Identifying threat from SMS Messages Using Text Classification technique

Dr.S.Sagar Imambi [#1], Sk.Rafi [#2],Sd.Rizwana [*3]

#1Prof., Dept of Computer Science
Narasaropeta Engineering College, Narasaaopeta,AndhraPradesh
simambi@gmail.com
*[*2]Asst.Prof Dept of Computer Science*
Tirumala Engineering College, Narasaaopeta,AndhraPradesh
*[*3]Asst.Prof Dept of Computer Science*
Narasaropeta Engineering College, Narasaaopeta,AndhraPradesh

***Abstract*— The impact of SMS messages in our daily life is now more obvious than ever. Each minute, millions of plain text or enriched messages are being sent and received around the world. To recongnise spam message among them, is one of the important challenges in internet applications. Earlier Statistical methods are used to characterize user behavior, classifying spam and detecting novel email viruses. Later on data mining has emerged to address these problems. Data mining is used to classify structured data. However, previous techniques have not examined problems with the classification of unstructured text and they need some improvements. In this paper, we present prototype based classification algorithm which incorporates the Global relevant weighing schema. We experimentally proved that, with our proposed classification algorithm it is possible to detect threat messages with high accuracy.**

***Keywords*— Classification, SMS messages, threats, Text mining,.**

I. Introduction

With the recent explosive growth of e-commerce and wireless communication, a new genre of text, short text, has been extensively applied in many areas.The impact of SMS messages in our daily life is now more obvious than ever. Each minute, millions of plain text or enriched messages are being sent and received around the world. Since mobile devices are becoming the standard method of communication, mobile shopping and mobile banking are tremendously increased. Short Message Service is one of the popular and cheap services and most used service in mobile network. It has high response rate and having good confidentiality with trusted and personal service. Due to that unwanted SMS known as spam SMS will arise which will generate different problem to mobile user.

As mobile devices contain sensitive and personal information they are prone to criminal attacks. SMS provides a perfect environment for spreading spam quickly. While most cyber scams target computers, smashing scams target mobile phone, and they're becoming a growing threat with the growing number of mobile phones. Financial services are the most targeted sector of the spam messages.

Victim receives an SMS message with a hyperlink wherein a malware automatically finds its way to the cellular phone, or leads the victim to a phishing site formatted for cellular phones. It may also connect to automated voice response system. To recognise such spam message is one of the important challenges in internet and wireless networks. Some messages aims at getting personal information through this malware. Those messages may look like this

"Alert - this is an automated message from , your ATM card has been suspended. To reactivate call urgent at 8669876541"

The design and implementation of effective threat detection techniques to combat cybercrime and to ensure cyber security, therefore, is an important and timely issue. Earlier Statistical methods are used to characterize user behaviour, classifying spam and detecting novel email viruses. Later on data mining has emerged to address these problems. Data mining is used to classify structured data. However, previous techniques have not examined problems with the classification of unstructured text and they need some improvements. In this paper, we present prototype based classification algorithm which incorporates the Global relevant weighing schema. We build the classifier to analyze sms messages. We collected 5574 sms message from standard SMS collection v1.0.

II. Survey of Literature

A The machine learning approach to text classification has been studied and analysed for many years but there has been little previous work in the text classification domain. The techniques used for text classification work well for datasets with large documents such as scientific papers but suffer when the documents in the training corpus are short.[2]. Sarah Zelikovitz et al describe a method for improving the classification of short text strings using a combination of labeled training data plus a secondary corpus of unlabeled but related longer documents. [3].

Most existing spam-filtering techniques for mobile phones are based on the content of SMS [4, 5]. Most of these techniques are straightforward adaptations of email spam detection schemes and usually incorporate features specific words, character bi-grams and tri-grams – for classification of spam messages [6]. In 2002 a study was conducted to discover

© 2015 JCT. All Rights Reserved

spam messages by extraction unigram features but it will not filters word pairs, or even triples [7].

Fette et al. [8] proposed the method to detecting malicious phishing emails by incorporating features specifically designed to highlight the deceptive methods used to fool users. With their method they were able to accurately classify 92% of phishing emails, while maintaining a false positive rate on the order of 0.1%.

SpamAssassin uses a wide variety of local and network tests to identify spam signatures. This makes it harder for spammers to identify one aspect which they can craft their messages to work around. [9]

In a recent study conducted by Deepasikha Patel et al [10] shows that entropy term weighting scheme and then PCA are used for reparameterization and Artificial Neural Networks to classify Mobile SMS into predefined classes such as jokes, shayri and festivals etc.

Ion Androutsopoulos et al (2000) conducted a thorough evaluation on publicly available corpus and investigate the effect of attribute-set size, training-corpus size, lemmatization, and stop-lists on the filter's performance issues. They stated that additional safety needs are needed for Naive Bayesian anti-spam filter.[11]. Jaackko Hollmen stated that user profiling is possible by the Bayes classification in mobile network communication. But his study limited to identify fraudulent or illegal use of services.[12].

A hybrid system of SMS classification to detect spam or ham, using Naïve Bayes classifier and Apriori algorithm is proposed by Ahmed, et.el. Though this technique is fully logic based, its performance will rely on statistical character of the database. Naïve Bayes is considered as one of the most effectual and significant learning algorithms for machine learning and data mining and also has been treated as a core technique in information retrieval. However, by applying user-specified minimum support and minimum confidence, significant improvement is observed over the traditional Naïve Bayes classification.[15].

III. CLASSIFICATION OF SMS MESSAGES

Text mining process involves (a) Retrieving some texts relevant to the domain of interest; (b) representing the content of the text in some format useful for processing and (c) analyzing the data and represent the extracted information. The process of text-mining needs a well-organized integration of the phases of knowledge discovery. Every phase of the text-mining process can be addressed with several different methods and technologies. The text mining phases are shown in the fig1. In our work, we applied the classification algorithm to identify the spam messages.

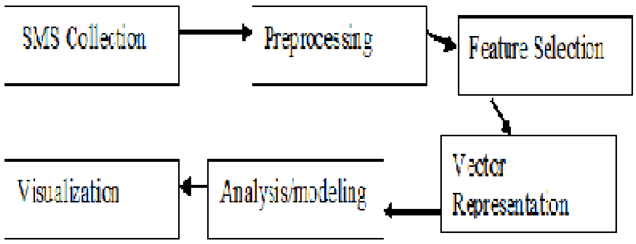

Fig. 1 Text mining process

A The Algorithm for predicting spam messages:

We developed an algorithm for identifying cyber threats from sms messages. Following are the steps in the algorithm.

Step 1: Prepare a set of training data. Attach topic information (class label) to the document in a target domain. Collection of Messages D= {d1,d2,d3……dn) Collection of Classes C={c1,c2} i.e Ham or Spam

Step2: Represent the data in vector form.

Step3: Assign global relevant weight for features representing the messages

Step4: Build the classifier using prototypes generated for each class.

Step 5: Apply classifier on the testing message a data

The Classifier Function is function ΦC : D-> C that maps the message to classes.

IV. EXPERIMENTAL RESULT

In our experiment we used 8865 messages, collected from the Spam Collection V1.0. Among 6780 are legimate messages and 2085 are spam messages. We partitioned the dataset into a training set of 5850 and a test set of 3000 messages. Our experimental results shows 90.2% accuracy and 89% precision and 92% recall. This analysis differs from previous results that are used Bayesian approach through enhancement of feature weighting schema and building an enhanced classifier. The results are tabulated in table 1 and Fig 2 shows the graphical representation of the result.

Classification technique	**Accuracy**	**Precision**	**Recall**
Bayes	86%	82.45%	81.5%
Proposed classification Technique	90.5%	89%	91%

Table 1 Comparison with Bayes.

© 2015 JCT. All Rights Reserved

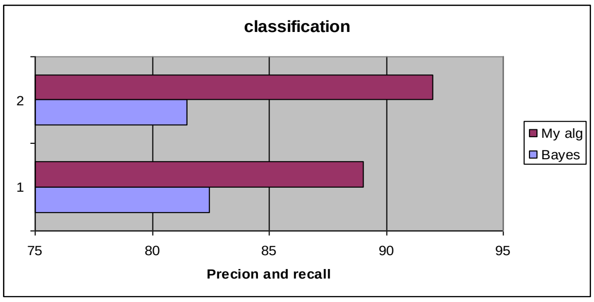

Fig 2 Evaluation metrics

V. Conclusions

Spam is sent from fraudulent addresses, causing inaccurate billing for subscribers and revenue loss for the mobile operators. To prevent subscriber churn and protect revenues, mobile operators need a flexible solution for identifying fraud. We developed to learning algorithm for classification of SMS spam, which is based on the novel feature weighting schema. We evaluated our work on standard Spam collection V1.0 datasets collected from http://www.dt.fee.unicamp.br/~tiago/smsspamcollection. In this paper, we have shown that it is possible to detect threat messages with high accuracy by using the proposed classification algorithm. The results of experiments demonstrate that our algorithm provides a more than 90% detection rate.

References

[1].www.macmillandictionary.com/buzzword/entries/smishing.html

[2]. Sebastiani, F.: Machine learning in automated text categorization. In: CM Computing Surveys. (2002) pp:1–47.

[3] Zelikovitz, S., Hirsh, H.: Improving short-text classification using unlabeled background knowledge to assess document similarity. In: Proceedings of the Seventeenth International Conference on Machine Learning (ICML). (2000).

[4] Cormack, G.; Hidalgo, J.; Sánz, E. Feature engineering for mobile (SMS) spam filtering. Proceedings of the 30th annual international ACM SIGIR conference on Research and Development in Information Retrieval, ACM (2007) 872.

[5] Cormack, G.; Hidalgo, G.; María, J.; Sánz, E. Spam fi ltering for short messages. Proceedings of the sixteenth ACM conference on Conference on information and knowledge management, ACM (2007) pp:313–320.

[6] Hidalgo, G.; María, J.; Bringas, G.; Sánz, E.; García, F. Content based SMS spam filtering." Proceedings of the 2006 ACM symposium on Document engineering, ACM (2006) 114–122.

[7] Paul Graham. A plan for spam, 2002. www.paulgraham.com/spam.html

[8] I. Fette, N. Sadeh and A. Tomasic, "Learning to Detect Phishing Emails", Technical Report CMU-ISRI-06-112, Institute for Software Research International, Carnegie Mellon University, June 2006.

[9]"The Apach SpamAssassin Project" 2010 [Online]. Available: http://spamassassin.apache.org/

[10] Deepshikha Patel, Monika Bhatnagar, Mobile SMS Classification,An Application of Text Classification, International Journal of Soft Computing and Engineering (IJSCE), Volume-I, Issue-I, March 2011.

[11Ion Androutsopoulos, Georgios Paliouras,et al - Learning to Filter Spam E-Mail: A Comparison of a Naive Bayesian and a Memory-Based Approach- Proceedings of the workshop "Machine Learning and Textual Information Access", 4th European Conference on Principles and Practice of Knowledge Discovery in Databases (PKDD-2000, September 2000, pp. 1-13

[12] Jaackko Hollman user profiling and classification fraud detection in mobile communication networks , Dissertation for the degree of Doctor of Science in Technology , December 2000.

[13] http://blog.proofpoint.com/smstext/

[14] YAN Rui, CAO Xian-bin, LI Kai, "Dynamic Assembly Classification Algorithm for Short Text," ACTA ELECTRONICA SINICA, Vol. 37(5), pp. 1019-1024, 2009.

[15]. Ahmed, Ishtiaq, Donghai Guan, and Tae Choong Chung. "Sms classification based on naive bayes classifier and atpriori algorithm frequent itemset."International Journal of machine Learning and computing (2014).

© 2015 JCT. All Rights Reserved