Camouflages and Token Manipulations- The Changing Faces of the Nigerian Fraudulent 419 Spammers

LONGE, Olumide Babatope
Dept. of Computer Science,
University of Ibadan, Ibadan, NIGERIA
longeolumide@yahoo.com

CHIEMEKE, Stella Chinye.
Dept. of Computer Science,
University of Benin, Benin City, NIGERIA
schiemeke@yahoo.com

ONIFADE, Olufade .F. Williams
Laboratoire Lorrain de Recherche en Informatique et ses Application (LORIA)
LORIA- Campus Scientifique, B. P. 239, 54506 Vandoeuvre-Lès-Nancy, France
fadowilly@yahoo.com

LONGE, Folake .Adunni
The African Regional Centre for Information Science,
University of Ibadan, Ibadan, NIGERIA
adefolakelonge@yahoo.com

Abstract

The inefficiencies of current spam filters against fraudulent (419) mails is not unrelated to the use by spammers of good-word attacks, topic drifts, parasitic spamming, wrong categorization and recategorization of electronic mails by e-mail clients and of course the fuzzy factors of greed and gullibility on the part of the recipients who responds to fraudulent spam mail offers. In this paper, we establish that mail token manipulations remain, above any other tactics, the most potent tool used by Nigerian scammers to fool statistical spam filters. While hoping that the uncovering of these manipulative evidences will prove useful in future antispam research, our findings also sensitize spam filter developers on the need to inculcate within their antispam architecture robust modules that can deal with the identified camouflages.

Keywords: 419-Spammers, Bayesian, Outbound-filtering, SPAMAng, Filters, Nigeria.

1. Introduction

Some spammers are legitimate businesses, engaged in overly aggressive marketing efforts, because there are no formal limits on their actions. In spite of the challenges created by needing to work at an international level, there is a reasonable expectation that legal strictures, both laws and contracts, will constrain these businesses to a tolerable level [25]. In contrast, *rogue* spammers actively seek to avoid accountability, to subvert barriers to their traffic, and to acquire unwitting and unwilling participation of machines owned by others. Independent of the legal details, the best social model to use for analyzing this latter group is crime. Often the activities do not violate particular laws, but what is most important is that the style of a spammer's conduct is the same as that of a criminal.

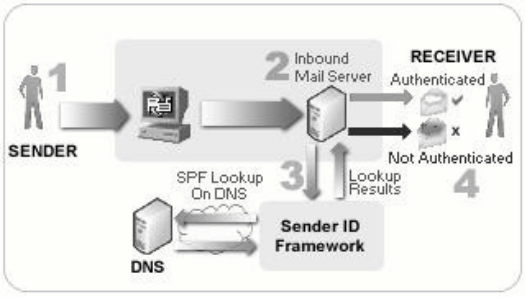

Figure 1: SPF Mechanism
(Source: Wong & Schlit [29])

Unfortunately, the technical and operational world of spamming has also developed in scale and sophistication. Spamming used to entail one sender and one sending machine. Its performance was limited by the capacity of that machine and the bandwidth of its Internet connection. Today, rogue spammers control vast armies of compromised systems, called *zombies*, as shown in Figure 1. Zombies are

owned by legitimate users who are unaware that their system has been compromised and is being used for spamming.

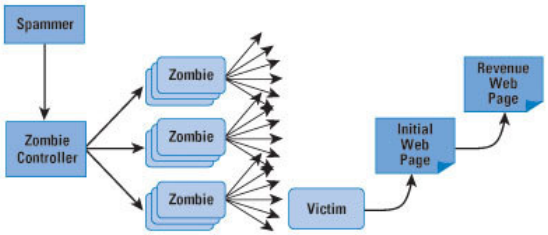

Figure 2: Rogue Spammer Control Network

The community of rogue spammers is remarkably well organized, and Nigerian 419 spammers fall into this category [24]. It has become an extensive, underground economy. Some participants specialize in developing methods for breaking through filters. Others take over machines and turn them into zombies. Others sell the use of a zombie collection for periods of spamming. The estimated number of zombie systems is in the many tens of millions. After spam delivery, recipients often "click" to a transaction Web page. Web hosting is provided at multiple levels, in order to obscure the server side of the process, further reducing accountability. Typically, spammers have the classic goal of selling products. However, they also can have political or religious motivations or even blatantly criminal intent, such as extortion. The ability to send very large number of messages to a specific destination gives spammers a tool that can be used to threaten an organization with a denial of service attack on their network [25].

2. Related Literature

Spam behavior is not simply a matter of one concept drifting to another in succession, but instead it is a superimposition of constant, periodic and episodic phenomena [17]. Researchers have shown that spam content changes over time. Swan and Allan [26] employed a 2-t test to discover "bursty" topics in daily news stories. Their test was designed to determine whether the appearance of a term on a given day was statistically significant. They concluded that that spam has complex time-varying behavior. Some terms recur intermittently, such as *adult, click,free, hot and removed*. Others are episodic, for instance the terms common in a "Nigerian 419 scam" such as *Nigeria, Lagos, assistance, beneficiary* and terms in a "pornstar video" such as *awesome, pornstars, jenna, lauren, nicki, orgy* also burst at some points. Terms such as *Christmas* burst late in the year and presumably reappears every year around the same time.

Spammers typically use purpose-built applications to distribute their spam [27]. Greylisting tries to deter spam by rejecting email from unfamiliar IP addresses, by replying with a soft fail (i.e. 4xx). It is built on the premise that the so-called 'spamware' does little or no error recovery, and will not retry to send the message. Any correct client should retry; however, some do not (either due to a bug or policy), so there is the potential to lose legitimate email. Also, legitimate email can be unnecessarily delayed; however, this is mitigated by source IP addresses being automatically whitelisted after they have successfully retried once. An analysis performed by Levine [28] over a 7-week period (covering 715,000 delivery attempts), 20% of attempts were greylisted; of those, only 16% retried. Careful system design can minimise the potential for lost legitimate email; certainly greylisting is an effective technique for rejecting spam generated by poorly implemented spamware.

SMTP path analysis [21] learns the reputation of IP addresses and email domains by examining the paths used to transmit known legitimate and spam emails. It uses the 'received' line that the SMTP protocol requires that each SMTP relay adds to the top of each email processed, which details its identity, the processing timestamp and the source of the message. Despite the fact that these headers can easily be spoofed, when operating in combination with a Bayesian filter, overall accuracy is approximately doubled.

Tom [17] opined that it will be difficult to estimate how much we can expect spam as a concept to drift over time, in part because no metric of concept drift has been adopted by the antispam community. Cunningham et al. [18] construct a case-based reasoning classifier that can track concept drift. They propose that the classifier both adds new cases and removes old cases from the system collection, allowing the system to adapt to the drift of characteristics in both spam and legitimate mails. An initial evaluation of their classifier suggests that it outperforms naive Bayesian classification. This is unsurprising given that naive Bayesian filters attempt to learn a "unified spam concept" that will identify all spam emails; spam email differs

significantly depending on the product or service on offer. In [19] the Teiresias pattern discovery algorithm was applied to email classification. Given a large collection of spam emails, the algorithm identifies patterns that appear more than twice in the corpus. Negative training occurs by running the pattern identification algorithm over legitimate email; patterns common to both corpora are removed from the spam vocabulary. Successful classification relies on training the system based on a comprehensive and representative collection of spam and legitimate emails. Experimental results are based on a training corpus of 88,000 pieces of spam and legitimate emails. Spam precision was reported at 96.56%, with a false positive rate of 0.066%.

2.1 Techniques Adopted By the Nigerian Spammers

In order to reach a large volume of users, Spammers require an equally large number of e-mail addresses. These are usually collected in three different ways. By using mail harvesters to scavenge for e-mail addresses listed on web sites and message boards (particularly USENET groups), by performing a dictionary attack (pairing randomly generated usernames with known domain names to 'guess' a correct address) or by purchasing address lists from other individuals or organizations. Once they have addresses, Spammers can use programs known as bulk mailers to automate the sending of Spam. These programs can send huge volumes of e-mail messages in a small amount of time. Some bulk mailing programs use open-relays (e-mail servers that allow unauthorized users to send e-mail) to send messages, effectively hiding the true address of the Spammers. Bulk mailers can also fabricate the *from* address in e-mail message headers to further hide the identity of the Spammer [31].

Another technique spammers utilize to send e-mails is with the use of *zombie network*s, also know as *bot network*s. Zombie is the term given to a computer that has been infected by a virus, worm, or Trojan Horse, which allows remote entities to take control and use it for their own (usually illegal) purposes. A large amount of these computers, usually called a *network* or *army* can be co-opted to send spam e-mails, requiring little of the spammer's own computing power and network bandwidth. This technique is also popular as it protects the identity of the spammer. What follows is a short summary of some of the major techniques and tactics adopted by the Nigerian 419 scammer.

2.2 Current Filters Against 419 Mails

Dealing with the 419 Spam problem at the destination will not always yield the desired results as Spammers have evolved different measures to beat Spam filters at these nodes.. This is particularly so with 419 mails. Available benchmarks though promising, still reveals some degrees of inefficiency when compared with the rate of false positives (Process Software, 2007). SPAMAng, an outbound filtering to combat Nigerian Fraudulent 419 mails from the source was proposed in [24] Other major challenges are discussed below:

(a) The fact that the design of efficient filtering systems depends on spamicity measures means that accuracy must be a goal when designing antispam systems. Accurate spamicity measures can only be obtained if the filter designers have a balanced corpus of Spam and real mails (ham) from the domain at which the filtering efforts are targeted. Unfortunately, most Spam designers have easy access to the Nigerian 419 mail corpus but are disadvantaged at having a corpus of ham mails originating from the source at which the Spam mails have emanated. The consequences of these are the occurrence of false positives, false negatives and lack of efficiency in the filtering systems. The contribution of Spam mails in training the text classification engine is as important as that of ham mails.

(b) Generic filtering, where a single filtering package is designed to filter different types of Spam becomes disadvantageous in a situation where there is serious deviations in the test categories and manipulations by Spammers in specific domain. This is a major challenge of using existing filters to deal with the Nigerian 419 mails. Rule-based approaches are as deficient as non-domain specific approaches in filtering junk mails that have diversified text categories. This is due to the fact that logical rule sets usually make rigid binary decisions as to whether to classify a given message as junk [30].

2.3 Challenges of Collaborative Filtering Against 419 Mails

Alan and Mards [20] suggested movement of spam filters away from monolithic repositories situated on central servers towards dynamic knowledge bases located on local servers. They see content-based filters tending towards collaborative filters, whereby email is filtered at the mail server using content-based techniques, with users feeding information back about false positives and false negatives. This feedback enables the spam filter to track concept drift in spam and to be retrained in the case of false positives. While these filters can achieve statistically impressive accuracy rates, they remain prone to false positives.

We feel that another important but highly neglected factor is the validation of the identity of the client that is feeding information back about false positives and false negatives. Are they casual e-mailers or spammers? If they are spammers, then collaborative filtering in the context of this paper is prone to creating more troubles for the troubled. Sadly, the "*mark as spam*" features provided to enable feedbacks about wrong classifications in most e-mail platforms are used by unscrupulous Nigerian 419 spammers to fool Bayesian filters. Most classification mechanisms in email applications require users to place messages into fixed categories. As a result of the fact that categories shifts, placing the onus of categorizing and recategorizing e-mail either as spam or ham on the users requires a refinement policy that can assist users in making such fuzzy decisions. People's categories shift over time, and frequently become dated and decline in usefulness. Recategorization is time-consuming because users must move each message to the new category. Often old categories are never fully removed after recategorization leading to "category drift." [22][23]. Subject line drifts are also used in which the subject line is aligned with the sender identity. For instance the sender identity reads *FROM LONGE OLUMIDE* and the subject line also reads *FROM LONGE OLUMIDE*

Parasitic spamming is another method adopted by the Nigerian Spammer. If a user's machine has been compromized by a spammer (or his proxy), any aspect of the machine can be subverted. While current bots merely use their own SMTP program to send out spam, another alternative is to hook into the existing TCP/IP stack or MAPI infrastructure (on Windows). In a p-spam-bot, this hook would be used to monitor for email being sent from the system, which is then modified to contain spam as well as the original message. The spam has therefore effectively parastically 'infected' the original message, hence the name 'parasitic spam'. Likewise, if an email server or relay is compromised, the spammer will have access to a greater volume of email to which to attach spam. The concept of modifying legitimate email is not new. There has been the dubious custom of free email services and some mailing lists to append an advertisement or some other message as a signature to the email (see Fig. 1). Because these 'signatures' are often perceived as a nuisance in mailing lists, some mailing list software include tools for stripping these signatures. This works because the ads tend to be fairly predictable and false positives can be kept to a minimum, just like parasitic viruses. P-spam is similar, but trickier, because the message can be altered in many more ways than just in the signature.

3.0 COMPUTING SPAMICITY

Once a filter has the list of tokens in a message, it computes the probability that the appearance of the word in a message makes the message Spam or ham (real mails) as a factor of the frequency of occurrence of the same words in the token databases. This probability value assigned to each word is commonly referred to as *spamicity*, and ranges from 0.0 to 1.0. A spamicity value greater than 0.5 means that a message containing the word is likely to be Spam, while a spamicity value less than 0.5 indicates that a message containing the word is likely to be ham. A spamicity value of 0.5 is neutral, meaning that it has no effect on the decision as to whether a message is Spam or not.

In simplest terms, the spamicity is based on the number of times a word occurs in Spam messages as opposed to the number of times it occurs in non-Spam messages. For example, if a word has occurred 50 times in Spam messages but only 2 times in non-Spam messages, a message that contains it has a good chance of being Spam. The opposite is also true. If a word appears 50 times in non-Spam messages but only 2 times in Spam messages, a message that contains it is not very likely to be Spam. The neutral spamicity domains are occupied by words that commonly occur about the same frequency in Spam and non-Spam messages.

Expressed mathematically,

$$Ham\,\Pr obability\,is\;\;given\,as = \frac{Token\,Frequency\,in\,Ham\,Messages}{Number\,of\;Ham\,Messages\,Used\,for\,Training\,Filter}$$

$$Spam\,\Pr obability = \frac{Token\,Frequency\,in\,Spam\,Messages}{Number\,of\;Spam\,Messages\,Used\,for\,Training\,Filter}$$

$$Spamicity\;\; = \frac{Spam\;\Pr obability}{(Ham\;\Pr obability\;\; + Spam\;\Pr obability)}$$

In basic terms, Bayes' Formula allows us to determine the probability of an event occurring based on the probabilities of two or more independent evidentiary events. Assuming that the variables a and b are the probabilities of two evidentiary events, the probability would be equal to:

$$\Pr obability = \frac{ab}{ab\; + (1-a)(1-b)}$$

For three evidentiary events a, b, and c, the formula expands so the probability is equal to:

$$\Pr obability = \frac{abc}{ab\; + (1-a)(1-b)(1-c)}$$

In this fashion, the formula can be expanded to accommodate any number of evidentiary events.

3.1 Creating Bayesian Token Database

Before mails can be filtered correctly using Bayesian statistics, the filter designer needs to generate a history for each word or token (such as the $ sign, IP addresses, domains etc.) A probability value is then assigned to each word or token; the probability is based on calculations that take into account how often that word occurs in spam as opposed to legitimate mail. In our approach, this will be done by analyzing the users' outbound mail and by analyzing known spam. All the words and tokens in both pools of mail are analyzed to generate the probability that a particular word is spam. For example, if the word "mortgage" occurs in 400 of 3,000 spam mails and 5 out of 300 legitimate e-mails, its spam probability is:

(400/3000) / (5/300 + 400/3000) = 0.8889.

3.2 Designing Efficient Filtering Systems

The fact that the design of efficient filtering systems depends on spamicity measures means that accuracy must be a goal when designing Antispam systems. Accurate spamicity measures can only be obtained if the filter designers have a balanced corpus of Spam and real mails (ham) from the domain at which the filtering efforts are targeted. Unfortunately, most Spam filter designers have easy access to the Nigerian 419 mail corpus but are disadvantaged at having a corpus of ham mails originating from the source at which filtering is targeted hence the occurrence of false positives, false negatives and lack of efficiency in the filtering systems.

The contribution of Spam mails in training the text classification engine is as important as that of ham mails. Secondly, generic filtering, where a single Antispam system is designed to filter different types of Spam becomes disadvantageous in a situation where there is serious deviations in the text categories and manipulations by Spammers in specific domain. This is a major challenge of using existing filters to deal with the Nigerian 419 mails. Rule-based approaches are as deficient as non-domain specific approaches in filtering junk mails that have diversified text categories. This is due to the fact that logical rule sets usually make rigid binary decisions as to whether to classify a given message as junk or not [30]

The most important factor on which a Bayesian filters based its decision to flag a message as Spam or ham is the message content. This decision is aided by tokenizing the message in the form of a table of text categories identified in Spam and non-Spam messages. These tokens are then compared with the ones in the Spam and non-Spam database tokens with which the antispam system has been trained in order to determine the Spamicity of the identified tokens. It follows then, that the ability of the filter designer to train the antispam with the right tokens with high Spamicity (in the case of Spam) will enhance the efficiency of the filtering system in quickly identifying Spam messages. The opposite is also true for ham (words with low

Spamicity must be used to train the filter in order to identify ham correctly. In most cases, words common to both ham and Spam possess low spamicity values. We have identified a corpus of text categories with high spamicity within the "Nigerian 419" or "yahoo" mails.

3.3 Spamicity Measures

Different forms of Spam have peculiarities in the use of language. Therefore an understanding of the nature of text categories and possible manipulations by spammers to fool Spam filters within specific Spam corpus is imperative in the design of effective filters.

3.3.1 Training Sets

Building on an earlier research (Longe et al, 2007) we improved on the training text for NIMFilter to train the text classification engine for the development of SPAMAng (SPAM Management for Nigerian Mails), an outbound filtering antispam system. A total of 112700 mails partitioned into two equal halves were used for the experiment. These mails were harvested over a three year period. Existing corpus at the 419 coalition website, Nigerian Fraud Mail Gallery, Process Software Website, the Ling Corpus and other Spam mails sent into mail accounts specifically opened for this research constitute the manually identified Spam messages used for determining the Spamicity of text categories. The ham messages consists of regular mailing contents common to the Nigerian e-mailer in order to balance the filtering capacity. An observation of profiled mails showed that the 419 Spammers use some subtle manipulations such as word stemming, deliberate spelling errors, word toggles, insertion of underscores and a combination of American and British English to fool Spam filters.

3.3.2 Finding Spam Based on the Bayesian Filter – A Simple Example

Suppose that Virgin Nigeria Airlines flights between Lagos and New York City are delayed 75% of the time if it's raining. Also suppose that if a flight is scheduled to leave Lagos before noon, it's only delayed 10% percent of the time (rain or shine). If you take a Virgin Nigeria flight from Lagos to New York City on a rainy day, and the flight is scheduled to depart before noon, what are the odds the flight will be delayed? Since there are only two pieces of evidence to consider (the weather conditions and the scheduled departure time), we can use the basic form of Bayes' Formula to solve this problem. The probability that the flight will be delayed on a rainy day (75%, or 0.75) is represented by the variable *a*, and the probability that the flight will be delayed if it's scheduled to leave before noon (10%, or 0.10) is represented by the variable *b*.

Filling in Bayes' Formula from above, we see that the probability is equal to:

$$\Pr obability = \frac{(0.75)(0.10)}{(0.75)(0.10) + (1\ 0.75)(1 - 0.10)} = 0.25$$

……(14)

Solving this equation yields a probability of 0.25, or a 25% chance that the flight will be delayed.

3.3.3 Observation

An important observation from this example is that we're dealing with *independent* events – the probability of one event has no impact on the other event. In the case of our example, there's a 75% chance the flight will be delayed on a rainy day regardless of whether or not it's scheduled to leave before noon. The probability of 75% includes both cases where the flight leaves before noon, and cases where it doesn't. Likewise, the fact that there's a 10% chance of the flight being delayed if it leaves before noon takes into account all flights – not just ones that leave on rainy days.

Using this concept to filter spam messages is known as *naive* Bayesian filtering, because we don't take into account the relationships between the various words contained in e-mail messages. While it may certainly be true that a message containing all three of the words "clinical", "trial", and "Viagra" is never spam, all the naive Bayesian filter knows is that the words "clinical" and "trial" occur mostly in non-spam messages while the word "Viagra" occurs mostly in spam messages.

4. Data Analysis

Since a major challenge in filtering is the level of precision and recall, ham messages that fall into other categories of Internet correspondence peculiar to the Nigerian internet terrain were selected for use. These constitute the major content that can produce false positives as they contend with Spam mails in the filtering system. The Tables below

presents carefully selected text categories in Nigerian Scam mails messages, their frequency of occurrence, Spam probabilities, ham probabilities and Spamicity in descending order. Table 1 reveals the nature of manipulations some of the selected words are subjected to by Spammers in order to fool Spam filters. Tables 2 and 3 presents our observation of the changes in Spamicity as observed when some of the selected words were manipulated in one way or the other in Spam mails.

Table 1: Token Manipulations And Their Frequencies Of Occurrence

Token Compounded/ Manipulate	Nature of Manipulation	Frequency of Occurrence in Spam Messages	Frequency of Occurrence in Ham Messages
Beneficiary	Beneficary (spelling)	13	0
Cooperation	Co-operation (hyphenation)	32	09
Date	Date ofbirth (compound/spelling)	34	0
Director	Directr (spelling) DIrector (Toggle)	23 45	0 0
Discovered	Disc0vred (spelling)	35	0
Documents	DOCUMENt (Toggle)	21	0
Dollar	Dolar (spelling) Dollarrs (Spelling)	27 09	3 1
Fax	Faxnumber (compound)	53	5
First	Firstname (compound)	3	23
Foreign	Foreing (Spelling) Foreign Account (compound)	27 45	1 15
Funds	Funds-transfer (compund/hyphenated) Fund-transfer (compund) Fun-transfer (Spelling error)	65 75 08	05 0 0
Invoice	Invoce (Spelling Error) Over-invoiced (Compound) Over-invoice (Grammar)	26 32 32	1 1 0
Joint	J0int (Toggle) Jonit-business (compound)	15 2	0 0
Lottery	LOTTERy (Toggle) Lotery	15 5	0 0
Mobile	MobiLe (toggle) Mobile-number (hyphen/Compound)	12 55	0 8
Next	Nxt (spelling) Next-of-kin Next_of-Kin (Toggle/underscore) Nextofkin (Compound)	5 98 18 27	0 5 0 0
Offset	Off-set (hyphenation)		12
Partners	Partiners (spelling) Pcitners (stemming)	23 19	0

Table 2: Changes In Frequency of Occurrence For Selected Tokens

S/NO	Token	Old Frequency in Spam messages	New Frequency in Spam messages	Old Frequency in Ham Messages	New Frequency in Ham Messages
1	Beneficiary	277	290	7	7
2	Cooperation	104	136	12	21
3	Director	291	359	13	13
4	Discovered	237	272	16	16
5	Documents	398	419	121	121
6	Dollar	676	712	93	97
7	Invoice	100	126	12	13
8	Joint	187	202	25	25
9	Lottery	765	795	2	2
10	Mobile	767	779	324	324
11	Next	895	900	234	234
12	Partner	34	76	12	12
13	Personal	102	114	30	30
14	Please	2800	2899	223	227
15	Swift	109	121	5	5
16	Transferred	134	193	56	58

Table 3: Observation Of The Changes In SpamicitiesFor Selected Tokens

Old Spam Probabilities	*New Spam Probabilities*	*Old Ham Probabilities*	*New Ham Probabilities*	*Old Spamicities*	*New Spamicity*
0.1154167	0.120833333	0.0029167	0.002916667	0.975352	1
0.0433333	0.056666667	0.005	0.00875	0.896552	1
0.12125	0.149583333	0.0054167	0.005416667	0.957237	1
0.09875	0.113333333	0.0066667	0.006666667	0.936759	1
0.1658333	0.174583333	0.0504167	0.050416667	0.766859	1
0.2816667	0.296666667	0.03875	0.040416667	0.879064	1
0.0416667	0.0525	0.005	0.005416667	0.892857	1
0.0779167	0.084166667	0.0104167	0.010416667	0.882075	1
0.31875	0.33125	0.0008333	0.000833333	0.997392	1
0.3195833	0.324583333	0.135	0.135	0.703025	1
0.3729167	0.375	0.0975	0.0975	0.792737	1
0.0141667	0.031666667	0.005	0.005	0.73913	1
0.0425	0.0475	0.0125	0.0125	0.772727	1
1.1666667	1.207916667	0.0929167	0.094583333	0.926232	1
0.0454167	0.050416667	0.0020833	0.002083333	0.95614	1
0.0558333	0.080416667	0.0233333	0.024166667	0.705263	1

Figures 3(a-f5) depicts the graphical status of text categories as the computation progresses.

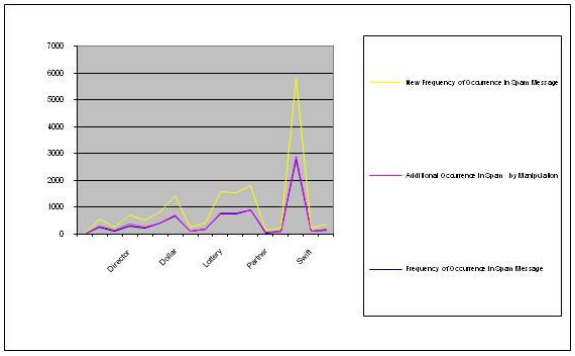

Fig 3(a): Changes in Frequencies Spam Messages

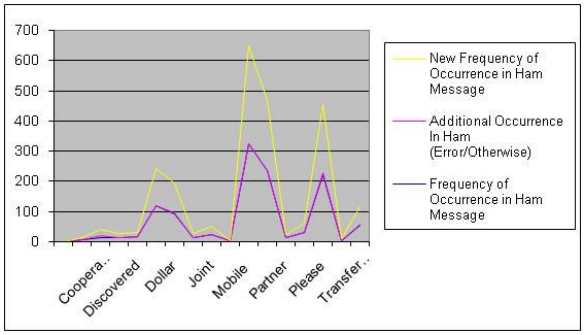

Fig 3(b): Changes in Frequencies in Ham Messages

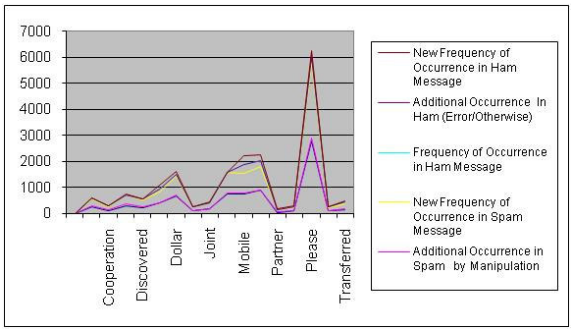

Fig 3(c): Additional Occurrences in Spam by Manipulation

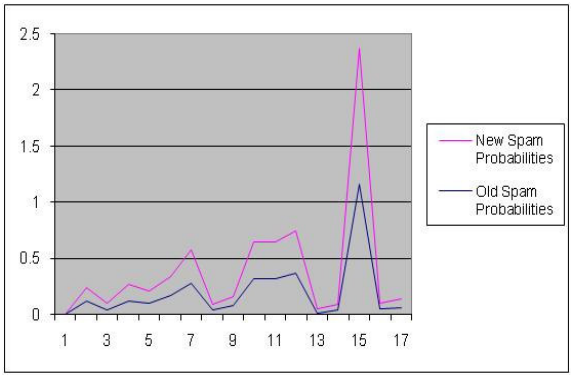

Fig 3.(d): Old and New Spam Probabilities

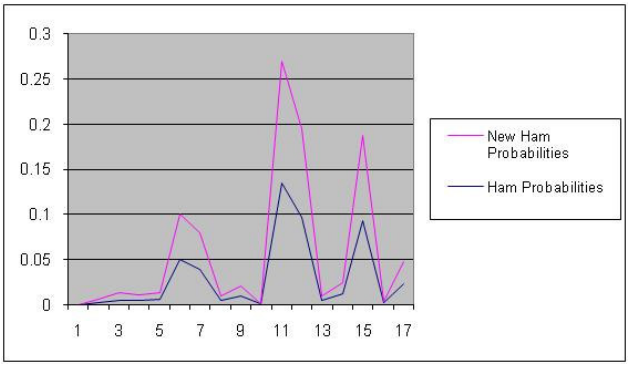

Fig 3(e): New Ham Probabilities

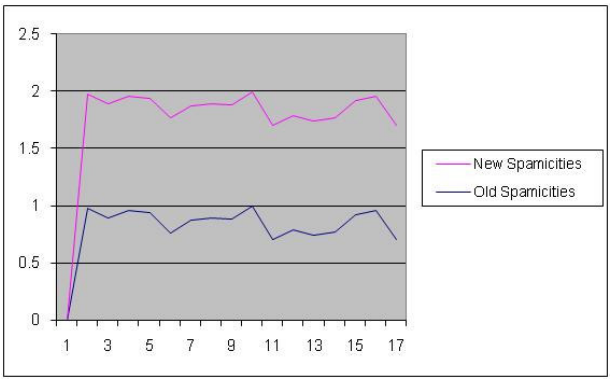

Fig 3.(f): Old and New Spamicities

VI EXPERIMENTAL ON 419 SPAMMING TECHNIQUES

We analyzed a set of preselected 419 spam mails numbering 1200 categorized as shown in the table below. Similar characteristics in some of the mail necessitated collapsing them into the same spamming domain. Results from the analysis carried out by 3 groups of researchers are depicted in the Fig 4 and 5 and summarized Table 4 below.

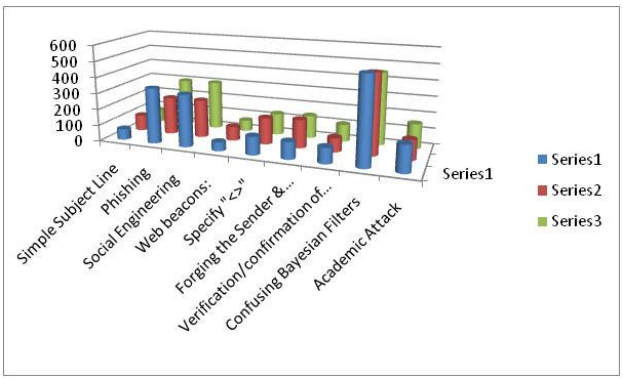

Fig. 4: Graph of Individual Group Responses

Table 4: Categories of Spam Mails

	Spamming Technique	No Of Mails In Category By Groups			
		Grp 1	Grp 2	Grp 3	**TOTAL**
	Simple Subject Line: **Spammers use a one-word subject line. Usually there is nothing more than a link in the body of the e-mail, which allow many e-mails to slide by the server undetected.**	67	98	79	**244**
2	Phishing: **Phishing is usually combined with spoofing. A spoofer will imitate companies and use forms inside of e-mails to gather personal information about the user. Spoofing: This is e-mail in which the sender's name is fictitious. 419 spammers spoof real companies. Domain Spoofing - Using an invalid or fake domain in the from line**	345	234	301	**880**
3	Social Engineering: **A common tactic is using a personal, and even touching subject lines to get a person to open spammer e-mail. "Hello," "I miss you," and "Your document is attached"**	325	237	304	**866**
4	Web beacons: **E-mails sent by spammers that contain an image and sometimes an invisible image to the recipient.**	54	87	69	**210**
5	**Specify "<>" : One of the most commonly used tactics is to specify "<>" as the sender. This tactic is based on a standard feature, present in all mail servers. By specifying the "<>" sender, they trick the server to deliver the message to the user's mailbox, since the "<>" corresponds to the server itself.**	**113**	**165**	**134**	**412**
6	**Forging the Sender & Sender Header: Specify the same information to the sender header as to the recipient header, to look like the message. Another filter bypassing tactic is to forge the sender and specify the same information to the sender header as to the recipient header, to look like the message was sent from the recipient's owner's account to himself.**	**106**	**176**	**142**	**424**
7	Verification/confirmation of delivery: **Spammers try to validate the aexistemnce of addresses by using software such as High Speed Verifier, or by tricking the receipt into manually verifying the e-mail by asking him or her to "unsubscribe".**	97	87	107	**291**
8	**Confusing Bayesian: Crafting messages to confuse and disturb statistic or keyword filters that use the Bayes algorithm. Word Obscuring/obfuscation - Text Manipulations, misspelling words, putting words into images, word toggling, toggling words and numbers etc. MIME Attacks - Putting non-spam content in one body part and spam content in another. Character Encoding - Pharmacy renders into Pharmacy.**	**534**	**497**	**452**	**1483**
9	**Academic Attack - Resending and forging conference and journal invitations**	**165**	**124**	**156**	**445**

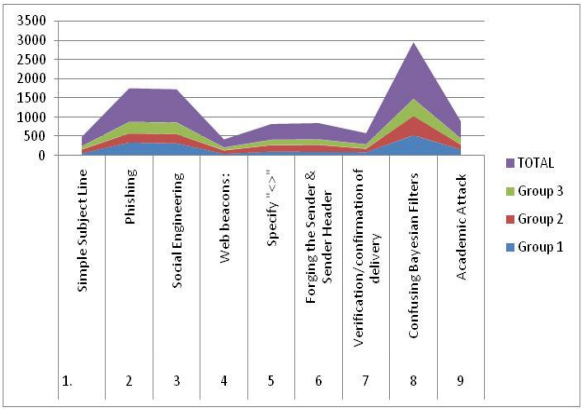

Fig. 5 Graph of Cumulative Group responses

5. Conclusions

Effort at developing *SPAMAng* for filtering fraudulent mails from the origin necessitates the adoption of the Bayesian model of filtering. We are therefore confronted with the usual challenge that Bayesian filters require the entire message to be received before analysis and are resource intensive since calculating Bayesian probabilities requires significantly more processing power than simply querying a list. Therefore any form of improvement on spamicity information, or the selection of tokens that aids the calculation of spamicity in order to quickly specify tokens with high Spamicities is a welcome development that will help filters achieve a higher precision, efficient recall and consequently low false positives.

Apart from his own mentality and the strength of his motivations, the criminal also needs to see the path of crime ahead of him clear of obstacles. If every single individual were to put up obstacles of their own, no matter how small, the crime path will seem to be far less lucrative in the eyes of even the most desperate criminal. The outbound mail filtering paradigm is an alternative that must be rigorously explored in the fight against 419 spam mails. The Internet community must engage in a collective effort to curb the Internet of the demeaning crimes it is helping to fuel.

Different forms of Spam have peculiarities in the use of language. Therefore an understanding of the nature of text categories and possible manipulations by Spammers to fool Spam filters within specific Spam domain is imperative in the design of effective filters. Total spamicity improves as a result of the increase in content spamicity made available by identifying possible text manipulations.

The lessons learned when training the SPAMAng's text classification engine based on our findings are as follows:

(a) All compound and hyphenated words should be tokenized. Hyphenations can be removed.
(b) Spell checking will assist in removing deliberate errors, mixture of alphabets and texts(as in J0INT; note that zero is used instead of the alphabet 0) and word-stemming by matching acceptable English words in the database with that on the mail.
(c) Convert all mails to upper or lower case to deal with text toggling.
(d) Underscores within mail contents should be removed except when referring to an e-mail address. All messages should be converted to either American or British texts using specific dictionary.

Fighting spam must be a collaborative effort, which will benefit from using tools and standards that aid in exchanging information and performing coordination. To this end, standard methods of reporting spamming events, of characterizing particular spam, and of sending spam control data can be helpful. Some work in that direction should be encouraged. Fighting spam also requires global operations collaboration; this will be aided by services to facilitate interactions between network administrators speaking different languages as well as law enforcement agencies across nations. It is also likely that there should be standards for the syntax and semantics of whitelists and blacklists in inbound mail filtering systems. On a more general note, e-mail addresses are very valuable commodities using them wisely can help users avoid both the junk e-mail and the frustration of dealing with them. Users can protect their inboxes from spam by following the simple rules listed below:

[1] Never accept the option to "click here to unsubscribe" or send a reply. That tells the spammer that they have a valid e-mail address. E-mail users may actually start getting MORE spam instead!

[2] When submitting forms over the Web, opt out of any newsletter or mailing list. Many companies share or sell their e-mail lists so once users are on their list, they will soon be on another, and another, and another.

[3] Refrain from forwarding chain letters, humor, news flashes, or even family messages. Spammers receive these messages too, and then extract the embedded address list for their own use.

[4] Use a disposable e-mail address (Yahoo! ®, AOL ®, *etc*.) when registering with retail Web sites or message boards. These are sure-fire targets for spam. By using a different address, you can keep your business address clean.

[5] Select longer, more complicated e-mail names. Shorter addresses tend to receive more spam mail than longer ones, according to The Center for Democracy and Technology, a policy group.

[6] Provide a different address for your friends and family. You may be careful with your business address, but if a friend or relative lets your address get out, all your other efforts are wasted.

[7] Run an anti-virus engine on your home PC and keep it current. Many viruses target the Outlook address list. If your home PC is used for work it has all of your important addresses. A personal firewall is a good idea too.

[8] Treat your e-mail address with respect. Give it out with the same consideration you use for your home address or personal cell phone number.

References

[1] Drewes, R. An artificial neural network Spam classifier. , Available online at http://www.interstice.com/drewes/cs676/spam-nn/spam-nn.html , 2002

[2] Chiemeke , S. and Longe, O.. Probability Modeling For Improving Spam Filtering Parameters. Unpublished Manuscript, 2007.

[3] Chih-Chien, W. . Sender and Receiver Addresses as Cues for Anti-Spam Filtering. Journal of Research and Practice in Information Technology, Vol. 36, No. 1. pp 3-7, 2003

[4] Damiani, E, Vimercati, S. Paraboschi, S & Samarati, P. An Open Digest-based Technique for Spam Detection. Paper presented to The 2004 International Workshop on Security in Parallel and Distributed Systems, San Francisco, CA USA, 2004.

[5] M . Delany. Domain-based Email Authentication Using Public-Keys Advertised in the DNS (DomainKeys). Available online at http://www.ietf.org/internet-drafts/draft-delany-domainkeysbase-03.txt ,2005.

[6] J. Golbeck and J. Hendler. Reputation network: Analysis for email filtering. In Proceedings of the First Conference on Email and Anti-Spam, Mountain View, CA, July 2004.

[7] P. Graham. A Plan for Spam. Available online at www.paulgraham.com/spam.html., 2002.

[8] G. Hulten, J. Goodman and R. Rounthwaite. Filtering spam e-mail on a global scale. In Proceedings of the 13th international World Wide Web conference on Alternate track papers \& posters, ACM Press, New York, NY, USA, pp. 366-7, 2004.

[9] O. Longe and S. Chiemeke. The Design and Implementation of An E-Mail Encryptor for Combating Internet Spam. Proceedings of the Ist International Conference of the International Institute of Mathematics and Computer Sciences. Pp 1 – 7. Covenant University, Ota, Nigeria. June, 2006.

[10] J. Lyon and M. Wong. Sender-ID: Authenticating E-mail. Available online at http://www.ietf.org/internet-drafts/draft-lyon-senderid-core-01.txt. , 2005.

[11] C. O'Brien and and c. Vogel. Spam filters: Bayes vs. Chi-squared; Letters vs. Words.In ISICT '03: Proceedings of the 1st international symposium on Information and communication technologies. Trinity College Dublin, 2003.

[12] C. Pfleeger and L. Pfleeger. Security inComputing, 3rd Int edn, Prentice Hall PTR, Upper Saddle River, N.J, 2003

[13] B. Rajkumar, M. Tianchi, S. Rei, S. Chris and S. Willy. Domain Specific Blacklists. Proceedings of the Fourth Australian Information Security Workshop (AISW-NetSec) 2006.

[14] G. Sakkis, I. Androutsopoulos, G. Paliouras,V. Karkaletsis, C. Spyropoulos and P. Stamatopoulos. A memory-based approach to anti-Spam filtering for mailing lists. Information Retrieval. Vol. 6, No 1 Pp 48–73, 2003.

[15] The Nigerian E-Mail Fraud Gallery. Available online at www.potifos.com/fraud, 2005.

[16] K. Yoshida, F. Adachi, T. Washio, H. Motoda, T. Homma, A. Nakashima , H. Fujikawa and K. Yamazaki, K.. Density-based spam detector. In KDD '04: Proceedings of the 2004 ACM SIGKDD international conference on Knowledge discovery and data mining, pages 486–493. ACM Press, 2004.

[17] Tom Fawcett : In vivo. spam _ltering: A challenge problem for KDD. SIGKDD Explorations. Volume 5,Issue 2 - Page 140. 2002

[18] Cunningham P, Nowlan N, Delany S, Haahr M. A case-based approach to spam filtering that can track concept drift. In: ICCBR'03 workshop on long-lived CBR systems; June 2003.

[19] Rigoutsos I, Huynh T. Chung-kwei: a pattern-discovery-based system for the automatic identification of unsolicited e-mail messages (spam). In: Conference on email and anti-spam; 2004.

[20] Alan Gray and Mads Haahr Distributed Systems Group, Department of Computer Science, Trinity College Dublin, Ireland. 2006

[21] Morton S, Leiba, B and Nathaniel , B . Breaking AntiSpam Systems with Parasitic Spam CEAS 2006. CEAS 2006 Third Conference on Email and AntiSpam,

[22] David Abrams, Ron Baecker, and Mark Chignell. Information archiving with bookmarks: Personal web space construction and organization. In Proceedings of ACM CHI'98 Conference on Human Factors in Computing Systems, pages 41–48, New York, NY, 1998. Association for Computing Machinery.1998

[23] Ann Lantz. Heavy users of electronic mail. International Journal of Human-Computer Interaction, 10(4):361–379,1998.

[24] Longe, O.B, Chiemeke, S.C., Onifade, O.F and Longe, F.A.: Text manipulations and spamicity measures: implications for designing effective filtering systems for fraudulent 419 scam mails. Paper presented at the International Conference on Adaptive Science and Technology, Accra, Ghana-10th - 12th December, 2007. ww:home.vicnet.net

[25] Grabosky, P. N. and Smith, R. G. .Crime in the Digital Age, Crime and Justice: An Australian Textbook in Criminology, (2nd ed.), Lawbook Co., Sydney, pp. 179-99. 2003

[26] Swan, R and Allan, J. Extracting signi_cant time varying features from text. In Proc. 8th Intl. Conf. on Information Knowledge Management, pages 38-45. ACM,1999.

[27] Cournane,A and Hunt, R: An analysis of the tools used for the generation and prevention of spam. Computers & Security 23(2): 154-166 2004

[28] Levine J. Experiences with greylisting; 2005 In James and Hunt - Tightening The Net A review of current and Next Generation Spam Filtering Tools. Computers & Security pp566-578. 2006

[29] Wong M. and Schlitt M.: "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-MAIL, Version 1," Internet Draft. Available online at www.draft-schlitt-spf-classic-02. 2005

[30] Sahami, M., Dumais, S., Heckerman, D. , and Horvits, E.. A Bayesian approach to filtering junk mail. learning for text categorization - Papers Presented at the AAAI Workshop, pp 55-62. 1998

[31] Garcia F, Hoepman J, Van J, and Nieuwenhuizen J.: Spam filter analysis. Proceedings of 19th IFIP international information security conference, WCC2004-SEC, Toulouse, France. Kluwer Academic Publishers. 2004

Babatope O. LONGE teaches computing and Information Technology at the Department of Computer Science, University of Ibadan, Ibadan, Nigeria. He has been actively involved both locally and internationally in the design and implementation of Anti-Spam Techniques. His research interests are in Web Security, Mail Filtering, Cyber Crime Control, Intellectual Property Laws, Policies and Free Open Source Software. He has published and presented papers both locally and internationally. In recent times, he is into

Wireless Network protocol design and implementation. He can be reached at: longeolumide@yahoo.com; Phone: +2348024071175

Stella C. CHIEMEKE (PhD) lectures and currently heads the Department of Computer Science, University of Benin, Benin City, Nigeria. She has authored several papers and served at various capacities in both local and international conferences. Her prominent area of present research are Gender, ICT and Education.She can be reached at: schiemeke@yahoo.com; Phone: +2348023158911

Olufade .F. W. ONIFADE is a lecturer in the Department of Computer Science, University of Ibadan, Oyo State, Nigeria. A recipient of the French Government Grant for the Doctoral co-supervised thesis (University of Ibadan, Nigeria & Nancy 2 University, France). His research interests are in High Speed Networks, ATM Networks, Mobility Management and Protocol Algorithm design for Mobile Ad hoc Networks, Video Streaming and Applications of Fuzzy Logic in system design and cognitive processes. He has published articles in International Journals of repute. Presently, his research is on Risk determination, prediction and management in Economic Intelligent processes towards strategic decision making employing Adaptive Neuro-Fuzzy Inference Systems (ANFIS). He can be reached at fadowilly@yahoo.com; +33673579135/+2348074010558

Longe, Folake ADUNNI is with the African Regional Centre for Information Science, University of Ibadan, Ibadan, Nigeria. A holder of postgraduate qualifications in computing and education, she has both local and international publications to her credit. Her research areas are High Speed Networks, and Information and Communication Technology. she can be contacted at adefolakelonge@yahoo.com or Phone: +2348051797237.