Improved Social Network aided personalized Spam Filtering Approach using RBF Neural Network

Shatabdi M. Bhalerao
M.E Student, Dept.of computer engg.
Saraswati college of Engineering
Mumbai University

Madhuri Dalal
Faculty, Dept. of computer engg
Saraswati College of Engineering
Mumbai University

ABSTRACT
Currently the spam filtering technology is based on the naive Bayesian model. Because of the extremely complex semantic environment as well as naive Bayesian algorithms are easily deceiving; it is not very good at spam filtering. The recent method presented is SOcial network Aided Personalized and effective spam filter (SOAP) using Bayesian spam filtering technique. SOAP showing better results as compared to existing methods, but still it can be further improved in terms of accuracy, efficiency and complexity. In this paper we are presenting extension to SOAP method termed as ISOAP (Improved SOAP) by using RBF (Radial Basis Function) neural network rather than naïve Bayes method for spam filtering. Unlike previous spam filters that focus on parsing keywords or building blacklists, ISOAP exploits the social relationships among email correspondents and their (dis) interests to detect spam adaptively and automatically.

Keywords
Spam filtering, Bayesian spam filters, social networks, RBF spam filter.

1. INTRODUCTION
Now day's electronic mail is becoming popular as many people as well as companies found it a convenient approach to allocate a huge quantity of unsolicited messages to an incredible amount of users at a very low price. These annoying bulk messages or junk emails are called spam messages. The common spam messages that has been stated recently are unwanted advertisements endorsing facilities and products including sexual fixings, low-priced drugs and herbal complements, health insurance, travel document, hotel reservations and software products. They can also include offensive content such pornographic images and can be used as well for spreading rumours and other fake commercials like make money fast.
E-mail spam has sustained to rise at a very fast amount over the last couple of years. It has become a most important risk for corporate users, network administrators and even normal users. Based on projections of current analysis and trends, it was expected that by the end of 2007, spam will endure to increase, reaching a level at around 92% of e-mail traffic. There is a likelihood that by year 2015 spam will go beyond 95% of all e-mail traffic. Although these figures might not be accurate enough, what can be concluded is that spam volume is intensely increasing over years.

Spam can be very costly to e-mail recipients; it reduces their productivity by wasting their time and making aggravation to cope with a large amount of spam. According to Ferris Research, if an employee got five e-mails per day and consumes 30 seconds on each, then he/she will waste 15 hours a year on them. Spam software can also be used to allocate harmful content like viruses, Trojan horses, worms and other malicious codes. It can be a medium for phishing attacks as well. As a result, spam has become a part of rising concern fascinating the attention of many security researchers and practitioners. However, most of the early anti-spam tools were static; for example using a blacklist of well-known spammers, a white list of decent sources, or a fixed set of keywords to detect spam messages. Although these list-based methods can substantially reduce the risk provided that lists are rationalised occasionally, they fail to measure and to adjust to spammers' strategies. They can be defeated easily by changing the sender's address each time, purposely misspelling words, or falsifying the content to avoid spam filters.

Spam emails are producing foremost resource wastage by needlessly inundating the network links. However many anti-spam solutions have been applied, the Bayesian spam score method looks quite favourable. E-mail spam slowly but exponentially grew for several decades to several billion mails a day. Spam has irritated, confused, and annoyed e-mail users. The amount received by most e-mail users has decreased, mostly because of better filtering. About 80% of all spam is sent by fewer than 200 spammers. An ideal spam filter must produce a false positive and a false negative. A more precise filter produces fewer false positives and false negatives. False positives are genuine emails that are incorrectly considered as spam emails. False negatives are spam emails that are not noticed. Unfortunately this is hard to achieve, quite impossible actually.

There are two types of spam filter attacks: poison attacks and impersonation attack. In poison attack, many legitimate words are added to spam emails so that the chance of it being detected as spam is decreased. In impersonation attack, a spammer impersonates the identities of ordinary users by forging their ID's or compromising their computers.

To protect against unsolicited e-mails there are number of techniques presented with goal of efficient, accurate spam filtering. Few previous spam filters can meet the requirements of being user-friendly, attack-resilient, and personalized. Most approaches do not take into account the closeness relationships and (dis)interests of individuals. Previous spam filtering approaches can be mainly divided into two categories: content-based and identity-based. However, both categories methods having limitations and hence suffered from number problems that invalidate such methods under real time settings. Some methods are accurate, but not user friendly. Some methods are user friendly but not personalized, and vulnerable to various other attacks.

The following sections of the paper are organized as follows: Section II will describe related works in the field of spam filtering. Section III will outline the approach taken by the proposed system. The framework will be evaluated in this

section. Finally, Section IV will describe concluding thoughts and ideas in this area.

2. RELATED WORK

The task of email spam filtering is nothing but automatically removing unwanted, damaging, or violent email messages before they are supplied to a user — is a vital, large scale application area for machine-learning methods. In this chapter investigates several categories of the recent related methods on spam filtering.

This study is used to show how the different spam filtering techniques are used to combat spam. We studied these ten papers which have used different techniques for spam filtering, which are described as follows:

In [1] N P. Oscar Boykin et al., uses a content filtering model in which it is used for antispam solutions and to make sending spam solutions unprofitable and thereby destroying the spammers underlying business model. This model is user friendly and resilient to poison attack. But it is Vulnerable to impersonation attack and this model is not personalized because it is installed in an email server to collect all the training samples.

Sufian Hameed et al., [2] proposes a novel spam system "LENS" which is used to select legitimate and authentic users from outside the recipient's social circle and within pre-defined social distances. This method drastically reduces the consumption of internet bandwidth by spam. It is proved to be fast in processing emails and scales efficiently with increasing community size. This method is Vulnerable to impersonation attack and it is also not personalized.

In [3] Michael S. et al., proposes SocialFilter which is a trust-aware collaborative spam mitigation system. This system enables nodes with no email organisation functionality to demand the network on whether a host is a spammer. SocialFilter is a first collaborative unwanted traffic mitigation system that assesses the reliability of spam reporters by reviewing their reports as well as by influencing the social network of reporters administrators. Issue can be generated as Spammer may use dynamic IPs which can lead to Impersonation attack.

In [4] Ze Li et al., proposes the filter which is accurate and user-friendly called "Social network Aided Personalized and Effective Spam filtering". This method combines three modules into the Bayesian spam filter: social closeness-based spam filtering component, social interest based spam filtering component and lastly adaptive trust management component. It is using the common relation between users to find out the junk message automatically. This filter is user-friendly, attack resilient and personalized. But it is Vulnerable to impersonation attack.

In [5] Savita T.et al., focuses on an algorithm for email classification based on naïve Bayesian theorem. The purpose of this is to automatically categorise emails into spam and genuine message. The emails are categorized based on email body. This algorithm found to be effective and reasonable method for email classification. This method is not user friendly because they require much user effort to manually distinguish spam from legitimate emails for training. It is not personalized. This method is Vulnerable to poison attack.

In [6] Harshal D.et al., proposes a spam detection system to detect text as well as image based spam using ANN algorithm. In this system, pre-processing of email text before executing the algorithms is used to make them predict better. Using this system High level, low level and grouping of both the features of image in a spam mail can be projected. . It is not attack-resilient.

Deepak A. et al., [7] focus on a popular machine learning algorithm SVM with different parameters using different kernel-functions. It is evaluated to get best accuracy. Different kernel functions are implemented for spam filtering. Speed and size for training and testing is more. Different kernel functions are implemented for spam filtering. Speed and size for training and testing is more.

In [8] T. Hemalatha et al., proposes an enhanced filtering measure by using a machine learning technique based on content filtering. In this a spam classification method based on machine learning and content feature has been used. In this method Word combinations are not used which can give better results.

In [9] Ajay S. et al., Proposes a KNN classification method with a new distance measure. Due to this new distance Measure the system achieves high accuracy for spam detection. More time is required for execution.

In [10] Reena S. et al., focuses on to make a RBF NN technique and then compared it with SVM based on two parameters i.e. precision and accuracy. This is an efficient spam filtering technique which gives high precision and accuracy. SVM does not perform better as compared to RBF.

To address these limitations recently improved method presented named as SOAP (Social network Aided Personalized and effective spam) [11], which is showing practically efficient results as compared to previous methods. The limitation of SOAP is that it uses basic Bayesian spam filters. This spam filtering technique is complex and suffered from limitations [12-16].The Bayesian filter have following limitations:

1) Bayesian poisoning. If spammers avoid using words that are more prone to being a spam message, the classifier is
   Weakened. (e.g.: hey man are you interested in games? Then email me at imlost@gmail.com. This was a spam message mistakenly classified as a ham message.)
2) Assumes independence of features (Ignores the correlation among inputs or events.) So there is a need of deep Understanding of data characteristics that affect the performance of NB.
3) It requires a training period to learn the difference between spam and non-spam.
4) It suffer from the 'curse of dimensionality'.
   This becomes new research problem in this domain.
   This becomes the motivation for this research work. A Spam filter should be attack-resilient, personalized and user-friendly

3. PROPOSED SYSTEM

As shown in figure 1, the proposed approach of ISOAP, this approach infers node closeness and email preference for individuals using the collected data.

The RBF filter keeps a list of spam keywords and their respective weights specifying the possibility that the email containing the keyword is spam. Created on the three social based modules, after analysing the keywords of a mail, SOAP

adjust the weights of the keywords. Then, ISOAP substitutes to the RBF filter for spam assessment.

The weights are so accustomed based on the familiarity between the receiver and the sender, the receiver's (dis)interests, the receiver's faith on the sender, and the received spammer warning from friends. If the closeness is high, the possibility that they send spam to each other is less, so the weight is reduced, and vice versa. But it is possible that close nodes are compromised. To solve this problem, the other components such as friend notifications and trust management are designed.

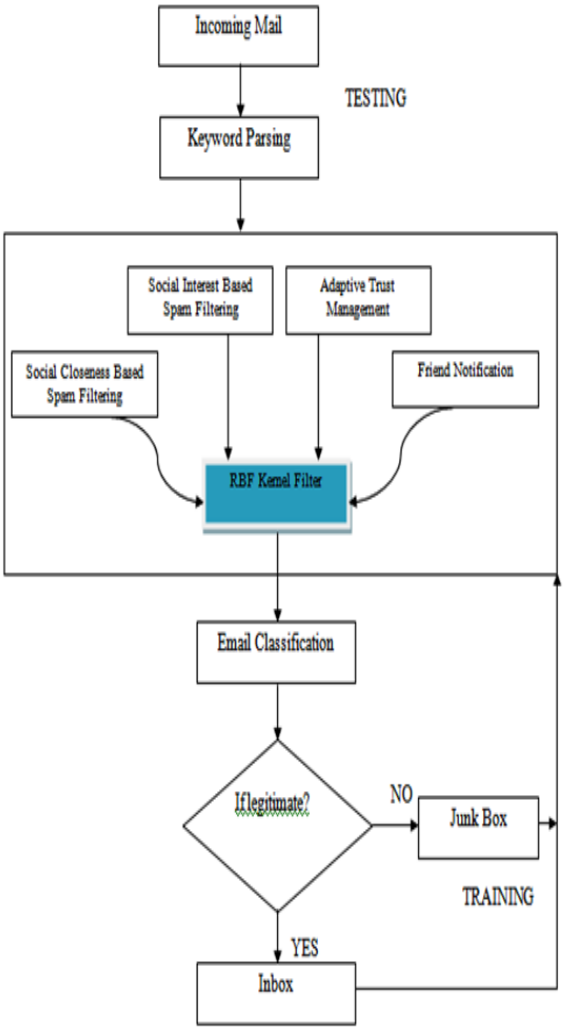

Fig 1: Proposed System

The content-based spam filters focus on email content and can prevent impersonation attacks. Identity based spam filters focus on the communication association between correspondents and henceforth are resilient to poison attacks. ISOAP combines the advantages of both types of spam filters. The accurate results from SOAP become training data to automatically train the RBF filter, thus making the filter user-friendly and personalized, which also reduces the training time. The proposed approach addresses the below issues:

- The closeness of individuals is calculation in a distributed manner and the consideration of closeness integrated into the RBF filter.
- The (dis) interests of individuals are inferred and integrated the email
- Mutual working of ISOAP components for efficient spam detection.

The proposed system leverages social networks to associate four components into the RBF NN filter:

(1) Social closeness-based spam filtering component: This component calculates the social closeness based on social relationships. Since, nodes with more closeness have a less probability of sending spam emails to each other, emails from nodes with lesser closeness are checked more firmly and vice versa. This component makes SOAP resilient to poison bouts.

(2) Social interest-based spam filtering component: This component infers nodes (dis)interests based on social profiles. The indirect information helps the filter to increase the correctness of spam detection by considering specific preferences. This component donates to the personalized feature of SOAP.

(3) Adaptive trust management component: In order to tackle impersonation attacks, SOAP relies on additive-increase/multiplicative-decrease (AIMD) algorithm to adjust the trust values of nodes.

(4) Friend notification component: In order to strengthen SOAP's capability to combat impersonation attacks, a node quickly notifies its friends and FoF (Friends of Friends) about a detected suspicious compromised node. ISOAP is a user oriented spam filter.

(5) Each user will run it independently to detect spam.

Fig 1 shows how the different components in ISOAP cooperate with each other for spam examination of an incoming mail. Using social closeness-based spam filtering a node calculates the closeness between other nodes and itself. Also it keeps a list of the closeness values. Firstly, when a node receives an email, ISOAP parses out the keywords in an email.

For each keyword, the RBF filter keeps the weight that an email containing the keyword is spam. In second stage, the different components adjust weight in order to increase the accuracy of spam detection. First, if the sender is not in the blacklist, established on the intimacy between the email sender and receiver, the weights for each keyword are adjusted. Then, the social interest based spam filtering is used. If keywords match the interests of the receiver, it means the email is useful to the receiver, so the weights of the words are decreased or vice versa. Finally, according to the weights of the keywords, RBF filter determines whether the email is spam. In third stage, the email is forwarded to the Inbox or the junk box. In last stage, these results are used for spam detection training. The goal of trust management and friend notification is to counter impersonation attacks i.e., decreasing false negatives while controlling false positives.

3.1 Working of Rbf Filter

RBF network have three layers: Input layer, Hidden layer and Output layer. Each node in the input layer has a connection to the each node in hidden layer. Each node in the hidden layer, they actually perform (computes) radial basis function. The output layer has a weighted amount of outputs from the hidden layer to form the output. The Euclidean distance is

computed from the point being evaluated to the centre of each neuron and RBF is applied to the distance to compute the weight for each neuron. The radius distance is the argument to the function. So, it is called as Radial Basis Function.so, weight= RBF (distance)

4. CONCLUSION

The work presented in this paper proposes a framework for ISOAP to efficiently filtering the spam emails using RBF Neural Network. This proposed approach is based on recently presented SOAP method. The limitation of SOAP is that it uses basic Bayesian spam filters. This spam filtering technique is complex and suffered from limitations. Therefore, rather than using Bayesian spam filtering approach, RBF Neural Network based spam filtering technique is proposed to filter spam more accurately and correctly. In future scope more focus towards less time and more accuracy.

5. REFERENCES

[1] Haiying Shen and Ze Li, "Leveraging Social Networks for Effective Spam Filtering", IEEE

[2] GFI Software, "Why Bayesian Filtering is the Most Effective Antispam Technology", http://www.gfi.com/whitepapers/Whybayesian-filtering.pdf,2011

[3] M. Uemura and T. Tabata, "Design and Evaluation of a Bayesian-Filter-Based Image Spam Filtering Method", Proc.(ISA),pp. 46-51,2008.

[4] X. Carreras, J. Salgado, "Boosting Trees for Anti-Spam Email Filtering", Proc. (RANLP),2001.

[5] P. H, T. Scheffer, "Supervised Clustering of Streaming Data for Email Batch Detection", 2007.

[6] [J.A.K. Suykens and J. Vandewalle, "Least Squares Support Vector Machine Classifiers", 1999.

[7] S.J. Delany ,P. Cunningham, "An Assessment of Case-Based Reasoning for Spam Filtering",2005.

[8] W. Zhao and Z.Zhang , "Email Classification Model Based on Rough Set Theory",2005.

[9] J.S.Kong, P.O. Boykin, "Let Your Cyber Alter Ego Share Information and Manage Spam", 2005.

[10] F. Zhou, Z Huang, "Approximate Object Location and Spam filtering on Peer-to-Peer Systems", 2003.

[11] SPAMNET, http://www.cloudmark.com

[12] P.O. Boykin, V. Roychowdhary, "Personal Email Networks: An Effective Anti-Spam Tool", 2004.

[13] S. Garris, H. Yu, "Re: Reliable Email", NSDL, 2006.

[14] S. Hameed, N. Sastry, "LENS: Leveraging Social Networking and Trust to Prevent Spam".

[15] I. Rish, "An Empirical study of naïve Bayes classifier".

[16] K. Jha, "Comparison of Naïve Bayes Classifier, Decision Tree and ANN for the purpose of spam detection".

[17] Pragya B, S. Bagwari, "Comparison of Feed Forward Network and Radial Basis Function for Detecting and Recognition of license Plate", IJCA, May 2015.