ISSN:0975-9646

SMS Spam Filtering Application Using Android

Gaurav Sethi[1] , Vijender Bhootna[2]

[1]*Studenent Dept Of MCA,*
[2]*Student Department of Applied Electronics and Instrumentation*
[1]*R V College Of Engineering*
[2]*JRE Group of Institutions*

Abstract— **In the recent years, we have witnessed a dramatic increment in the volume of spam email. Other related forms of spam are increasingly revealing as a problem of importance, specially the spam on Instant Messaging services (the so called SPIM), and Short Message Service (SMS) or mobile spam.**

Like email spam, the SMS spam problem can be approached with legal, economic or technical measures. Among the wide range of technical measures, Bayesian filters are playing a key role in stopping email spam. In this paper, we analyze to what extent Bayesian filtering techniques used to block email spam, can be applied to the problem of detecting and stopping mobile spam. In particular, we have built two SMS spam test collections of significant size, with some specific words. We have tested on them a number of messages representation techniques and Machine Learning algorithms, in terms of effectiveness. Our results demonstrate that Bayesian filtering techniques can be effectively transferred from email to SMS spam.

Keywords— Bayesian Algorithm, SPIM, Spam Filtering

I. INTRODUCTION

Millions of people send messages every day, but main problem of users is spam's. Spam's are undesired messages, which we don't want to be in our message box, so filtering of spam is becoming very necessary. Spam Filtering is the text classification technique which proved to be a great technique for dealing with spam's. The familiar method is Bayesian filter, Support Vector Machine (SVM) . Bayesian approach is the statistical-based spam filter method [2] which is strong algorithm for classification. Dynamic training and classification has shown impressive performance of filtering spam. So here we are trying to combine the advantages of this method with Bayesian approach into a single model. In this paper, we attempts to combine the mechanism of Naïve Baye's [3] and dynamic nature into a single algorithm [5].Our experiment results proved that this algorithm is effective to filter spam.

II. FROM EMAIL TO SMS FILTERING

The similarity of SMS spam filtering to email spam filtering suggests that proven technologies in email spam filtering may be useful in combating SMS spam. The content-based technologies used in email spam filtering that can also used for SMS spam filtering include both direct content filtering and collaborative content filtering techniques. The direct content filtering technologies search or use the direct textual content of the message and store them in a database that is updated dynamically. This set is known as the training set and the model learns from this training set how to distinguish spam from non spam and is used to predict whether new messages are spam or not. Automatic text classification requires a representation of each message typically an n-dimensional vector where each dimension represents a characteristic or feature that is predictive of the text classification problem. The messages are identified by parsing and tokenisation of their content. Collaborative content filtering techniques allow a group of users to share information on spam messages. A successful approach is to generate a signature sometimes known as a fingerprint. A signature is generated for all incoming messages and checked against the known spam signatures, and the unknown one's. The mobile technology is also a factor, all products don't have any specific location for spam messages, the messages simply combines with the others one. Here on this paper we also focusing on how to use this Bayesian algorithm in a way that we separate those spam messages automatically.

III. CONTENT BASED SMS SPAM FILTERING

Wu et al. (2008) used a Bayes learner to extract keywords from messages for monitoring the rate of spamming, and assigned each spammer a score based on his spamming Longzhen et al. (2009) proposed using a k-nearest neighbour algorithm (k-NN) as part of a multi-filtering approach. After black and white listing, a message is first classified by a filter , which provide approximate descriptions about the message. If this filter classifies the message as spam, it is then passed to the k-NN classifier for final classification. An evaluation on a data set of 100 spam SMS and 50non-spam SMS with k = 12 showed that this dual filtering method is faster and more accurate than using k-NN alone. Some others algorithm already proved by dividing the whole message into many small parts and with the help of an index on it they provide the filtering mechanism.

IV. BAYESIAN ALGORITHM

Bayesian approach is the statistical-based spam filter method [2] which is strong algorithm for classification. Dynamic training and classification has shown impressive performance of filtering spam. So here we are trying to combine the advantages of this method with Bayesian approach into a single model. In this paper, we attempts to combine the mechanism of Naïve Baye's [3] and dynamic nature into a single algorithm [5].Our experiment results proved that this algorithm is effective to filter spam.

Classification is a two step task.

Training stages

- Collection of known Messages

- Pre-processing of Messages
- Creating Hash map of words
- Calculating probabilities
- Sorting words in relevant order of probabilities

Classification stages

- Prepare a set of sms's for testing
- Pre-processing of Messages.
- Generate interesting word list
- Finding overall spam probability
- Classifying an email

Background :

Bayesian classification technique is based on baye's theorem [1]. This technique is useful to find probabilities related to every word and on the basis of those probabilities we can find spam probability on messages.

Bayes theorem:

Let X is a data tuple. X is considered "evidence." normally; it is described by a set of n attributes. Let H be some hypothesis, for example that the data tuple X belongs to a specified class C. For classification [9] of such data, we want to determine *P (H|X)* that is probability that the hypothesis H holds given the "evidence" or observed data tuple *X*. In other words, we are looking for the probability that tuple *X* belongs to class *C*, given that we know the attribute description of *X*. *P(H|X)* is the posterior probability, of *H* conditioned on *X*. conditional probability [5] is given as-

$P(C|X)= P(C)*P(X|C)/(P(X)$

Here *P(C)* is the probability of class and *P(X)* is probability of evidence.

V. PROPOSED METHODS

Training stages:

Collection of known Messages –for training of spam filter, collection of messages is needed whose classification labels are known. This collection should be from several and different kind of sources.

Pre-processing of Messages- in next step of training filter is necessary also sender information should be used for training purpose.So a record of senders is also maintained who send mostly spam's or who sends mostly genuine message.

Creating Hash map of words-after pre-processing task, a hash map of words is created and count of each word occurring in message is also maintained with words. Suppose if a word exists in hash map then count related to word is increased on occurrence of word, but if word is not in hash map, then put the word in hash map with single count.

Calculating probabilities of word occurring in spam and genuine message is calculated. Then spam probabilities of words are calculated. Spam probability of a word, Sp = f1/ (f1+f2) **,** Here f1 is frequency in spam's and f2 is frequency in genuine messages.

Classification stages :

Prepare a set of messages for testing a collection of emails is needed for testing our spam filter.Pre-processing those messages to remove unwanted words.Generate interesting word list which contains n words that exist in hash-map with very high spam probability or very low spam probability.

$P(A_1, A_2, \ldots, A_n|C) = P(A_1| C)* P(A_2| C)* \ldots * P(A_n| C)$

Here $A_1, A_2, \ldots, A_n$ are meant for words and C is meant for class Spam.

Classifying an email- if overall spam probability is more than 0.5 than an email can be classified as spam.

VI. RESULTS

100 known messages were used for training of spam filter in our algorithm, out of which 50 were spam and others were genuine messages. 100 more were used for classification or testing purpose. Test set also consist of 50 spams and others as genuine emails. There are two measures, which give the accuracy of a spam filter. One of them is sensitivity and other is specificity. Sensitivity of a spam filter is the probability of positive test given that message is spam. Sensitivity of spam filter, $S= p_t / (p_t + n_f)$ Here, p_t is no. of true positives and n_f is no. of false negatives. Calculated sensitivity = 36/50 = 0.974 Specificity of a spam filter is the probability of negative test given that the message is genuine. Specificity of spam filter, $s= n_t / (n_t + p_f)$ Here, n_t is no. of true negatives and pf is no. of false positives.

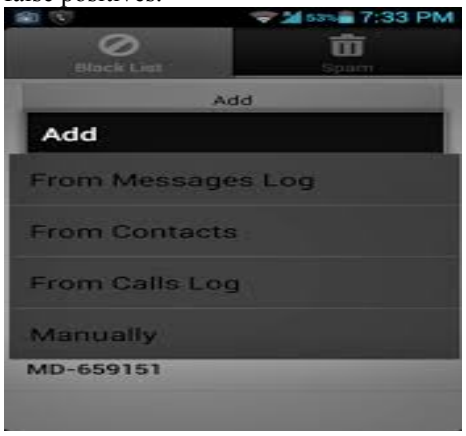

Fig1: Adding members to black-list

.The above figure explains the view to add members to the black-list from several sources like from message log, from contacts and also from calls log.Members are automatically added.

Fig2: Black-list password protection

The above figure (Fig2) explains the way to protect the black-list from unauthorized access by applying password protection.

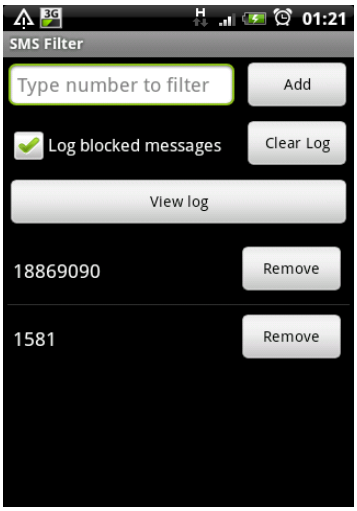

Fig3: Black-list Members Edit Page

The above figure explains the way to filter the black-list members like adding a new member, remove a member or clear the total log. Internally it produce a query and fetch the required data from memory then perform the work.

VI. CONCLUSION

Spam filtering has become a challenging task because there are lot of difficulties with it. Most of spam detection techniques are unable to find these spam's because regular training of these classifiers is not done yet, database of spam should be updated all the time dynamically that we discussed on this paper. Existing spam filters are static in nature, because of that these spam filter show false positive or false negative results. Dynamic training can improve spam filtering extremely. In this paper, Bayesian approach with dynamic training and classification is discussed.

REFERENCES

[1]. J. Han and M Kamber. "Data Mining: Concepts and Techniques", Morgan Kauf - man Publishers, 2000.

[2]. Meena, M.J.; Chandran, K.R.; "Naïve Bayes text classification with positive features selected by statistical method," Advanced Computing, 2009. ICAC 2009. First International Conference on, vol., no., pp.28-33, 13-15 Dec. 2009

[3]. Haiyi Zhang; Di Li; "Naïve Bayes Text Classifier," Granular Computing, 2007. GRC 2007. IEEE International Conference on , vol., no., pp.708, 2-4 Nov. 2007

[4]. Researchment and Realization Based on Android Database Application Technology. Ming Xu, XinChun Yin, Jing Rong ,College of Information Engineering Yangzhou University ,YangZhou, China Proceedings of the 2nd International Symposium on Computer, Communication, Control and Automation (ISCCCA-13)

[5]. Pang-Ning Tan, Michael Steinbach, and Vipin Kumar Introduction to Data Mining Addison-Wesley (2005).