately 16%, compared with the number of bots under its control at the end of 2009 [12]. The Pushdo/Cutwail botnet spreads Spam including online casinos pharmaceuticals, phishing, and links to Web sites which contain malwares.

2.1.4. Maazben

Maazben botnet is mainly responsible for spreading Casino Spam. To keeps the Spam source hidden, Spammers prefer proxy-based bots. But proxy-based bots do not work if the infected computer is behind a NAT device [9]. Maazben is one of the fastest-growing botnet and was responsible for over 5.2% of global Spam in year 2010. The number of active bots under Maazbens control has increased by more than 1,000% since March 2010, to between 510,000 and 770,000 bots worldwide [12].

2.1.5. Mega-D

Mega-Ds Spam is mainly responsible for advertising an online pharmacy. At its peak was responsible for almost 18% of global Spam. In November 2010 the Federal Bureau of Investigation arrested mastermind of Mega-D botnet.

2.1.6. Bagle/Beagle/Mitglieder/Lodeight

Spam volume has declined in March 2011 after the takedown of the Rustock botnet, but Bagle botnet is taking its place. Bagle is famous for spreading pharmacy spam and at its peak was responsible for 17.2% of the total global spam volume. It is more powerful than Rustock because it maintains high profit with less number of infected computers.

2.2. Compromised accounts

The accounts that are accessed by someone who is unauthorized are called compromised accounts. Spammers use these accounts to send Spam.

2.3. Malicious use of email accounts

Another way that spammer can use to send the spam is by creating email accounts and uses them for the purpose of sending unwanted content. As reported that one in eight users' accounts is openly sending out Spam and/or malware.

III. Common Spammer tricks

As Spam filters are becoming better and better, they pressurise Spammers to evolve new tactics to bypass the filters. We present some of the most common tricks applied by Spammers to circumvent available Spam filtering solutions.

3.1. How to Get More Victims: Email Address Harvesting

3.1.1. Dictionary attacks

The dictionary attack is one of the most popular techniques among Spammers who wish to evolve or keep accounts of recipient addresses. To collect accounts of working email addresses, a spammer send vestigial mails to email accounts. A normal user who receives such mails with no body and subject line may be weird, but for a spammer it is a way to collect the working email accounts.

3.1.2. From posts to UseNet

Spammers use readymade softwares to continuously scan UseNet for email address. Some software might be designed to just look at posts headers which contain email address, while other softwares might be designed to check the posts bodies. These softwares looks at signatures, through programs that collect everything that contain a '@' character and attempt to demunge munged email addresses.

It is also observed that if people stop posting on the UseNet then frequency of Spam mails decreased sharply in their email accounts. The obvious reason is that Spammers always look for active addresses; this technique seems to be the primary source of email addresses for Spammers.

3.1.3. From mailing lists

Spammers repeatedly try to obtain the lists of subscribers to mailing lists. When mail servers are designed to deny such requests, Spammers might send an email to the mailing list with the headers Return-Receipt-To: or X- Confirm-Reading-To:. A different technique used by Spammers is to request a mailing lists server to give him the list of all mailing lists it carries, and then send the Spam to the mailing lists address, leaving the server to do the hard work of forwarding a copy to each subscribed email address [13].

3.1.4. From various web and paper forms

Some sites ask for details in the form of guest books and registrations forms. Spammers target these sites to obtain the email addresses because this information becomes freely available on the internet, or some site sells the emails list also.

3.2. Traditional Tricks Used by Spammers to Fool Spam Filters

- Over time, Spammers have adopted many more or less sophisticated tricks to fool Spam filters, namely those that are based on statistical parameters of Spam messages [8].
- Frequent change in senders address,
- Message encoding (such as base64, commonly used for secure message transfer),
- Hashing (e.g. insertion of HTML tags into messages),
- Use of images instead of plain text.

3.3. New Spammer Tricks

In this section we discuss new tricks used by Spammers to fool anti Spam filters.

3.3.1. Character hashing in words

This tactic can be used by Spammers to circumvent a keyword based Anti Spam filter. The basic concept of this tactics is to misspell some English words of the Spam mail so that a keyword based spam filter will not be able to understand the word, but a human brain can easily make out the meaning of misspelled word.

Example of a message with character hashing:

I finlaly was able to lsoe the wieght I have been struggling to lose for years! And I couldn’t bileeve how simple it was! Amizang pacth makes you shed the ponuds! It’s Guanarteed to work or your menoy back!

3.3.2. HTML code interleaving

To hide the message a spammer can insert HTML code in the middle of words. Email recipient with HTML code support can understand the message as the message is kept in perfectly readable form. However, for Anti Spam technologies it is tough to identify keywords split by HTML code. But this is not a popular tactic among Spammers nowadays.

For example,

HTML:

Ma<!- - 63 - ->ke mon <! - - adf - ->ey f<!- - sdf - - >a<! - - e - ->st

Would be rendered as “Make money fast” in an email client.

3.3.3. Attachments

One can send the spam message as an attachment of mail to avoid contents analysis performed by Spam filters. On the other hand, the curious recipient may open the attachment, which usually contains neither body text nor subject line in order to mislead the Spam filter.

3.3.4. Keyword masking by repeating characters

Spammers try to confuse keyword based Spam filter by repeating some characters. The message remains readable for humans, but it becomes tough for spam filters to detect spam. Here is an example: Buuuyyyy cheeeeaaap viaaagraaa.

3.3.5. Text De-obfuscation

Spammers often replace alphabetical characters with similar looking LEET characters to circumvent the keyword based spam filter. For example, if you have content filter that traps messages containing “viagra” (because of the flood of via-gra spam), all the Spammer has to do is spell it as “v1@gr@” or “iagra” or even “viagara” and it will probably sneak past. Task becomes more difficult for Anti spam technologies due to spelling variations, such as there are 600,426,974,379,824,381,952 different ways to spell viagra [5]. Spammers regularly search for new ways to obfuscate a word to bypass the Spam filters, and this technique often appeared in Spam text:

Do you wnat to l00k c00l and w3althy but do not have the m0ney to aff0rd a=sweeeeet n3w R0lex wtach? Get a 98% L00kalike R0lex watc h here! We have replikas of all the fines t bran d watc hes. Check the m out here!

3.3.6. Use of CSS styles

The widespread application of CSS styles for web page formatting gives Spammers a new opportunity to use the same technique to format their messages and bypass Spam filters based on statistical parameters [8].

Example Insertion of CSS styles into HTML tags to encode the word Cialis:

```
<span style=“display: yes; display: none”>g</span>C
<span style=“display: yes; display: none”>l</span>I
<span style=“display: yes; display: none”>o</span>A
<span style=“display: yes; display: none”>c</span>L
<span style=“display: yes; display: none”>s</span>I
<span style=“display: yes; display: none”>z</span>S
```

The only word that is actually displayed upon opening the message is CIALIS a term that is known to all Spam filters.

3.3.7. Good word attacks

Spammers attack statistical Spam filters by inserting “good” words into their messages. Such words can be chosen from a dictionary (a dictionary attack). There is a more sophisticated approach to utilize words that appear most frequently in legitimate mail, such as reuters news, or USENET messages (such English corpora are freely available). By adding a relatively small number of easily found words, an attacker can get 50% of currently blocked Spam past a typical Spam filter. While current good word attacks may be less sophisticated, any weakness of current Spam filters will eventually be exploited. Active attacks are the most effective, but good words can still be found without issuing a single query [11].

3.3.8. Tokenization attacks

Tokenization is a task of modifying the mail such a way that it will be circumvent the spam filters easily by splitting or modifying features, for example putting extra spaces, or symbols like ‘-’ or ‘#’, in the middle of the words, U N $ $ U B S C R l B E, for instance.

3.3.9. JavaScript Messages

One can put whole contents of the Spam mails inside a JavaScript that is activated when the mail is opened. This JavaScript get executed and the text of the mail is written out to the mail display area. As we have discussed earlier that simple filters ignore HTML interleaved mails and usually JavaScript is contained inside an HTML comment block. Smart Spammers can also encode the text that is written out to the mail display area. Same JavaScript can be used to decode it. Encoding the message text allows it circumvent filters that are good enough to recognize JavaScript.

3.3.10. URL One-Liner

Avoiding any text at all in the message is the best way discovered by Spammer to hide their message from Keyword based Spam filter. To achieve this Spammer only put a brief sentence and a URL in email. When the recipient of the mail clicks on the URL, they are redirect to a web page where the Spammer hosts his product. Since the mail only contains a brief text and a URL, It is tough for a Spam filter to identify that mail is Spam or not. A simple way to get rid of such spam mails is to block emails that contained a URL referencing one of the systems who hosts the site. But the Spammers use several redirects and domain shortenings to hide the actual identity of the systems hosting their sites.

The only way to identify such mails as Spam is to actually visit the website which URL appears in the email. On the basis of website contents, the Anti Spam filter can decide whether the message was Spam. Visiting sites to check mail is spam or not is not preferable because it slows down the flow of email by a huge amount.

3.3.11. Copy and Paste

Target of this trick become the user who are curious about every mail they receive. In some email messages the Spammers split the URL into two or more sections, and provide instructions for putting it back together in a web browser. For example:
type www.cnn then the follow URL into your browsers address bar:
.24750.net/content.htm

3.3.12. Personalized messages and exciting subject lines

Using this trick Spammers try to make their mailings look like personal messages. This may be done with a exciting subject line for the messages, or by making the messages look as though they were supposed to go to someone else [4].

3.4. Most popular Trick among Spammers: Redirecting URLs

URL redirection or URL forwarding and domain redirection or domain forwarding are techniques on the internet for making a web page available under many URLs [4]. Spammer use disposable “portals” to point to their actual websites. The portals may be any of the following:

3.4.1. Sites on free hosting services

Spammer use free web hosts and free blog services for placing redirectors. As these sites are free, users need not provide much information, and it is even possible for Spammers to use automated tools to create and store large numbers of redirectors for later use.

3.4.2. Links registered with URL-shortening services

URL-shortening service is another way to set up a redirection. The advantage of short URLs is that it does not have any clues as to where they really point. Spammers can use short URLs to redirect undetectably to their real websites. Many URL shortening services follow strict anti-Spam policies that allow them to break links that are reported to point to “Spamvertised” websites, but this can take a few days to happen.

3.4.3. Public redirector services controlled by search engines

Many search engines and other large web enterprises use internal redirector links to send you to sites that you might click on in your searches. One example of such a public redirector is rd.yahoo.com:
http://rd.yahoo.com/?http://www.romispam.net/

All that rd.yahoo.com does here is simply to redirect your browser to the URL named after the question mark. Yahoo often uses this technique when it provides you links to non-Yahoo sites. Yahoo does not have a thing to do with the sites listed in such redirection links, but the naive user might assume that the Spammer’s site is hosted by Yahoo so that he could not be such a untrustworthy person [4].

3.4.4. Breaking into trusted sites

Spammers hack into trusted sites and add hidden redirection code into a new or existing page on the site. So the Spam message contains a trusted link, but the page itself redirects to the Spam/porn/malware site, or causes a popup window containing the Spammed site.

For example, www.example.com is a well-established, widely-trusted site. Web reputation databases agree that links to this site are perfectly acceptable in email. However, our Spammer discovers that the site's version of Apache has a known vulnerability, allowing him to break in and add redirection code. He then sends Spam, linking users to www.example.com/.ed/pills.html, which redirects to the Spammer's site. Because the link is trusted, the Spam filters don't suspect a problem [4].

IV. EXISTING ANTI SPAM TECHNIQUES AND THEIR DRAWBACKS

Many techniques currently exist for identifying Spam emails.

4.1. Black list

Black list is one of the first generation anti-Spamming methods. A list of recognized Spamming email addresses and domain names is kept in the Mail Transfer Agent (MTA) or the email client system. Emails originated from these email addresses or domain names are discarded automatically. The method has the advantage of offering almost no false positive since every discarded Spam that is detected is well-known to be a Spam.

Disadvantages

- Continuous update of filter is required.
- Spammers tend to forge header information like sender information in Spam emails and legitimate senders are also being added to blacklists.
- This method is unable to attain high filtering accuracy because Spammers can either use new or spoofed email addresses to Spam.

4.2. White list

White list works similarly like black list, except that the list contains permissible email addresses or domain names that are known to the user instead. Most of the time, these email addresses are only either from the address book or previously sent to the mailbox, so the filtering capability of this method is fairly limited.

Disadvantages

- As emails from fresh unfamiliar email addresses will be naturally denied, this method introduces extremely high false positive rate.
- If Spammers are able to access to the list, they can readily bypass this filter with spoofed addresses in the list. A common spoofed email address can be a well known mailing list address that is white-listed by many users.
- The IP address of the trusted user should be known in advance and should be continuously updated manually.

4.3. Keyword searching

Keyword searching is one of the most widely used methods to combat Spam. Advantage of these techniques is high filtering accuracy. A large fraction of common Spam can be eliminated through identifying keywords found in common Spam messages.

Disadvantages

- This method is ineffective in identifying context or word variations. Thus, there may be intolerable false positives Spam rate at the same time. For example, a legitimate email which contains the common words like "offer" can be classified as Spam mistakenly.
- Spammers can bypass these static filters simply using tricks like using LEET characters in words or misspelling the words.
- Spammers can simply bypass these filters by hiding their Spam mails in images.
- This method will not be able to detect Spam messages in images.
- The situation becomes worse because many recent Spam do not include any text. Instead, they contain only figures or URLs or both.
- Spammers change their tricks very frequently to fool Spam filters. So regular and time consuming training is required to maintain the high filtering rate.
- Most recent Spam technique of using similar looking words, for e.g. @ instead of a, or \/ instead of V, will also need to be identified.

4.4. Reputation services

Reputation service is one of the most famous MTA level anti-Spamming techniques. A traffic monitor system keeps tracks the volume of email traffics of various domain names or email addresses. The reputation of the domain names or email addresses will vary drastically with any unusual change of volume, which may be an indication of Spam. One of the most successful email traffic monitoring networks is SenderBase, which tracks about 25% of the worlds email traffic. This service can identify and block 75% of incoming Spam with about one false positive in a million emails.

Disadvantages

- By the time the Spamming email addresses or domain names are known to have bad reputation, they have already sent out millions of Spam.
- Spammers can spoof email addresses or domain names of innocent users and spoil their reputation.

4.5. Hash/signature filter

This is a MTA level Spam filtering technique. In this technique, MTA maintains the database of the hashes of previously detected Spam mails. All incoming emails will be compared with the database of hashes to classify Spam from normal emails. This method is effective in filtering a fraction of Spam.

Disadvantages

- Newly generated Spam will still be able to bypass the filter.

- Spammers can easily bypass the scheme by including a random string into the Spam mail to generate different hashes.
- Another big problem with this technique is size of the database which increases over time since every day thousands of newly generated Spam will be added into database. The checking process time will increase significantly over the time.

4.6. Header analysis

Every email contains header attached to it which contains its routing information. Fake routing information can be inserted by Spammers to protect their identities from being tracked. Therefore, analysis of the email header can be done to determine if it has a wrong format to find out whether it is a Spam. Although this method can detect Spam, it can also help to indicate a wrongly configured mail server.

Disadvantages

- To check whether mail header is well formed, does not signify that it is not from a Spammer.
- Spam can be sent undetectable by taking control over machine zombies.

As a result, this method can be used with other anti-Spamming techniques to be effective.

4.7. Heuristics

In this technique, a combination of two or more anti-Spamming techniques such as header analysis and signature filter can be used to determine if an email is a Spam. User can set a threshold level to identify an email Spam.

Disadvantages

- Complex fine tuning is required to reduce the false positive rate.
- This method is good enough but can be bypassed by new Spammers tricks such as text hiding, character encoding and text hidden in images.

4.8. Artificial intelligence

There are multiple researches are going on for email content analysis based on Artificial Intelligence (AI), machine learning and statistical techniques. The advantage of these techniques is the ability for the system to retrain itself while it is put in use. Thus it decreases the need of any manual work while maintaining high filtering accuracy.

Disadvantages

- Complex fine tuning and testing are required before putting them for use.
- On the receiving end complex analysis is required which makes the process of receiving email laborious and time-consuming.
- It seems impossible to detect Spam perfectly even best AI algorithms are used.
- Lastly, this method may lead to high false positives which will be intolerable by legitimate users.

4.9. Obfuscation

Obfuscation is a technique which tries to work on the root cause of Spam that is email addresses harvesting. It prevents email addresses harvesting by displaying it in an altered but obvious form (e.g., xyz@gmail.com can be displayed as xyz at gmail dot com). This method is easy to apply since no changes are required for the email system.

Disadvantages

- As there are limited combinations, Spammers can use AI-based harvest programs to retrieve real addresses easily.
- Since Spammers have other sources to get email addresses, the technique is not much effective practically.
- The scheme only prevents email addresses harvesting but it does not offer any Spam protection.

4.10. Legislation approaches

Many countries have adopted different laws and legislations to protect businesses and individuals alike against Spam. These laws place restrictions and regulations to control Spammers activities. CAN-SPAM Act (controlling the assault of non-solicited pornography and marketing) is an example of legislation approaches. These laws or Acts prohibits Spammers from e-mail addresses harvesting and creating Botnets. Failure to comply with CAN-Spam Act can result in a monetary penalty of 16,000 dollar per incident. However the CAN-Spam Act does not stop Spammers to send Spam e-mails. McAfee Research reported on 2009 despite the six-year-old CAN-SPAM Act, Spammers routinely abuse the law and continue to deliver Spam [14].

4.11. Rule based Spam filters

Rule based filters are one of the most famous Spam filtering techniques. They filter mails on the basis of the email contents with a set of words or phrases and would block a message if a certain number of hits were met.

Disadvantages

- As each time one fine tunes rule based Spam filters, Spammers come up with the new technique to bypass it. False positive and false negative rate is very high even after the fine tuning of the filter. By replacing characters with the LEET characters, these kinds of filters can easily be bypassed.
- It is observed that Spammers use available rule based filters to test their Spam mails before sending them. As the filters are becoming more and more complex, the chances of high false positives may also increase.

4.12. Grey listing

This behaviour of Spammers, more likely to give up when the going gets tough, has led to a solution called grey listing. The idea is to modify the email server on the receiver end to initially refuse the connection for any incoming email from a source not whitelisted. Spammers traditionally broadcast a burst of email. If there are any delivery problems, they are not likely to return to retry later. In contrast, most legitimate email servers attempt retransmission for up to three days. By combining grey listing, whitelisting, and blacklisting, one author reported an 88% reduction in Spam [7]. Information about servers that do not retry to send messages could be shared to allow collaborative detection of Spammers.

Disadvantages

- The technique has high false positive rate: it delays most of junk but also gives unnecessary delay to good mail.
- Greylisting may pose problems with poorly configured legitimate servers that might drop connections.

4.13. Decision Tree

A decision tree is a structured way to model chance events. It uses a tree-like structure of decisions and their possible consequences, including chance event outcomes, and resource costs. Unique classification is represented by each leaf and representation of the conjunction of features is done by branches of tree that lead to the classifications at various leaves. The advantage of using decision tree algorithm is that it generates understandable rules without any complex computations. They provide a clear indication of which features are most important for classification. Decision tree can also handle missing data by assuming it is randomly distributed within the dataset.

Disadvantages

- The cost of sorting all candidate fields before the best split can be found, increases with the growth of a decision tree.
- Pruning bears the cost of generating and comparing several sub trees. Due to these reasons, it is hard to measure its performance with the size of training data.

4.14. Support Vector Machine (SVM)

SVM performs well even if a plenty of features are used; it automatically tunes itself and maintains accuracy and generalization. Therefore, there is no necessity to find the optimum number of features.

Disadvantages

- Choice of an appropriate kernel function, high memory requirement and increasing training time with training data size are its problems.

4.15. Fuzzy logic

The main feature of this Spam filtering is that it checks the message content to classify mail as Spam rather than relying on a fixed static set of keywords. Therefore it can adapt to Spammer tricks and dynamically build its data base. Realizing the ambiguity in word usage in English, the fuzzy association method avoids this problem by noticing the relationship or association among different index terms or keywords in the documents.

Disadvantages

- Fuzzy modelling is difficult for discrete data.
- To maintain the performance of the fuzzy logic engine experimental fine tuning with respect to all the relevant parameters is required.

4.16. K nearest neighbours (KNN)

The main strength of the KNN algorithm is that it provides good generalized accuracy on many domains and the learning phase is fast.

Disadvantages

- In order to classify one mail we have to measure distances to all training mails and find the k nearest neighbours. It slows down the decision procedure.
- The accuracy of the approach decreases with increase of noise in training data.

4.17. Image-Based Spam filter

Spammers have recognized that intentional distortion of words or putting the text inside an image can easily defeat word filtering. Pre-processing of documents is therefore necessary, involving scanning of email images using character recognition techniques, applying a sophisticated text filtering method in the second phase. Image filters must be trained similarly to text-based filters. OCR is applied to detect text contained in images and convert the message into a standard ASCII document.

Disadvantages

- Spammers have adopted obfuscation techniques, such as replacement of letters with numbers or other similar symbols, use of similar words, etc.
- Spammers are enhancing their messages by adding various noise items (such as randomly placed dots, lines or waves) on the background. Such emails remain legible for humans, but become hard to handle for OCR methods.
- Some OCR algorithms are language-dependent, which is a great disadvantage in the context of Spam filtering.

4.18. Collaborative filtering

Collaborative Spam filters use the feedback from the other users to reliably identify Spam. That is, for every new Spam sent out, some user must first identify it as Spam; any subsequent user who receives a suspect e-mail can then query the user community to determine whether the message is already tagged as Spam.

Disadvantages

- The problem with this filtering is that it can only share information within the same e-mail server, since different e-mail servers do not share information. Further, Spammers may include random words to generate many versions of the same Spam e-mail, so that they are recognized as different e-mails.
- They may also continually change their e-mail or server addresses.

4.19. Spam classification through social network

This method is based on social network analysis. Senders of the e-mails are represented as nodes on a graph, and the relationship between sender and receiver of e-mails is represented as a link on the graph. The node does not belong to the linked list on the graph is considered as Spammer.

Disadvantages

- The problem with this filtering is that it needs to keep track of e-mail history, which can only be done in the same e-mail server; and it classifies as Spam all e-mails from first time senders.

V. CONCLUSIONS

The most common approach to fight junk mails is by using a filter, which tries to identify Spam mails and filter them out. Currently available Spam filters reduce the number of Spam mails that the user receives, but it does not entirely eliminate the problem. Moreover, filters have basic problems. For example, it is difficult to maintain their accuracy due to new Spam tricks, senders of Spam mail adapt to their strategies, and Spam filters sometimes filter innocent mails. On top of that, once filters improve, Spammers increase the amount of Spam mails to reach their customers, so improvements of Spam filters do not make much effect. Finally, since the volume of Spam mails increases, the internet becomes more and more loaded, and its efficiency decreases.

One other possibility is that the users, who are still using their old filters, might receive more Spam messages, and the internet might become less efficient. In response to improvements in filtering techniques, Spammers introduce new tricks to fool the anti-Spam filters and decrease their effectiveness. In previous sections we have discussed various possible Spammer tricks and attacks include tokenization attack, obfuscation attack and statistical attacks etc. that a Spammer can use to reduce the efficiency of Spam filters.

Techniques that control Spam at the client side only decrease the costs associated with recipients. These techniques do not reduce the costs associated with network bandwidth to carry heavy load of Spam and email servers to process Spam emails. Spam should be stopped before it reaches the receiving email server to reduce these costs. To actually reduce the volume of Spam, a negative feedback loop is required in the system. If Spammers would be made to bear more of the costs, they would be less inclined to send large volumes of Spam.

REFERENCES

[1] S. Anthony, S. "Microsoft shuts down spam behemoth rustock, reduces worldwide spam by 39%." http://downloadsquad.switched.com/2011/03/18/microsoft-and-feds-shuts-down-spam-behemoth-rustock-reduces-worldwide-spam/, 2011.

[2] Aycock, J. and Friess, N. "Spam zombies from outer space." In EICAR, pages 164–179, 2006.

[3] Clark, K. P. "A survey of content-based spam classifiers. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.173.2685, 2008.

[4] Conner, R. C. "Popular spammer tricks. http://www.rickconner.net/spamweb/tricks.html, 2008.

[5] Hayes, B. "How many ways can you spell v1@gra?" Scientific American, 95(4):298–302, 2007.

[6] Heron, S. "Technologies for spam detection." Network Security, 2009(1):11–15, 2009.

[7] Hoanca, B. "How good are our weapons in the spam wars?" Technology and Society Magazine, IEEE, 25(1):22–30, 2006.

[8] Jezek, K. and Hynek, J. "The fight against spam - a machine learning approach." In International Conference on Electronic Publishing, pages 381–392, 2007.

[9] Kassner, M. "The top 10 botnets. http://www.thespamcryer.com/the-top-10-botnets/. 2010.

[10] Kim, W., Jeong, O.-R., Kim, C., and So, J. "The dark side of the internet: Attacks, costs and responses." Information systems, 36(3):675–705. 2011.

[11] Lowd, D. "Good word attacks on statistical spam filters." In Proceedings of the Second Conference on Email and Anti-Spam (CEAS). 2005.

[12] MessageLabs. "Messagelabs intelligence: 2010 annual security report." Technical report, MessageLabs. 2010.

[13] Raz, U. "How do spammers harvest email addresses?" http://www.private.org.il/harvest.html

[14] Wosotowsky, A. and Winkler, E. "December 2009 spam report." Technical report, McAfee Research Report. 2009.