*Communications on Applied Electronics (CAE) – ISSN : 2394-4714*
*Foundation of Computer Science FCS, New York, USA*
*Volume 3– No.3, October 2015 – www.caeaccess.org*

# Enhancing the Rate of Accuracy and Precision in Spam Filtering in Farsi SMS

Maryam Poorshahsavari
Department of Computer Science
Kerman Branch, Islamic Azad University
Kerman, Iran

Omid Pourgalehdari
Department of Computer Science
Kerman Branch, Islamic Azad University
Kerman, Iran

## ABSTRACT

This paper introduces a technique for increasing the rate of accuracy in spam filtering and reducing the false positive (fp) in Farsi SMS. This technique is based on combination of naïve bayes assumption with an introduced formula to increase the filtering accuracy up to 90%. In order to validate introduced formula and to measure the accuracy, the obtained results have been surveyed by precision-Recall techniques.

## Keywords

SMS Filtering, Naïve bayes Assumption, Spam SMS, Data Mining, False Positive

## 1. INTRODUCTION

Short Message Service (SMS) is telephone text service communication component mobile or web communication system, which is following a standard protocol named SMPP that allows exchange short text messages between telephone systems [1]. SMS is a dependable service for exchange of confidential information, which has a suitable cost and high rate of response [2]. However, this advantage of short message service (e.g., low cost and wide band width of SMS network) makes it as a great target for commercial abuse [4]. Totally, incoming SMS can be categorized into two types of authorized and spam form. An unwanted SMS is conveyed to a great number of short message recipients [1]. Deleting unwanted SMS can be tedious and time-consuming [3] [4].

Since 1992 the using of short-message-service in Iran has become common and familiar. In a way that in twenty years ago, Iranian users daily exchanged twenty million SMS. While nowadays, not only this figure has been increased highly [5]. But also advertisement and unwanted SMS also has become an important anxiety of Iranian mobile users.

Increasing of spams has been resulted to development of a set techniques to fight against them [1]. Filtering of spam SMS is a developed idea that can be defined in automatic classification of SMS as spam or authorized. The spam SMS challenge is the small number of words and sometimes artificial abbreviated words [6]. One of the spam filtering techniques is text–based technique that includes collaborative content filtering and direct content filtering models. The latter technic allows a group of users to share information on SMS [2]. One of its successful ideas is production a signature for created SMS which signature of each new short message is checked according to known spam signatures. In this paper we have used the direct content filtering technic for Persian spam SMS filtering. In order to measure accuracy, we stored a set of known spam and authorized SMS into a database as a set of training set. Training set used to identity being a new spam or authorized SMS. This technique uses the naïve bayes training algorithm to obtain word event probability from two proposed formulas at [7] and our proposed formula. The results of test showed that out proposed formula for Persian spam SMS filtering has had better results.

## 2. RELATED WORKS

Two technics are accessible for filtering spams SMS. The technics are whitelist, blacklist and text classifier [3]. Filtering technic of whitelist and blacklist is based on sender number. Blacklist based on sender number has a list of sender numbers that the user does not want from them a short-message. Whitelist includes sender numbers that the user accepts their short-message. Black and white list technic are based on text involves a list of words that SMS containing those word is known as spam.

In this paper assessment of ten spams filtering application by measuring the precision and accuracy is given (see Table 1). In general, all of these applications filter incoming SMS from unknown senders as spam and allow entering of SMS known senders SMS (such as senders in the contact list) in the message inbox.

**Table 1. Obtained results from comparison of ten spam filtering applications taken from [8]**

| Application | Precision | Accuracy |
|---|---|---|
| SmsBlocker | 0.00 | 0.50 |
| SpamBlocker | 0.33 | 0.38 |
| AVG Antivirus | 0.00 | 0.50 |
| Postman | 0.00 | 0.50 |
| SmsBlocker | 0.00 | 0.50 |
| SMS Spam Blocker | 0.00 | 0.50 |
| Quickheal | 1.00 | 1.00 |
| Quickheal | 0.00 | 0.00 |
| AntiSpam SMS | 0.64 | 0.56 |

Although two applications (e.g., SMS blocker, and numbercop) filter a few number of identified sender numbers as spam. According to implement analysis was specified that all applications have the possibly of blacklisting of the numbers. Almost 85 percent of applications block SMS of unidentified sender and less than 25 percent of applications utilize string conformity. None of these applications use machine learning technic for spam classification and a number of applications filter SMS spams from identified senders in correct form.

## 2.1 Bayesian Classifier

Bayesian classifier technic is based on Bayes theory and used for calculation of secondary probabilities. Bayes theory is based on information that has been collected in the past. Using this technic can be obtained probability of event any word in every spam and authorized class and according to those probabilities can be determined probability of spam or authorization. Bayesian Classifier is represented as follows [9]:

Suppose that a set of m samples S= {$s_1$, s2… $s_m$} exists as a set of prepared training data that each $s_i$ sample is presented by a vector from n dimension {$x_1$, $x_2$… $x_n$}. Some quantities of $x_i$ are related to {$A_1$, $A_2$… $A_n$ }attributes. Moreover there are classes {$c_1$, $c_2$… $c_k$} and each sample belongs to one of these classes. In order to forecast class a new x sample is used the conditional probability of P($C_i$|X) which i=1,…,k. probabilities from Bayesian theory are obtained as follows:

$$P(C_i \mid X) = \frac{P(X \mid C_i) \cdot P(C_i)}{P(X)}$$

P(X) is constant for all classes. P($C_i$) is a number of trained samples in form $C_i$/m class (m is number of total trained samples).

## 3. PROPOSED METHODOLOGY

In order to use Bayesian classifier two stages of works have been preformed which each stage has some steps as follows:

## 3.1 Training Stage

In order to set up the training stage, there is a need for a set of spam and authorized SMS. Therefore, this technique also used from a set of “message center” and “read messages” databases for authorized SMS set and from unwanted messages entry in users inbox for spam SMS set. In order to do so, 100 SMS for each set has been picked. Preprocessing of SMS was done by deleting symbols, pictures, hyperlinks and redundant words. Further, a words event table for authorized and spam SMS has been created. First of all, the authorized SMS were placed in the event table without iteration then number of word events was done using two different formulas:

The expressed formula in the work at [7] that probability of spam words is as follows:

$SP_1=F_1/(F_1+F_2)$

$F_1$ is repetition of a word in the spam event table and $F_2$ is repetition of a word in authorized event table. This formula only considers shared words of tables. While, in proposed formula the spam probability words is as follows:

$SP_2=(Ns/Nx_i)$

Ns is number used spam SMS in spam event table and $Nx_i$ is repetition of word in spam event table.

## 3.2 Classifying Stage

In order to test the classifier some set of SMS has been prepared. Carried out preprocessing on these SMS set until was created the list of SMS words after preprocessing. Overall probability of test SMS being spam or authorized was carried out using bayesian classifier as follows;

$P(x|c_i)=p(A_1,…,A_n|c_i)=p(A_1|c_i)*…*p(A_n|c_i)$

According to this definition, the probability of SMS being a classifier is high.

## 4. RESULTS AND TEST

In order to validate defined method, 50 SMS for test of authorized messages and 50 SMS for spam sets has been picked. Implementation of classifier was carried out using five parameters as follows:

Spam Precision =SP=Nss /( Nss+Nls)

Spam Recall =SR=Nss /( Nss+Nls)

Accuracy =(Nll+Nss) / (Nl+Ns) F-measure =2 * SP*SR / (SP+SR)

FP =Nls / (Nll+Nls)

The used symbols are defined in this fashion:

Nss : Number of spam SMS that have been recognized as spam

Nls : Number of authorized SMS that have been recognized as spam

Nll : Number of authorized SMS that have been recognized as authorized

Nsl : Number of spam SMS that have been recognized as authorized

Ns :Number of spam SMS used in training stage

Nl :Number of authorized SMS used in training stage

## 4.1 Comparison Of Classifiers

In order to tabulate the classifier results, Table 2 shows classifier symbols on the basis of two word event probability formulas and Table 3 shows classifier formulas on the basis of two word event probability formulas.

**Table 2: Classifier symbols on the basis of two word event probability formulas.**

| Word Event Probability Formulas | TP | FN | TN | FP |
|---|---|---|---|---|
| $P=F_1/F_1+F_2,F_2/F_1+F_2$ | 44 | 6 | 43 | 7 |
| P=Ns/Nxi , Nm/Nxi | 43 | 7 | 46 | 4 |

**Table 3: Classifier formulas on the basis of two word event.**

| Classifier by | SP | SR | Acc | F-measure | FP |
|---|---|---|---|---|---|
| $P=F_1/F_1+F_2,F_2/F_1+F_2$ | 0.86 | 0.88 | 0.87 | 0.87 | 0.14 |
| P=Ns/Nxi , Nm/Nxi | ~ 0.915 | 0.86 | 0.89 | 0.89 | 0.08 |

It is so evident from table 3 that using proposed word event probability formula has improved in all parameters except for spam Recall (see Table 3). Amount of fp parameter is considerable (see Table 3).

## 4.2 Comparison Of Classifier And Studied Programs In Google Play Storage

The downloaded programs from Google play storage, which has been explained in part 2 are the best spam SMS filtering options in Iran. In order to validate the introduced filtering system, the results of these applications as well as the results of the proposed classifier have been compared. According to this table only the Quickheal program if the blacklist is on has 100 percent accuracy and in default state that blacklist is off it has zero accuracy. Accuracy of other programs is less than proposed filtering system (see Table 4).

**Table 4: Results obtained from Google play storage classifiers and proposed filtering system**

| Application | Precision | Accuracy |
|---|---|---|
| SmsBlocker | 0.00 | 0.50 |
| SpamBlocker | 0.33 | 0.38 |
| AVG Antivirus | 0.00 | 0.50 |
| Postman | 0.00 | 0.50 |
| SmsBlocker | 0.00 | 0.50 |
| SMS Spam Blocker | 0.00 | 0.50 |
| Quickheal | 1.00 | 1.00 |
| Quickheal | 0.00 | 0.00 |
| AntiSpam SMS | 0.64 | 0.56 |
| Proposed filtering system | ~ 0.915 | 0.89 |

As discussed in section 2 the accuracy and precision of some existing spam filtering applications has been surveyed (see Table 1). Further, in this section obtained results in terms of accuracy and precision from existing applications has been compared with obtained results from proposed filtering system. In proposed filtering system the accuracy has been increased up to 89%. While the precision in proposed system has been increased up to 91%. Comparing proposed system results with existing applications shows that proposed system has better results except to compare with Quickheal with 100% efficiency. However, Quickheal filters all SMS's (e.g., authorized and unauthorized) coming from unknown sources. While in proposed system may the accuracy and precision being less than Quickheal. But on the other hand proposed system is able to distinguish between (e.g., authorized and unauthorized) SMS's, which are coming from unknown source.

## 5. DISCUSSION

In existence of a great unwanted and advertisement SMS that make troubles for users, still there is no suitable filtering system. In this paper, by use of Naïve bayes assumption classification method provided means to classify and filter unwanted and advertisement SMS. In this paper in order to obtain the probability of word in the classifier used two formulas that formula one was based on study carried out by Sethi et, al.[7] and second formula was based on proposed formula. After testing both formulas on specific data set, obtained results showed that combining two formulas (Sethi, and proposed formula) has better results in terms of false-positive rate. Further, combination of these two formulas has been compared with some existing applications in market. Obtained results also proved that the work carried out, in many cases (e.g., accuracy and precision) works better than other existing applications.

## 6. REFERENCES

[1] Almeida, T. A., Hidalgo, J. M. G., & Yamakami, A. (2011, September). Contributions to the study of SMS spam filtering: new collection and results. In Proceedings of the 11th ACM symposium on Document engineering (pp. 259-262). ACM.

[2] Delany, S. J., Buckley, M., & Greene, D. (2012). SMS spam filtering: methods and data. Expert Systems with Applications, 39(10), 9899-9908.

[3] Nuruzzaman, M. T., Lee, C., & Choi, D. (2011, August). Independent and personal SMS spam filtering. In Computer and Information Technology (CIT), 2011 IEEE 11th International Conference on (pp. 429-435).

[4] Alzahrani, A. J., & Ghorbani, A. A. (2014, May). SMS mobile botnet detection using a multi-agent system: research in progress. In Proceedings of the 1st International Workshop on Agents and Cyber Security (p. 2). ACM.

[5] http://blog.melipayamak.com/posts/look-at-the-history-of-sms-in-the-world/

[6] Mahmoud, T. M., & Mahfouz, A. M. (2012). SMS spam filtering technique based on artificial immune system. *IJCSI International Journal of Computer Science Issues*, *9*(1).

[7] Sethi G, Bhootna V ( 2014) "SMS Spam Filtering Application Using Android "International Journal of Computer Science and Information Technologies, Vol. 5 (3) ,(pp 4624-4626) IJCSIT.

[8] Narayan, A., & Saxena, P. (2013, November). The curse of 140 characters: evaluating the efficacy of SMS spam detection on android. In *Proceedings of the Third ACM workshop on Security and privacy in smartphones & mobile devices* (pp. 33-42). ACM.

[9] Kantardzic, M. (2011). Data mining: concepts, models, methods, and algorithms. John Wiley & Sons.