SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM
TMLAI TRANSACTIONS ON MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE
Volume 7 No 5
ISSN 2054-7390

A Survey of Emerging Techniques in Detecting SMS Spam

[1]Sahar Saad Alqahtani, [2]Daniyal Alghazzawi
[1,2] Department of Information Systems, Faculty of Computing and Information Technology at King Abdulaziz University, Jeddah, Saudi Arabia;
sqahtanie@kku.edu.sa; dghazzawi@kau.edu.sa

ABSTRACT

This In the past years, spammers have focused their attention on sending spam through short messages services (SMS) to mobile users. They have had some success because of the lack of appropriate tools to deal with this issue. This paper is dedicated to review and study the relative strengths of various emerging technologies to detect spam messages sent to mobile devices. Machine Learning methods and topic modelling techniques have been remarkably effective in classifying spam SMS. Detecting SMS spam suffers from a lack of the availability of SMS dataset and a few numbers of features in SMS. Various features extracted and dataset used by the researchers with some related issues also discussed. The most important measurements used by the researchers to evaluate the performance of these techniques were based on their recall, precision, accuracies and CAP Curve. In this review, the performance achieved by machine learning algorithms was compared, and we found that Naive Bayes and SVM produce effective performance.

Keywords: SMS spam detection, Text classification, SMS spam filtering, SMS spam dataset, Text features extraction.

1 Introduction

By the advancement in technology of mobile communications and mobile phones expansion, Short Message Service (SMS) has turned out to be a popular mode of communication due to its ease of operation and less cost. SMS technique is used to send a text message from one mobile device to another. Some of these messages that reach the user's device are unwanted and annoying which called spam. In the smartphones age, user has confidential and personal information such as passwords, images, numbers of credit card, contact lists that stored on these phones, making those users more vulnerable to cyber-attacks by spam SMS. Spam may leak sensitive information, privacy invasion, or access unauthorized information. Spammer are people with unethical activities can access data in smartphone without the end-user knowledge, exposing the privacy of the user to the path that results in financial or functional loss. Nowadays, Spam messages appear to be increasing where it is annoying users and also dramatically lose their data. This kind of problems has inspired many researchers to develop collections of techniques to assist effectively in detect and prevent spam SMS. The availability of SMS datasets to be applied in train and test techniques in order to detect spam in SMS are small sized and still limited. Moreover, the availability of features number needed to detect spam messages in text are less, this is due to the text messages length is short.

DOI: 10.14738/tmlai.75.7116
Publication Date: 05th October, 2019
URL: http://dx.doi.org/10.14738/tmlai.75.7116

The objective of this paper is to review the emerging technologies used in detect SMS spam. Our survey includes various datasets of SMS spam used by researchers. This work also provides comparison and analysis of the different techniques on different datasets and their performance according to their accuracies, precision and recall.

The structure of our paper is as follows: Section 2 presents overview of detecting SMS spam. In section 3, we review applications of researchers in detecting SMS spam. The techniques used in the process of filtering SMS spam were investigated and displayed in section 4. The feature extraction process is discussed in section 5 while section 6 presents the available and used dataset of SMS. The measurements used by researchers to evaluate the performance of the techniques used were discussed in section 7. Finally, the paper concludes in last section.

2 Overview of Detecting SMS Spam

Over the past decade, spam SMS number causing issues to users through advertisement has been increased dramatically. consequently, researchers have produced different techniques of spam detection over last years to achieve the results accuracy. Recently, there are many published papers by researchers whose working in this field. In the context, spam messages are very similar to spams in email that usually have several business interests. Spam messages in SMS is typically utilized for spreading phishing links and commercial advertising. Spammers in commercial advertising use malware for sending SMS spam as it is illegitimate in many countries [1]. The service of SMS has restricted number of characters, that involve a few symbols, numbers and alphabets. Usually the pattern of SMS spam seems is asking the users to visit some URL, reply by SMS or call a number. In general, spams in SMS can be detected by reviewing and examining contents of message that means features of content. The pattern can be observed from the output of simple queries on the spam dataset. Spammers are usually utilizing minimal volumes and advanced methods in order to avert detection that seems a worrying dynamic. They transmit tiny amounts of SMS spam to observe how the infrastructure of operator in SMS reacts and then identify the policies of volume limits [2]. Based on that, content-based filtering technology is very important to counteract the rising threat in spam messages. There is a continual discussion on SMS spam filtering where the researchers have come up with technical measures that concrete for tackling this issue. The majority of discovered practices and measures can be utilized for dealing with SMS spam. From the literature, the most widely accepted technique and the prominent ones is Bayesian filters. In the following sections we will review all the researchers' applications to detect SMS spam, what techniques have been used, which data set has been applied, and what their method is to extract features from messages.

3 Application of Detecting Spam In SMS

Recently, the research on detecting the SMS spam messages was the focus of attention of researchers worldwide. In this section, we attempt to present all the previous studies conducted to detect SMS spam messages sent to mobiles' users. The application of filtering spam in short messages differed, according to these studies as we shall see in this section. Whereas Support Vector Machine (SVM), Convolutional Neural Network (CNN), Latent Dirichlet Allocation (LDA), Logistic Regression (LR), Random Forest (RF), AdaBoost, Artificial Neural Network (ANN), k-Nearest Neighbor (k-NN), Decision Tree (DT), Optimum-Path Forest (OPF), Fisher's linear discriminate analysis (FDA), Non-negative Matrix Factorization (NMF) and Naive Bayes (NB) were the approaches used in these studies. The description of these technologies in details is presented in section 4.

In 2018, Mehul et al. used different eight machine learning algorithms i.e. SVM, NB, DT, LR, RF, AdaBoost, ANN and CNN. They analyzed and compared the detection capability of these classifiers on two various datasets i.e. 'SMS Spam Collection V.1' and 'Spam SMS Dataset 2011-12'. All of these classifiers have been evaluated based on their accuracies, precision, recall and CAP Curve values. They approved that CNN classifier achieved the highest accuracy of 99.19% and 98.25% on the two used datasets. Among the remaining used algorithms, NB and SVM showed good outcomes, very close to convolutional neural network on both the data sets [3].

In this context, Neelam and Ankit in [4] used four algorithms from machine learning field which are NB, LR, DT, and RF on 'SMS Spam Corpus v.0.1' in addition to 200 messages collected manually. They also studied SMS spam characteristics deeply and then prouduce ten features that are presence of mathematical symbol, URLs, dots, special symbols, emotions, lowercased words, uppercased words, mobile number, keyword specific for spam and not spam, message length. They evaluated these classifiers based on the following criterias, that will be discussed in section 6, f1 score, true negative (TN), true positive (TP), false negative (FN), false positive (FP) accuracy, recall and precision. The best algorithms of their proposed approaches in the process of detecting SMS spam was Random Forest that accomplished 1.02% false positive rate and 96.5% true positive rate.

On other hand, researchers in [5] planned to feed the classification algorithms essentially with two features: the matrix of count vectorizer and the message length on one dataset i.e. 'SMS Spam Collection V.1' by using Logistic Regression, Random Forest and Naïve Bayes classifiers. Their priorities in ranking the used classifier based on accuracy of algorithm in detecting spam messages. They found that NB outperforms RF and LR algorithms in classifying SMS spam where it achieved a high accuracy (98.445).

Authors in 2016 [6] perform many modifications in Support Vector Machine (VSM) method in order to address the difficulties in filtering issue of spam SMS. The dataset they are working on has been collected from 'Dahan Tricom database'. The result of their technology has been evaluated by precise, recall and F1 score that deployed in Dahan Tricom Corporation and this technology will be applicable in SMS commercial companies.

Traditionally, convolutional neural network has been utilized for problems related to classifying image. The paper by Milivoje et al. [7] in 2018 ran counter to this idea by using CNN for classifying SMS spam messages. Crucial step in their work was preprocessing the data by removing stop words, tokenization, reducing text to lower case where they are working on 'SMS Spam Collection V.1' dataset. They prove that their proposed CNN for spam classification can produce the best compared to several other machine learning techniques where it achieved accuracy of 98.4% and AUC score of 0.955.

British English SMS Corpora (BEC), UCI Machine Learning (UCI) and Dublin Institute of Technology (DIT) are three dataset that used by Nurul and Mohd [8]. They consider that numbers and symbols in dataset should not be cleaned because it may help in the detection process beside the SMS length and keywords. They train and test these datasets on four classifiers i.e. Decision Tree (DT), Support vector machine (SVM), k-Nearest Neighbor (k-NN), Naïve Bayes (NB). They found that all of these algorithms correctly classified the SMS spam in the three used datasets.

Research's Naresh aims to determine and category spam SMS from 'SMS Spam Collection V.1' dataset and also to identify the priority SMS messages. He used Non-negative Matrix Factorization (NMF) and Latent

Dirichlet Allocation (LDA) in combinations with Support Vector Machine (SVM) and Naïve Bayes (NB). The performance of these classifiers measured by accuracy and f score that showed that SVM classifier produces the best in filter SMS spam and classifying the priority SMS [9].

Some researchers focus on suggesting methods to extract features from messages. Such as Noura et al. [10] that used topic modelling technique such as latent Dirichlet allocation to extract the features from 'SMS Spam Collection V.1' dataset. They tried many algorithms with these features and their result are compared against other spam detection algorithms. They reported that their suggested method accomplishing over 97% accuracy comparing favorably to better reported classifiers displayed in the literature. In this context, Jialin et al. in 2016 [11] suggest a method for filtering SMS spam called a Message Topic Model (MTM) that work on two different datasets: 'DIT SMS Spam Dataset' and 'SMS Spam Collection v.1'. The proposed method compared with Support Vector Machine and the standard Latent Dirichlet Allocation on the same dataset and they found that Message Topic Model is more efficient for filtering spam in SMS spam.

In 2015, the paper of Dheny et al. [12] used OPTIMUM-PATH FOREST on 'SMS Spam Collection V.1' dataset with preparing a dictionary of 12,622 words as features that help algorithm to perform the classification task without any other preprocessing technique on the data. They validated their approaches against with k-NN, Artificial Neural Networks classifier and Support Vector Machine. They have shown promising results for their used classifier as there is no need for a high computational load compared with SVM classifier and it correctly classified all ham messages.

4 Techniques Used for Detecting SMS Spam

In the literature, various preprocessing techniques have been implemented on various SMS spam datasets to detect spam in short text messages. A brief description of these techniques is presented as follow:

4.1 Naive Bayes (NB) [13]:

It is a classification technique based on theorem of 'Bayes' that assume independence among predictors. This classifier of Bayesian supposes that there is no relationship between presence of a specific feature in one class and the existence of any other features. Even if there are dependencies between the existence of the feature with each other, this classifier will treat all desired properties as independent that contribute in the probability score. The Naive Bayes classifier is still simple and sturdy in the case of the dimensionality of desired input is high. Multinomial Naive Bayes (MNB) is a new advanced version of Naive Bayes classifier. The basic advancement is the presence of independency among document class and length. this classifier includes multinomial distribution that works well for data type that is countable like the words inside a text or document. So, with classifier of NB is a conditional independency between each the feature in the model, while classifier of MNB is a particular case of a Naive Bayes algorithm that utilize a multinomial distribution for each feature. In our reviewing process, we found that using Naive Bayes algorithm in SMS spam filtering the first most prominent technique used by researchers as its applied by [3][4][5][8][9].

4.2 Support Vector Machine (SVM) [14]:

It is a characteristic classifier that is vastly utilized for the task of classification. The algorithm of SVM plots all item in n-dimensional space as a point supposing each feature value as a specific coordinate value. Then it constitutes a line which divides the full data into two variously data groups. The adjacent points in

these groups will be the furthest from the dividing line. In our reviewing process, we found that using support vector machine algorithm in SMS spam filtering the second most prominent technique used by researchers as its applied by [3][7][8][9].

4.3 Decision Tree (DT) [15]:

DT is an algorithm based on supervised learning that is usually used for tasks related to classification. This algorithm works with both continuous and categorical variables. Initially, the algorithm will split the population for many homogeneous groups that is done according to the basis of independent variables or significant attributes. As decision tree is non-parametric, the requirement for examining existence of outlier or separation data linearity is not needed.

4.4 Random Forest (RF) [16]:

It refers for a crew of Decision Trees. Meaning that, the RF classifier is a crew learning mode involving set of decision trees. This classifier works as vote for a specific class by each tree to classify a new object. The class that have the greatest votes number will deciding the label for classification.

4.5 Logistic Regression (LR) [17]:

It is binary classification techniques that is utilized in estimate the discrete values based on group of independent variables. In most comparative terms, logistic regressions produce the event probability through fitting them into logistic functions that assists in the prediction process. These functions are mostly utilized as sigmoid.

4.6 AdaBoost [18]:

AdaBoost is an algorithm of metamachine learning that is refers as Adaptive Boosting. Its utilized to arise the classifier performance by using weakly classifiers in order to merge them into a strong classifier. The boosted classifier output relies on the weighted total of all weakly classifiers output. Although this technique is performing more accurate prediction, it occupies more time to build the adaptive boosting model.

4.7 Artificial Neural Network (ANN) [19]:

They are techniques for statistical model of nonlinear data with a complex relation among outputs and inputs. They learn from observing datasets that will work on. they are seeming as tool for approximate the random functions that assist in estimate the efficient method in achieving solution. One such network is convolutional neural network (CNN) that will be described in the next section.

4.8 k-Nearest Neighbor (k-NN) [20]:

It is one of the simplest machine learning algorithms. The KNN algorithm used for predictive problems in both regression and classification task. It is characterized by easy of interpretation with low calculation time. Even with this simplicity, it gives extremely competitive outcomes. This algorithm supposes that similar things similar things are near to each other where similarity, sometimes called closeness, proximity, or distance, are considered through calculate the distance among datapoints on a graph.

4.9 Convolutional Neural Network (CNN) [21]:

This network is also known as a ConvNet, it's a specific type of artificial neural network that utilizes supervised learning perceptron. This type of learning is utilized to data analysis. There are a broad range of implementation including convolutional neural network such as image processing (traditionally) and natural language processing (nowadays).

4.10 Optimum-Path Forest (OPF) [12]:

Optimum-Path Forest is a classifier algorithm that model the pattern recognition as the problem of graph partition where samples are considered as nodes in graph that connected according to the adjacency relations of them. The segmentation of graph is ruled by the process of competition between several prototypes (key nodes) aiming at grab the surviving samples that leads to cost in optimum path.

4.11 Fisher's linear discriminate analysis (FDA) [7][11]:

Linear discriminate analysis is a classification technique that develop by Fisher. It can classify the multi-dimensional data in multiple classes according to the separating line between the components. It is statistical method used to model the predictors distribution separately in every response class. After that, Bayes' theorem will be used for estimating the probability. This method can be used in statistics, machine learning and pattern recognition for finding a linear features combination that separates two or more classes of events.

4.12 Latent Dirichlet Allocation (LDA) [7] [9] [11]:

It is topic modeling technique used for discovering the topics in the collections of data that have certain probabilities. Set of similar topics constitute mixture in the space where the topic is a set of words. In the literature, some of researchers use LDA to extract the feature form data to be ready to apply by any machine learning algorithms.

4.13 Non-negative Matrix Factorization (NMF) [9]:

It is a text mining technique where their algorithm has been employed in the process of features extraction. It has a predictive power that make it useful when there are many ambiguous attributes with e weak predictability. This algorithm can introduce significative patterns, themes or topics.

5 Features Extraction Process

Successful methods of machine learning rely primarily on selecting the convenient set of features for the issue involved. The feature selection must be heavily related to type of message to arise the spam detection accuracy [10]. It is also necessary to delete the noisy features and choose the best messages features to classify them. Moreover, selecting features carefully also facilitates calculation, avoiding over-fitting and increasing accuracy [11]. Some of researchers focused on engineering feature to produce the best messages features which would be assisted in message representation and classification. They used specific methods from text mining field such as Non-negative Matrix Factorization and Latent Dirichlet Allocation (LDA) that are described in the previous section. In this section, we display the different messages features suggested in various reviewed papers. Part of these features may also perform as rules of classification and qualified by users that leads to personalization in filtering process. From the literature, we can summarize the proposed features set that have been utilized for filtering spam in SMS and

improved the classification algorithms performance on SMS spam data. In Table 1, we introduce these feature sets.

Table 1. Most Popular Features Extracted in The Reviewed Papers.

Feature name	description
Spam Keywords	Generally, spammers attract users by using some suspicious keywords in spam messages like delivery, Prize, claim, Please, Congrats, cash, visit, video, mins, service, awards, accident, free, send, etc.
Special symbols	Spammers tend to utilize special symbols. Like • "$" is utilized to refers 'money', 'dollar' in spam SMS. • "!" is utilized to attract the user attention. like CONGRATULATIONS! WINNER! • Emotion and dots usually used by people in chatting and refers for legitimate messages. Such as (: , :(etc. • Mathematical symbol like + utilized as free services messages.
URLs	Spammer tend to ask users to visit some URLs in order to steal their private information.
lowercased and uppercased words	Lowercased and uppercased words in messages that utilized to seek attention of user. Like: FREE, PRIZE, ATTENTION, RINGTONE, WON, etc.
Mobile Number	Spam messages are usually containing mobile number.
Message Length	Spam messages tend to be longer in size than the legitimate messages.

6 SMS Spam Dataset

Accessibility to the required data set is one of the challenges researchers often face in conducting a successful search for filtering or classifying SMS messages. Unlike spam in email that has a huge diversity of datasets, filtering of mobile spam has very few datasets. Lacking in the presence of public, available, real databases leads to compromises in developing various methods. Choosing a SMS spam dataset is a critical stage in measuring the performance of SMS filtering techniques methods as it is will work on it. Different repositories have been utilized by researchers for constructing a comprehensive dataset. Most researchers tend to use two or more sets of data in order to analyze the proposed methods. In this review, we have introduced the credible research datasets utilized by authors to experiment the algorithms. These SMS spam datasets are: SMS Spam Collection V.1, Spam SMS Dataset 2011-12, UCI SMS Spam Dataset, British English SMS Corpora (BEC), Dublin Institute of Technology (DIT), Dahan Tricom SMS corpus. In details, the description of these datasets is presented in Table 2. SMS Spam Collection V.1 developed by Tiago is the most widely used by researchers. It is consisting of four different datasets as follow:

- National University of Singapore (NUS): It is a set of 3375 non spam SMS messages
- Grumbletext: It includes 425 spam SMS.
- Caroline Tag's PhD: It is a collection of 450 SMS ham messages

- SMS Spam Corpus v.0.1 Big: It includes of 1,002 ham and 322 spam messages.

Table 1. Most Popular SMS Dataset.

Datasets	Total no. of SMS	Ham Messages	Spam Messages	Used references
SMS Spam Collection V.1	5574	4827	747	[3][12][10][11][9][5][7]
Spam SMS Dataset 2011-12	2000	1000	1000	[3]
UCI SMS Spam Dataset	5572	4825	747	[8]
British English SMS Corpora (BEC)	875	450	425	[8]
Dublin Institute of Technology (DIT)	1353	-	1353	[8][11]
Dahan Tricom SMS corpus	20000	8000	12000	[3]
SMS Spam Corpus v.0.1 Big	1324	1002	322	[3][7][5][12][10][4][9][11]
SMS Spam Corpus v.0.1 Small	1084	1002	82	[4]

7 Performance Evaluation

In this section, the most significant performance indicators that evaluate the algorithms' strength in filtering spam were reviewed. There are different criterions of performance measurement such as Accuracy, F1 score, Recall, Precision, Cumulative Accuracy Profile (CAP) Curve and Receiver Operating Characteristics (ROC) Curve used by authors in reviewed researches. These are the standard metrics to evaluate the effectiveness of any spam detection techniques. It is essential to select the right metrics of performance to gain the required information for systems validation or comparison. Most of researchers compare and analyze the spam filtering ability in the different algorithms according to their result of performance metrics. The terminologies of these performance metrics are explained in Table 3. To understand these metrics, we should define four related terms as follow:

- True positive (TP): The spam messages rate that were accurately categorized as spam messages by the used classifier
- False positive (FP): The ham messages rate that were incorrectly classified by the used classifier as spam messages
- True negative (TN): The ham messages rate that were accurately classified by the used classifier as ham messages.
- False negative (FN): The spam messages rate that were wrongly categorized by the used classifier as ham messages.

Table 3. Units for Magnetic Properties.

Evaluation metrics	Mathematical equation	definition
Accuracy	$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$	It identifies the all messages proportion that have been classified correctly.
Recall	$Recal = \frac{TP}{TP + FN}$	It identifies the legitimate messages proportion that have been correctly classified,
Precision	$Precision = \frac{TP}{TP + FP}$	It identifies the all correctly classified messages proportion that are actually legitimate.
F1 score	$F1\ score = \frac{2 * precision * Recall}{precision + Recall}$	It is referring to the harmonic mean of Recall and Precision
AUC-CAP	$Accuracy\ ratio\ by\ CAP\ curve = (area\ under\ model's\ CAP\ curve) / (area\ under\ model\hat{}'sCAP\ curve)$	It is utilized to assist and compare machine learning algorithms that shows the positive outcomes cumulative number on the y-axis and the corresponding classifying parameters cumulative number on the x-axis [8].
AUC-ROC	$Accuracy\ ratio\ by\ ROC\ curve = 2 *\ area\ under\ ROC\ curve - 0.5$	It is used to explore the tradeoffs between various classifiers on a costs range. the large area under the curve represent the best performance [8].

8 Discussion

Nowadays, automating the process of detecting spam in SMS is still a challenge task. There are three basic issues hindering the algorithms advancement in this research domain: the lack of real and public datasets, the text is full of abbreviations and idioms, decrease the number of features extracted from the message. To fill some of these gaps, we presented the commonly used data sets and some of the practical and effective methods used by the researchers. We found that 'SMS Spam Collection V.1' are the most commonly dataset used among researches as it is used by [1][6][7][10][9][5][4] in their work followed by Dublin Institute of Technology (DIT) SMS dataset that used by [2][10]. From the survey presented, we observe that most of researchers filtering spam in short text messages by using techniques from two major fields: machine learning and topic modelling. Topic modelling usually used to enhance the process of feature extraction of dataset that assist in increasing the performance of used algorithm. The most algorithms used in the reviewed research: Decision Tree (DT), Support Vector Machine (SVM), Logistic Regression (LR), Naive Bayes (NB), Random Forest (RF), AdaBoost, Artificial Neural Network (ANN), k-Nearest Neighbor (k-NN), Optimum-Path Forest (OPF), Fisher's linear discriminate analysis (FDA), Latent

Dirichlet Allocation (LDA), Convolutional Neural Network (CNN) and Non-negative Matrix Factorization (NMF). From the literature, the most widely accepted technique and the prominent ones is Bayesian filters that applied by [3][4][5][8][9]. However, the second most prominent technique used by researchers was Support Vector Machine as its applied by [3][7][8][9]. In this context, convolutional neural network showed great achievement in detecting spam in SMS compared by the traditional algorithms. As well, it also attains in textual data the highest accuracy. CNN's accomplishments have opened up the broad research aspect of its implementation in classifying the texts. On another hand, artificial neural networks, AdaBoost and Optimum-Path Forest have not been broadly utilized for SMS classification. In this review, the performance achieved by machine learning algorithms was compared, and we found that Naive Bayes and SVM produce effective performance. In most of researches, the measurements of algorithms performance are done by calculating the Accuracy, F1 score, Recall and Precision. Accuracy is the famous standard in evaluating the performance of the classifier algorithms. There is one research that add Cumulative Accuracy Profile (CAP) Curve and Receiver Operating Characteristics (ROC) Curve in measuring the classifier performance. In summary, there is a continual discussion on SMS spam filtering where the researchers have come up with technical measures that concrete for tackling this issue. The majority of discovered practices and measures can be utilized for dealing with SMS spam.

9 Conclusion

Short Message Service (SMS) is the most common and cheapest way of communication for mobile's users. Some company or Spammer used this service for marketing that caused in sending unwanted spam message that disturb mobile's users. To avoid this problem, researchers have proposed techniques for filtering spam SMS. In this paper, we have reviewed the emerging technologies used by researchers in detect SMS spam. Machine learning and topic modelling were the most widely techniques used by researchers. Topic modelling usually used to enhance the process of feature extraction of dataset that assist in increasing the performance of used machine learning algorithm. The success of machine learning techniques in filtering SMS spam depends primarily on selecting a suitable SMS dataset and also extracting a set of features for the problem involved. In this work, we present various SMS datasets and different features of SMS spam messages that have proposed in various reviewed papers. The availability of SMS datasets to be applied in train and test techniques in order to detect SMS spam are small sized and still limited. The most commonly dataset used among researches was 'SMS Spam Collection V.1'. Moreover, the availability of features number needed to detect spam messages in text are less, this is due to the text messages length is short. Also, our survey provides comparison and analysis of the different techniques on different datasets and their performance according to their accuracies, precision and recall. This review discover that the majority of papers are based on the Bayesian network and support vector machine to construct SMS spam classifiers and they also achieved the highest accuracy.

REFERENCES

[1]. S. J. Delany, M. Buckley, and D. Greene, "SMS spam filtering: Methods and data," Expert Syst. Appl., vol. 39, no. 10, pp. 9899–9908, 2012.

[2]. S. Stolfo, A. Stavrou and C. Wright, Research in attacks, intrusions and defenses.

[3]. M. Gupta, A. Bakliwal, S. Agarwal, and P. Mehndiratta, “A Comparative Study of Spam SMS Detection Using Machine Learning Classifiers,” 2018 11th Int. Conf. Contemp. Comput. IC3 2018, pp. 1–7, 2018.

[4]. N. Choudhary and A. Jain, "Towards Filtering of SMS Spam Messages Using Machine Learning Based Technique", Communications in Computer and Information Science, pp. 18-30, 2017. Available: 10.1007/978-981-10-5780-9_2 [Accessed 7 April 2019].

[5]. P. Sethi, V. Bhandari, and B. Kohli, “SMS spam detection and comparison of various machine learning algorithms,” 2017 Int. Conf. Comput. Commun. Technol. Smart Nation, IC3TSN 2017, vol. 2017–Octob, pp. 28–31, 2018.

[6]. W. Li and S. Zeng, “A Vector Space Model based spam SMS filter,” ICCSE 2016 - 11th Int. Conf. Comput. Sci. Educ., no. Iccse, pp. 553–557, 2016.

[7]. M. Popovac, M. Karanovic, S. Sladojevic, M. Arsenovic, and A. Anderla, “Convolutional Neural Network Based SMS Spam Detection,” 2018 26th Telecommun. Forum, TELFOR 2018 - Proc., pp. 1–4, 2019.

[8]. N. Sulaiman and M. Jali, "A New SMS Spam Detection Method Using Both Content-Based and Non Content-Based Features", Lecture Notes in Electrical Engineering, pp. 505-514, 2015.

[9]. N. K. Nagwani, “A Bi-Level Text Classification Approach for SMS Spam Filtering and Identifying Priority Messages,” Int. Arab J. Inf. Technol., vol. 14, no. 4, pp. 473–480, 2017.

[10]. N. Al Moubayed, T. Breckon, P. Matthews and S. McGough, "SMS Spam Filtering Using Probabilistic Topic Modelling and Stacked Denoising Autoencoder", Lecture Notes in Computer Science, 2016.

[11]. J. Ma, Y. Zhang, J. Liu, K. Yu, and X. Wang, “Intelligent SMS spam filtering using topic model,” Proc. - 2016 Int. Conf. Intell. Netw. Collab. Syst. IEEE INCoS 2016, pp. 380–383, 2016.

[12]. D. Fernandes, K. A. P. Da Costa, T. A. Almeida, and J. P. Papa, “SMS spam filtering through optimum-path forest-based classifiers,” Proc. - 2015 IEEE 14th Int. Conf. Mach. Learn. Appl. ICMLA 2015, pp. 133–137, 2016.

[13]. M. Horný, “Bayesian Networks,” Boston University, scool of public health, 5, 2017.

[14]. R. Gandhi, “Support Vector Machine — Introduction to Machine Learning Algorithms,” Towards Data Science, 07-Jun-2018. [Online]. Available: https://towardsdatascience.com/support-vector-machine-introduction-to-machine-learning-algorithms-934a444fca47. [Accessed: 13-Mar-2019].

[15]. "Introduction to Decision Tree Learning – Heartbeat." [Online]. Available: https://heartbeat.fritz.ai/introduction-to-decision-tree-learning-cd604f85e236. [Accessed: 13-Mar-2019].

[16]. R. Zafarani, M. A. Abbasi, and H. Liu, Social Media Mining: An Introduction. Cambridge: Cambridge University Press, 2014.

[17]. A. C. Rencher and G. B. Schaalje, Linear models in statistics, 2nd ed. Hoboken, N.J: Wiley-Interscience, 2008.

[18]. R. F. de Mello and M. A. Ponti, Machine Learning - A Practical Approach on the Statistical Learning Theory. 2018.

[19]. P. Kim, MATLAB deep learning: With Machine Learning, Neural Networks and Artificial Intelligence. 2017.

[20]. "k-nearest neighbors algorithm," Wikipedia, 17-Feb-2019. [Online]. Available: https://en.wikipedia.org/w/index.php?title=K-nearest_neighbors_algorithm&oldid=883754172. [Accessed: 13-Mar-2019].

[21]. Jürgen Schmidhuber. Deep learning in neural networks: An overview. Neural networks, 61:85–117, 2015.