A Bi-Level Text Classification Approach for SMS Spam Filtering and Identifying Priority Messages

Naresh Kumar Nagwani
Department of Computer Science and Engineering, National Institute of Technology Raipur, India

Abstract: *Short Message Service (SMS) traffic is increasing day by day and trillions of sms are sent and received by billions of users every day. Spam messages are also increasing in same proportionate. Numbers of recent advancements are taking place in the field of sms spam detection and filtering. The objective of this work is twofold, first is to identify and classify spam messages from the collection of sms messages and second is to identify the priority or important sms messages from the filtered non-spam messages. The objective of the work is to categorize the sms messages for effective management and handling of sms messages. the work is planned in two level of binary classification wherein at the first level of classification the sms messages are categorized into the two classes spam and non-spam using popular binary classifiers, and then at the second level of classification non-spam sms messages are further categorized into the priority and normal sms messages. four state of the art popular text classification techniques namely, Naïve Bayes (NB), Support Vector Machine (SVM), Latent Dirichlet Allocation (LDA) and Non-negative Matrix Factorization (NMF) are used to categorize the sms text message at different levels of classification. The proposed bi-level classification model is also evaluated using the performance measures accuracy and f-measure. Combinations of classifiers at both levels are compared and it is shown from the experiments that SVM algorithm performs better for filtering the spam messages and categorizing the priority messages.*

Keywords: *SMS spam, priority sms, important sms, sms spam filtering, bi-level binary classification.*

Received March 24, 2014; accepted August 13, 2014

1. Introduction

Short Message Service (SMS) is the text communication service over the mobile devices. It is one of the essential components of phone, mobile and Personal Digital Assistant (PDA) devices communication systems. SMS allows the information sharing using standard wireless application protocols for transferring the short text messages between the moving devices. According to the International Telecommunication Union (ITU) [13], SMS has become an enormous commercial industry, worth over 81 billion dollars globally as of 2006. The report of Portio research also indicates the importance of SMS messaging services and its impact on mobile business and economy, as per this research, "the worldwide mobile messaging market was worth USD 179.2 billion in 2010, has passed USD 200 billion in 2011, and probably will reach USD 300 billion in 2014. The same study indicates that annual worldwide SMS traffic volumes rose to over 6.9 trillion at end-2010" [31]. As per mobile marketing association [23], "Worldwide over 350 billion text messages, also known as "SMS Messages" are exchanged across the world's mobile networks every month, with over 15% of these messages, according to the Yankee Group, being classified as commercial, or marketing, messages" [23].

The stated facts shows that, in recent years, SMS has become one of the most common communication methods due to rapid increase in the number of mobile phone users worldwide. This increase has inevitably attracted and increased spammers and caused SMS spam (unsolicited) message problem like spam e-mails. Today, majority of SMS messages received by mobile phones are unfortunately disturbing spam messages such as credit opportunities of banks, promotion and discount announcements of stores, fake lottery winning notifications new tariffs of communications service providers and bunch of unwanted advertisements.

The major challenge with the SMS text messages is the standard SMS messaging is limited to 140 bytes (characters) [27]. Moreover, their text is commonly with idioms and abbreviations. So it is a challenging task to identify the Spam from such short messages. Spam SMS's are the unsolicited SMS's which a user does not wish to receive on their mobile devices. SMS spam filtering techniques helps to identify and categorize the incoming SMS as spam and non-spam. SMS spam filtering techniques also helps in reducing the burden of notifications for a mobile user. SMS messaging services today are used by a number of applications also such as mobile banking uses it for multiple purposes like one time password communication. So apart from SMS spam messages, another problem with SMS messaging is identification of priority (important) messages out of received non-spam messages in the mobile devices. Email communication system is also one of the popular communication systems along with the SMS messaging system and most of the Email systems implement the “Priority Inbox” concept in messaging for important messages for the users, however, the same concept is still missing in the SMS messaging communication. Since SMS messaging is also becoming one of the popular messaging system rapidly, it is need of the day that concept like “Priority Inbox” be implemented in such systems. This paper addresses both of the problems by presenting a two level classification system for filtering the spam and priority messages from incoming SMS messages. The purpose of the presented work is to provide an effective categorization of SMS messages for effective handling and management of priority and normal SMS messages.

2. Related Work

Classification of SMS messages is a popular and recent research area, particularly the binary classification of SMS messages where a SMS message is classified as SPAM or Non-SPAM message. A number of innovative approaches are suggested in analyzing and classifying SMS messages, some of the latest development in this direction is discussed here. Performance comparisons of several machine learning methods for classifying SMS messages are performed by Almeida *et al.* [3], where it is shown that Support Vector Machine (SVM) performs better that other evaluated classifiers. Analysis of spam dataset in carried out by Almeida *et al.* [2] in order to ensure that there are no duplicated messages coming from previously existing datasets. An anti-spam framework using hybrid of content-based filtering and challenge-response mechanism is proposed by Yoon *et al.* [44]. This impact analysis of several feature extraction and feature selection approaches for SMS spam filtering is carried out by Uysal *et al.* [34], where an analysis is performed on two different languages, namely Turkish and English. An index-based online text classification method for English and Chinese SMS messages is proposed by Liu and Wang [20].

Rules of spam text messages classification are identified by Wang *et al.* [38] and then filters are designed as per these rules for filtering spam messages. A filtering system without computer system support is proposed by Nuruzzaman *et al.* [28], various activities of SMS spam filtering like training, filtering and updating processes are carried out on mobile phone in the proposed system. Graph data mining based approach is proposed by Xu *et al.* [40], to distinguish spammers from non-spammers and the proposed approach also detects spam without checking a message’s contents. A SMS spam message filter based on feature selection and pattern classification techniques is proposed by Uysal *et al.* [36]. A framework for SMS spam filtering is proposed by Uysal *at el.* [35], the proposed framework is based on two feature selection techniques namely, information gain and chi-square metrics to identify discriminative features for SMS messages. Liu and Yang [19] discusses the classification method of filtering spam messages, and suggested some more work in the direction of SMS classification method. A SMS spam detection algorithm based on spam patterns is proposed by Androulidakis *et al.* [4].

Three corpora of short messages SMS, blog, and spam messages are evaluate using feature-based and compression-model-based spam filters in the work of Cormack *et al.* [8], it is demonstrated that bag-of-words filters can be improved using different features. A survey of existing spam filtering techniques is carried out by Cormack [7]. A worm detection system for Email is presented by Abdulla and Altyeb [1], where two machine learning algorithms namely, K-Nearest Neighbors (KNN) and Naïve Bayes (NB), are used for classifying the worms in Emails. The survey includes the study of spam filtering in email, similarities and differences with spam filtering in other communication and storage media. The feasibility analysis of applying Bayesian learning and SVM for email spam filtering is carried out by Yadav *et al.* [42] and a mobile-based system SMSAssassin is proposed for filtering SMS spam messages. Junaid and Farooq [16] have worked on identifying the features that distinguishes the spam from benign SMS (ham). In the proposed work the SMS is intercepted at the mobile phone access layer and extracted two features namely, octet bigrams, and frequency distribution of octets. Then these features are applied to a number of classifiers to identify mobile spam’s. An analysis of the SMS Spam Collections is performed by Hidalgo *et al.* [12].

An anti-spam technique based on Artificial Immune System (AIS) for filtering SMS spam messages is proposed by Mahmoud *at el.* [21]. The proposed technique is designed using set of some features that can be taken as inputs to spam detection model. A anti text-based message platform for SmartPhones is presented by Lahmadi *et al.* [17]. The proposed spam filtering solution designed using social network based collaborative approach to filter the spam’s using bloom filters and content hashing. A comprehensive study of SMS spam in a large cellular network of US is carried out by Jiang *et al.* [14] and to identify SMS spam activities, a text clustering techniques is proposed to group the associated spam messages. Various characteristics of SMS spamming are demonstrated from the study like spamming rates, victim selection strategies and spatial clustering of spam numbers. A SVM based text message classifier using document frequency threshold is proposed by Parimala and Nallaswamy [29]. For the proposed algorithms experiment are performed with NUS SMS text messages data set.

Tan *et al*. [32] demonstrated that using simple textual features better accuracies can be achieved in spam classification tasks. A review of various SMS spam filtering techniques is carried out by Delany *et al*. [9]. Various issues related to data collection are discussed in the work. A method which uses byte-level data coding scheme of SMS to detect spam messages is proposed by Rafique and Farooq [30]. The proposed method is designed using a model of byte-level distributions of spam messages along with the spam models using Hidden Markov Models (HMM). A study of the methods used in spam filtering is carried out by Narayan [27], a two-level stacked classifier is also proposed for short text messages and shown that accuracy is improved over Bayesian email spam filters. An analysis on SMS spam traffic is performed [25, 26, 27] to identify the key characteristics of fraud activity. Communication patterns of spammers are compared with legitimate cell-phone users and Machine to Machine (M2M) connected appliances. It is demonstrated that M2M systems give similar communication profiles to spammers, which can affect spam filters. Latent Dirichlet Allocation (LDA), a generative topic modeling technique is used to extract latent features arising from mobile SMS communication for identifying the user interest by Modupe [24].

3. Text Classifiers

Text categorization is a process of approximating an unknown category assignment function F:D×C→{0, 1}, where D is the set of all possible documents and C is the set of predefined categories. The value of F (d, c) is 1 if the document d belongs to the category c and 0 otherwise. The approximating function M:D×C→{0, 1} is called a text classifier by Feldman and Sanger [11]. A number of text classifiers exist for categorization of text document collections, four popular text classifiers namely, NB, SVM, LDA and Non-negative Matrix Factorization (NMF) are used in this work which are discussed here in brief.

NB algorithm [15, 22] is a probability based model for classification. NB algorithm is based on assumption that all features are statistically independent of each other. NB algorithm is used in number of applications for classification tasks. NB classifiers can predict class membership probabilities, like the probability of a given object belongs to a particular class (category). SVM [10, 37] is a boundary based classifier that constructs hyper planes which splits the classes. These hyper planes identify boundaries for object classification. It uses nonlinear mapping to transform the original training data into a higher dimension. Within this new dimension, it searches for the linear optimal separating hyper-plane. With an appropriate nonlinear mapping to a sufficiently high dimension, data from two classes can always be separated by a hyperplane. The SVM finds this hyperplane using support vectors and margins.

LDA by Blei *at el*. [5] models text documents as mixtures of latent topics, which are key concepts presented in the text. The topic mixture is drawn from a conjugate Dirichlet prior that is the same for all documents. The topic modeling for SMS text collection using LDA is performed in four steps. LDA estimates the topic-term distribution and the document topic distribution from an unlabled collection of documents using Dirichlet priors for the distributions over a fixed number of topics. NMF [18, 41] is a matrix factorization algorithm. NMF algorithm is used to identify the positive factorization for a given positive matrix. NMF algorithm is used for document clustering for a given Term Document Matrix (TDM) in text mining. The TDM is consisting of terms present in row and document in column, each cell T_{ij} in TDM presents the number of occurrences of a Term T_i in the document D_j. One of the most useful properties of NMF is that it generates a sparse representation of the data for better analysis. TDM is a positive matrix and if positive factors of this matrix can be generated then it can be utilized effectively better analysis of text document collections. In this work NMF is utilized for analysis of SMS text collections.

4. Methodology

The methodology of the proposed work is presented in the Figure 1. The work is performed in three major stages. In the first stage SMS spam collection is retrieved and pre-processed for analyzing it. Then in the next stage a binary classifier is applied (first level classification L1) to classify the SMS message as Non-spam (Ham) or Spam. Then in the last stage another binary classifier is applied (second level classification L2) on the Ham messages classified in the stage two to further filter the prioritized SMS message and normal SMS messages.

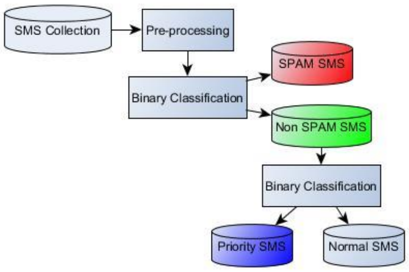

Figure 1. The process of Bi-level classification for spam filtering and priority message identification.

In the first stage a suitable SMS spam collection is identified the pre-processing techniques are applied on it. The problem with the SMS messages is that, the keyword can easily be replaced by other symbols, which increase the difficulty of understanding and analyzing by computer programs, hence sophisticated pre-processing techniques are required for processing of SMS text messages and making it ready for the classification. The pre-processing task is consist of two major pre-processing techniques namely stopping and stemming and one special pre-processing technique particularly related to short messages pre-processing named as homoglyphing.

Generally in the text collection a number of words exists which are not having any significance meaning from the analysis (pattern discovery) point of view for example the words “The”, “is”, “was”, “were” and so many do not considered to be important from analysis point of view, such words are called as stop words or useless words. In stopping the useless words are eliminated from the text collection. Generally, the stopping is implemented with the help of maintaining a stop list, which is consist of all the stop words required to be deleted (omitted) from the text collection in order to prepare the text collection ready for the analysis. After stopping, stemming pre-processing technique is applied over the text collection. The purpose of stemming is to convert the words to their root forms so that all the occurrences of the words are presented uniformly in the text collection for perfect analysis. For example the words “works”, “working”, “worked” will be concerted to the word “work” to its root meaning to make sure that the words is considered uniformly as a unique word for textual analysis.

Homoglyphing and Eliminating textese-Apart from the stopping and stemming a special pre-processing technique namely, homoglyphing is applied on SMS text collection which is generally not required for the other textual data. A homoglyph or glyphs word appears identical to a particular standard word. For example the word “Hello” can be written as “Hell0” or “He11o” which looks identical while reading. Most of the SMS messaging users use homoglyphs frequently in SMS messaging fashion. Homoglyphs are formed by replacing the particular characters by similar appearance characters in a word for example the digit zero and the capital letter “O” (i.e., “0” and “O”); and the digit one, the lowercase letter “L” and the uppercase “i” (i.e., “1”, “l” and “I”) appears similar while reading. Homoglyphs are the great source of confusion particularly by the computer programs, since program will differentiate the homoglyphs words although they are meant for the same word in the same context. Since the homoglyphs are frequently used in SMS messaging pre-processing is required in order to covert the homoglyphs to its actual form for better analysis of SMS text collection. SMS (Mobile) messages are formed in a linguistic style with the help of abbreviations for faster messaging which is named as SMS language or textese. In order to analyze the SMS messages effectively these textese terms should be addressed properly which requires advance pre-processing techniques to identify the actual equivalent terms for the given abbreviations.

First Level Classification (L1)-After the pre-processing on the SMS collection various binary classifications like NB, SVMs, Nonnegative Matrix Factorization and classification using LDA is applied for categorizing the SMS messages into two categories namely, Ham and Spam.

Second Level Classification (L2)-After the first level of binary classification, the SMS collections are categorized in two categories Spam and Ham (Non-Spam). Then binary classification techniques are again applied over the Ham (Non-Spam) messages to further categorize the Ham SMS messages into two categories namely, Priority SMS and Normal SMS.

Parameter Evaluation-After successful completion of categorization at both of the levels the classification performance is evaluated using various classification parameters such as F-measure (combined measure of precision and recall) and Accuracy. The evaluations for both levels are performed to measure the performance of proposed system.

A term message matrix is generated for the message collection, where each row gives the frequency of a particular term present in messages represented by columns. This matrix presents the initial data for analyzing SMS text collections.

$$T = \begin{bmatrix} t_{11} & L & t_{1m} \\ M & O & M \\ t_{n1} & L & t_{nm} \end{bmatrix}$$

The binary classifier is applied on the processed SMS text collection to categorize the SMS message as Spam and Non-Spam (Ham). The binary classifier is again applied on the Non-Spam messages to further categorize as Priority message and Normal message. Clustering and creating groups of similar spam and priority SMS to get characteristics of spam and priority messages and predict the new SMS as spam or priority as per these characteristics. Priority SMS are categorized on the basis of SMS message content, considering the date mentioned in the message along with the other keywords such as urgent, important and priority.

5. Performance Evaluation

5.1. Accuracy

The accuracy of the classifiers is evaluated in terms of ratio of correctly classified SMS messages to the total number of SMS messages selected for classification from SMS collection as shown in the Equation 1.

$$Accuracy = \frac{Number\ of\ Correctly\ Classified\ SMS\ Messages}{Total\ Number\ of\ SMS\ Messages} \quad (1)$$

5.2. F-measure

The parameters for performance evaluation are derived from confusion matrix which is presented in the Table 1.

Table 1. Confusion matrix.

	Predicted Spam	Predicted Ham
Actual Spam	TP	FP
Actual Ham	FN	TN

True Positive (TP) is the number of spam messages detected as spam, False Positive (FP) is the number of non-spam messages detected as spam, True Negative (TN) is the number of non-spam messages detected as non-spam, False Negative (FN) is the number of spam messages detected as non-spam. F-measure is computed by combining the two popular measures in text mining namely, precision and recall. Precision (P) is the ration of TPs to all positives (i.e., sum of TPs and FPs) and Recall (R) is the ration of TPs to TPs and FNs. Precision, Recall and F-measures calculations are presented in the Equations 2, 3, and 4, respectively. Accuracy can also be computed using the confusion matrix as the ration of true observations to all observations as shown in the Equation 5.

$$F\ or\ F_1\text{ - }measure = \frac{2 \times P \times R}{P + R} \quad (2)$$

$$Precision(P) = \frac{TP}{TP + FP} \quad (3)$$

$$Recall(R) = \frac{TP}{TP + FN} \quad (4)$$

$$Accuracy = \frac{TP + TN}{TP + FP + FN + TN} \quad (5)$$

6. Experiments

The implementations are carried using Java based Weka API [39] and SVM implemented using LIBSVM [6, 10].

6.1. Datasets

The SMS Spam Collection is public available at http://www.dt.fee.unicamp.br/~tiago/smsspamcollection.

Table 2. Examples of messages present in the SMS Spam Collection.

Category	SMS
Ham	U dun say so early hor... U c already then say...
Ham	Nah I don't think he goes to usf, he lives around here though
Spam	FreeMsg Hey there darling it's been 3 week's now and no word back! I'd like some fun you up for it still? Tb ok! XxX std chgs to send, Â£1.50 to rcv
Ham	Even my brother is not like to speak with me. They treat me like aids patent.
ham	As per your request 'Melle Melle (Oru Minnaminunginte Nurungu Vettam)' has been set as your callertune for all Callers. Press *9 to copy your friends Callertune
spam	WINNER!! As a valued network customer you have been selected to receivea Â£900 prize reward! To claim call 09061701461. Claim code KL341. Valid 12 hours only.
spam	Had your mobile 11 months or more? U R entitled to Update to the latest colour mobiles with camera for Free! Call The Mobile Update Co FREE on 08002986030
ham	I'm gonna be home soon and i don't want to talk about this stuff anymore tonight, k? I've cried enough today.

The collection is composed by 4,827 legitimate messages and 747 mobile spam messages, a total of 5,574 short messages. It is the one of the largest SMS spam corpus [2]. Example of SMS message in the SMS dataset is shown in the Table 2. Another dataset is available on UCI machine learning repository [33].

The dataset has a total of 81,175 tokens and mobile phone spam has in average ten tokens more than legitimate messages. Total 63,632 and 17,543 tokens are present in non-spam and spam messages [2]. The selected SMS text collection is consisting of 6840 unique non-spam (Ham) terms and 1798 unique Spam terms available in it. The twenty tokens that most appeared in ham messages and spam messages after pre-processing of SMS text messages are presented in the table. The top 20 Terms in Ham and Spam messages after Pre-processing are shown in the Table 3.

Table 3. Top 20 terms in ham and spam messages after Pre-processing.

No	Ham (Non-Spam) Term	Spam Term
1	msgs	Nos
2	mis	Cds
3	dis	Ans
4	thts	Tcs
5	loos	Msgs
6	ps	Member
7	hrs	Inclus
8	imposs	Uks
9	hows	Yrs
10	bros	Pics
11	frnds	Chgs
12	whos	girl
13	class	Tscs
14	realis	bid
15	miss	cs
16	gas	Wks
17	mas	txts
18	cos	age
19	pls	service
20	Teas	tncs

6.2. Identification of Spam and Priority Messages

Discrimination between the spam and non-spam (ham) messages is performed using taxonomic terms present in SMS text messages. The frequent terms available in non-spams and spam SMS messages are presented in the Table 3. These terms are used for differentiating between the spam and non-spam messages by various classification algorithms. Example of spam term mentioned in table is “tncs” which is present in most of the spam messages in the abbreviation of “terms and conditions”. In the similar manners the priority messages are also indentified from the non-spam SMS messages by filtering them using a set of terms which indicates the importance of a SMS messages. A set of such terms are identified from non-spam messages. Similarly, the terms which indicate the importance of a SMS messages are identified for categorizing the non-spam messages into the two categories namely, priority and normal messages. Terms like “urgent”, “important” and “deadline” etc. are considered while identifying a priority message from the non-spam SMS messages.

6.3. Result Analysis

Four binary classification techniques namely, NB, SVM, NMF and classification using LDA is applied for two level classification of SMS messages. The classification task is performed in two levels. In the first level classification is performed for categorizing the SMS into two categories Spam and Non-Spam (Ham). Then in the second level again classification is performed for Non-Spam (Ham) messages to categorize the Non-Spam messages into Normal and Priority SMS message. In classification using LDA technique, first clustering is performed on SMS text collection and two clusters are created then by applying LDA one each cluster topic terms are generated for each clusters using which the categories of each cluster is decided as Spam and Non-Spam. The result of applying four classifiers at both of the levels is tabulated in the Table 4.

Table 4. Performance parameters for both levels of classification for various classifiers.

First Level Classification (L1)			Second Level Classification (L2)		
Algorithm	Accuracy	F-measure	Algorithm	Accuracy	F-measure
NB	84.2	0.87	NB	90.21	0.88
			SVM	94.44	0.92
			NMF	93.22	0.91
			LDA	93.18	0.89
SVM	93.45	0.94	NB	92.45	0.90
			SVM	96.68	0.95
			NMF	94.25	0.86
			LDA	91.23	0.89
NMF	91.65	0.92	NB	92.68	0.88
			SVM	96.37	0.94
			NMF	92.24	0.93
			LDA	91.48	0.89
LDA	90.42	0.92	NB	89.21	0.87
			SVM	93.63	0.92
			NMF	92.29	0.91
			LDA	90.88	0.87

To analyze and compare various classifiers used in this study, graphs are generated and shown in the Figures 2 and 3. The value of performance parameter accuracy and F-measure for classifier at both levels is shown in the Figures 2 and 3. It is clearly shown from the Figure 2 that accuracy wise algorithm SVM performs better in both of the levels of classifying the SMS text messages. At the second level SVM algorithm performs better than other algorithms irrespective of the algorithm used at the first level of SMS message classification. Similarly it is clearly shown from the Figure 3 that SVM algorithm performs better in terms of F-measure parameter also. The algorithm SVM performs better in second level of categorization also irrespective of the algorithm used in first level of SMS message classification.

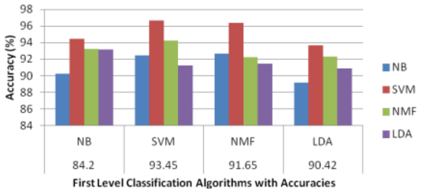

Figure 2. Accuracies of various classifiers at bi-level classification of SMS message collection.

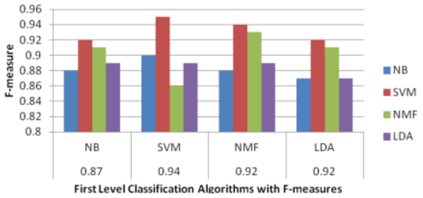

Figure 3. F-measure of various classifiers at bi-level classification of SMS message collection.

7. Practical Implication of the Work

The proposed work can be utilized efficiently in a number of ways to create the advance applications for SMS messaging services. Some examples of such applications are described here.

- Identification of SPAM’s for short messaging-The basic application of proposed technique is to classify the SMS message as Spam and Non-Spam, so an efficient SMS Spam filter can be designed for filtering the Spam SMS filter.
- Personalized SMS Prioritization (PSP)-With the help of two level SMS message classification system, SMS Spam’s can be filtered at initial level then in the subsequent levels further classification can be performed in order to create the priority inbox for incoming SMS messages for implementing personalized SMS prioritization. Email prioritization [43] is a very popular existing technique in Email communication whereas this is new in SMS message communication.
- Creating groups of similar SMS messages-Groups of similar SMS messages can be created by using LDA and NMF techniques discussed in this work. It will help the users in understanding the similar messages received together.
- Identification of SMS Threading-Email threading is a popular research area where the groups of Email messages belonging to the same communication context is formed to represent a single communication thread. A number of techniques for identifying Email threads are available but it is still a novel area in SMS messaging. Identification of SMS threads can be performed by the proposed work by configuring the clusters generated by LDA and NMF techniques.

8. Conclusions

In this study a bi-level classification model is developed for categorizing the SMS messages to spam and non-spam at first level and then the non-spam messages are further classified into normal and priority messages at second level. Various combinations of classifiers are selected at different level of classifying the SMS messages. From the experiments and results it is shown that accuracy and F-measure wise algorithm SVM performs better than other three algorithms NB, NMF and LDA. It is also shown that SVM performs better in second level classification also irrespective of the first level of classification algorithm.

References

[1] Abdulla S., Ramadass S., Altaher A., and Al-Nassiri A., "Employing Machine Learning Algorithms to Detect Unknown Scanning and Email Worms," *The International Arab Journal of Information Technology*, vol. 11, no. 2, pp. 140-148, 2014.

[2] Almeida T., Hidalgo J., and Silva T., "Towards SMS Spam Filtering: Results under a New Dataset," *International Journal of Information Security Science*, vol. 2, no. 1, pp. 1-18, 2013.

[3] Almeida T., Hidalgo J., and Yamakami A., "Contributions to the Study of SMS Spam Filtering: New Collection and Results," *in Proceeding of ACM Symposium on Document Engineering*, California, pp. 259-262, 2011.

[4] Androulidakis I., Vlachos V., and Papanikolaou A., "Spam Goes Mobile: Filtering Unsolicited SMS Traffic," *in Proceeding of IEEE 20th Telecommunications Forum*, Serbia, pp. 1452-1455, 2012.

[5] Blei D., Ng A., and Jordan M., "Latent Dirichlet Allocation," *The Journal of Machine Learning Research*, vol. 3, pp. 993-1022, 2003.

[6] Chang C. and Lin C., http://www.csie.ntu.edu.tw/~cjlin/libsvm/, Last Visited 2014.

[7] Cormack G., "Email Spam Filtering: A Systematic Review," *Foundations and Trends in Information Retrieval*, vol. 1, no. 4, pp. 335-455, 2007.

[8] Cormack G., Hidalgo J., and Sánz E., "Spam Filtering for Short Messages, Methodology," *in Proceeding of ACM 16th Conference on Information and Knowledge Management*, Lisbon, pp. 313-320, 2007.

[9] Delany S., Buckley M., and Greene D., "SMS Spam Filtering: Methods and Data," *Expert Systems with Applications*, vol. 39, no. 10, pp. 9899-9908, 2012.

[10] EL-Manzalawy Y., http://www.cs.iastate.edu/~yasser/wlsvm/, Last Visited 2014.

[11] Feldman R. and Sanger J., *The Text Mining Handbook*, Cambridge University Press, 2007.

[12] Hidalgo J., Almeida T., and Yamakami A., "On the Validity of a New SMS Spam Collection," *in Proceeding of 11th IEEE International Conference on Machine Learning and Applications*, Florida, pp. 240-245, 2012.

[13] International Telecommunication Union (ITU), http://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-IR.DL-2-2006- R1-SUM-PDF-E.pdf, Last Visited 2014.

[14] Jiang N., Jin Y., Skudlark A., and Zhang Z., "Understanding SMS Spam in a Large Cellular Network: Characteristics, Strategies and Defenses," *in Proceeding of the 16th International Symposium on Research in Attacks, Intrusions, and Defenses*, Rodney Bay, pp. 328-347, 2013.

[15] John G. and Langley P., "Estimating Continuous Distributions in Bayesian Classifiers," *in Proceeding of 11th Conference on Uncertainty in Artificial Intelligence*, Montréal, pp. 338-345, 1995.

[16] Junaid M. and Farooq M., "Using Evolutionary Learning Classifiers to do MobileSpam (SMS) Filtering," *in Proceeding of the 13th Annual Conference on Genetic and Evolutionary Computation*, Dublin, pp. 1795-1802, 2011.

[17] Lahmadi A., Delosieres L., and Festor O., "Hinky: Defending Against Text-Based Message Spam on Smartphones," *in Proceeding of IEEE International Conference on Communications*, Kyoto, pp. 1-5, 2011.

[18] Lee D. and Seung H., "Learning the Parts of Objects by Non-Negative Matrix Factorization," *Nature*, vol. 401, no. 6755, pp. 788-791, 1999.

[19] Liu G. and Yang F., "The Application of Data Mining in the Classification of Spam Messages," *in Proceeding of International Conference on Computer Science and Information Processing*, Shaanxi, pp. 1315-1317, 2012.

[20] Liu W. and Wang T., "Index-based Online Text Classification for SMS Spam Filtering," *Journal of Computers*, vol. 5, no. 6, pp. 844-851, 2010.

[21] Mahmoud T. and Mahfouz A., "SMS Spam Filtering Technique Based on Artificial Immune System," *International Journal of Computer Science*, vol. 9, no. 2, pp. 589-597, 2012.

[22] Mccallum A. and Nigam K., "A Comparison of Event Models for Naive Bayes Text Classification," *in Proceeding of 15th National Conference on Artificial Intelligence Workshop on Learning for Text Categorization*, Wisconsin, pp. 41-48, 1998.

[23] Mobile Marketing Association http://www.mmaglobal.com, Last Visited 2014.

[24] Modupe A., Olugbara O., and Ojo S., "Investigating Topic Models for Mobile Short Messaging Service Communication Filtering," *in Proceeding of World Congress on Engineering*, London, pp. 3-5, 2013.

[25] Murynets I. and Jover R., “Analysis of SMS Spam in Mobility Networks,” *International Journal of Advanced Computer Science*, vol. 1, no. 1, pp. 1-8, 2011.

[26] Murynets I. and Jover R., “Crime Scene Investigation: SMS Spam Data Analysis,” *in Proceeding of ACM Conference on Internet Measurement Conference*, Massachusetts, pp. 441-452, 2012.

[27] Narayan A., “The Curse of 140 Characters: Evaluating the Efficacy of SMS Spam Detection on Android,” *in Proceeding of 3rd ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, Berlin, pp. 33-42, 2013.

[28] Nuruzzaman M., Lee C., and Choi D., “Independent and Personal SMS Spam Filtering,” *in Proceeding of IEEE 11th International Conference on Computer and Information Technology*, Paphos, pp. 429-435, 2011.

[29] Parimala R. and Nallaswamy R., “A Study on Analysis of SMS Classification Using Document Frequency Thresold,” *International Journal of Information Engineering and Electronic Business*, vol. 1, pp. 44-50, 2012.

[30] Rafique M. and Farooq M., “SMS SPAM Detection by Operating on Byte-Level Distributions Using Hidden Markov Models (Hmms),” *in Proceeding of 20th Virus Bulletin International Conference*, Vancouver, pp. 1-7, 2010.

[31] Ranjbarian B., Rehman M., and Lari A., “Attitude toward SMS Advertising and Derived Behavioral Intension, an Empirical Study Using TPB (SEM method),” *Journal of American Science*, vol. 8, no. 7, pp. 297-307, 2012.

[32] Tan H., Goharian N., and Sherr M., “$100,000 Prize Jackpot. Call Now! Identifying the Pertinent Features of SMS Spam Categories and Subject Descriptors,” *in Proceeding of 35th International ACM SIGIR Conference on Research and Development in Information Retrieval*, Oregon, pp. 1175-1176, 2012.

[33] UCI Spam Collection-http://archive.ics.uci.edu/ml/datasets/SMS+Spam+Collection#, Last Visited 2014.

[34] Uysal A., Gunal S., Ergin S., and Gunal E., “The Impact of Feature Extraction and Selection on SMS Spam Filtering,” *Electronics and Electrical Engineering*, vol. 19, no. 5, pp. 67-72, 2013.

[35] Uysal A., Gunal S., Ergin S., and Gunal E., “A Novel Framework for SMS Spam Filtering,” *in Proceeding of IEEE International Symposium on Innovations in Intelligent Systems and Applications*, Trabzon, pp. 1-4, 2012.

[36] Uysal A., Gunal S., Ergin S., and Gunal E., “Detection of SMS Spam Messages on Mobile Phones,” *in Proceeding of 20th IEEE Signal Processing and Communications Applications Conference*, Mugla, pp. 1-4, 2012.

[37] Vapnik V., *The Nature of Statistical Learning Theory*, Springer, 1995.

[38] Wang Q., Han X., and Wang X., “Studying of Classifying Junk Messages Based on The Data Mining,” *in Proceeding of IEEE International Conference on Management and Service Science*, Wuhan, pp. 1-4, 2009.

[39] Waikato Environment of Knowledge Analysis, http://www.cs.waikato.ac.nz/ml/weka/, Last Visited 2014.

[40] Xu Q., Xiang E., Yang Q., Du J., and Zhong J., “SMS Spam Detection Using Noncontent Features,” *IEEE Intelligent Systems*, vol. 27, no. 6, pp. 44-51, 2012.

[41] Xu W., Liu X., and Gong Y., “Document Clustering Based on Non-Negative Matrix Factorization,” *in Proceeding of 26th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval*, Toronto, pp. 267-273, 2003.

[42] Yadav K., Kumaraguru P., Goyal A., Gupta A., and Naik V., “Smsassassin: Crowdsourcing Driven Mobile-Based System for SMS Spam Filtering, System,” *in Proceeding of 12th Workshop on Mobile Computing Systems and Applications*, Arizona, pp. 1-6, 2011.

[43] Yang Y., Yoo S., Lin F., and Moon I., “Personalized Email Prioritization Based on Content and Social Network Analysis,” *IEEE Intelligent Systems*, vol. 25, no. 4, pp. 12-18, 2010.

[44] Yoon J., Kim H., and Huh J., “Hybrid Spam Filtering for Mobile Communication,” *Computers and Security*, vol. 29, no. 4, pp. 446-459, 2010.

Naresh Kumar Nagwani has completed his graduation in Computer Science and Engineering in 2001 from G. G. Central University, Bilaspur. He completed his post-graduation Master of Technology in Information Technology from ABV-Indian Institute of Information Technology, Gwalior in 2005 and completed the Ph.D. in Computer Science and Engineering in 2013 from National Institute of Technology Raipur, India. His area of interest is data mining, text mining, mining software repositories and information retrieval. His employment experience includes Software Developer and Team Lead at Persistent Systems Limited and presently Assistant Professor at NIT Raipur. He has published more than 20 research papers in various journals and conferences.