International Journal of Electrical and Computer Engineering (IJECE)
Vol. 11, No. 1, February 2021, pp. 596~601
ISSN: 2088-8708, DOI: 10.11591/ijece.v11i1.pp596-601

Differential evolution detection models for SMS spam

Sarab M. Hameed
Department of Computer Science, College of Science, University of Baghdad, Iraq

Article Info

Article history:

Received Nov 23, 2019
Revised Jun 17, 2020
Accepted Jun 27, 2020

Keywords:

Differential evolution
Feature extraction
Machine learning
SMS spam classification
SMS spam detection

ABSTRACT

With the growth of mobile phones, short message service (SMS) became an essential text communication service. However, the low cost and ease use of SMS led to an increase in SMS Spam. In this paper, the characteristics of SMS spam has studied and a set of features has introduced to get rid of SMS spam. In addition, the problem of SMS spam detection was addressed as a clustering analysis that requires a metaheuristic algorithm to find the clustering structures. Three differential evolution variants viz DE/rand/1, jDE/rand/1, jDE/best/1, are adopted for solving the SMS spam problem. Experimental results illustrate that the jDE/best/1 produces best results over other variants in terms of accuracy, false-positive rate and false-negative rate. Moreover, it surpasses the baseline methods.

Corresponding Author:

Sarab M. Hameed,
Department of Computer Science, College of Science,
University of Baghdad,
Baghdad, Iraq.
Email: sarab.m@sc.uobaghdad.edu.iq

1. INTRODUCTION

The usage of short messaging service (SMS) became increasing rapidly as a result of its cheap cost and ease of use. This directed to an increase in the amount of spam, which is unsolicited and undesired SMS sent to a large number of receivers. The precise definition of spam does not exist. Essentially, spam regards as an undesirable email, however, it is not all undesirable e-mails are spam.

SMS spam has a significant influence on users because users view each SMS they get, so SMS spam affects the users immediately [1, 2]. In addition, to disturbing, users require a degree of secrecy with their mobile phones and unaffected by spam and viruses intrusions [3-5]. Therefore, considerable attention to the SMS spam problem is provided to develop a set of approaches to bypass this problem. Among the approaches developed to combat the SMS spam is a classification of messages into SMS spam and ham. The challenge is that the messages are short and contains few words and these words may be abbreviated [6, 7].

Detecting SMS spam turns to be of significant worth due to the huge loss that could result from the SMS spam. Two types of methods that are collaborative based and content-based methods can be used to detect SMS spam. Collaborative based depends on usage and user experience. While the content-based method concentrates on examining the textual content of messages [8, 9]. Zainal and Jali performed a study of the distinguishing control of the features and examining it's informational or impact circumstance in SMS spam messages classification [10]. Kaya and Ertuğrul introduced a method based on local ternary patterns to extract two distinct features set low and up features from SMS messages and several machine learning methods were applied for classifying SMS spam. The evaluation results over three separate SMS datasets gained accuracy 93.318%, 87.15%, and 94.10% [11].

Sulaiman and Jali introduced a method for detection SMS spam based on well-known characters used at transmitting SMS, SMS length and keywords. Five different algorithms and three different datasets were used to verify the proposed method. The results indicated that the proposed method could produce a reasonable detection rate [12].

Choudhary and Jain presented an approach for detecting spam messages using ten features and five machine learning algorithms viz naïve Bayes, logistic regression, J48, decision table and random forest. SMS Spam Corpus was used as an evaluation dataset and the results showed that the random forest is the best one with detection rate equals 96.1% [13].

Abdulhamid *et al*. presented a review of the possible ways and challenges of spam detection and future research direction that can help specialist researchers to know the areas that need further improvement [1]. Kaliyar *et al*. proposed a general model to distinguish SMS spam messages based on several machine learning algorithms. The proposed SMS spam filtering model was able to filter messages from several families: Singapore, American, and Indian English. The results showed the proposed model achieved a high precision using Indian English SMS [14].

Sharaff presented a comparative study of the effect of feature selection techniques on several classifiers. The results showed that the feature selection technique impacts the performance of the classifier and can assist in enhancing the performance of some classifiers [15]. Ojugo and Eboka developed SMS spam detection method based on Bayesian Network. A set of features is deterministically selected from SMS using the genetic algorithm (GA). The results showed that the feature selection technique impacts the performance of the classifier [16].

A two-fold contribution is coupled in this paper. First, we raise the following question: How to design an efficient feature extraction model to improve the accuracy. Second, to ensure more efficacious performance, we exploit multiple variants of differential evolution (DE) models that offer positive cooperation with a set of features for SMS spam to correctly divide the search space into two and non-overlapping classes SMS spam and ham.

The rest of this paper is organized as follows. Section 2 elaborates on an approach for detecting SMS spam by suggesting of a feature set. In Section 3, the results and discussion of the proposed approach are reported. Finally, the concluding remarks and future work for other research directions are provided in section 4**.**

2. RESEARCH METHOD

This section clarifies the methodology used for SMS spam detection which consists of two stages. The first stage attempts to extract from SMS specific features that may be used to characterize SMS spam. Based on the extracted features, three differential evolution alogirthms are used in the second stage to detect SMS spam. Consider an SMS collection $\mathbb{S}$ of N text messages, i.e. $\mathbb{S} = \{s_1, \dots, s_N\}$. Each message, s_i, $1 \leq i \leq N$ consists of words, numbers, etc. and its size is limited to 160 characters. Figure 1 demonstrates some samples of SMS spam and ham in [17].

ham	Today am going to college so am not able to atten the class.
ham	I'm in class. Will holla later
ham	Easy ah?sen got selected means its good..
ham	Mmm thats better now i got a roast down me! iĺ'd b better if i had a few drinks down me 2! Good indian?
spam	We know someone who you know that fancies you. Call 09058097218 to find out who. POBox 6 LS15HB 150p
ham	Come round it's .
ham	Do 1 thing! Change that sentence into: "Because i want 2 concentrate in my educational career im leaving here.."
spam	1000's flirting NOW! Txt GIRL or BLOKE & ur NAME & AGE eg GIRL ZOE 18 to 8007 to join and get chatting!
ham	I walked an hour 2 c u! doesnĺ't that show I care y wont u believe im serious?
spam	18 days to Euro2004 kickoff! U will be kept informed of all the latest news and results daily. Unsubscribe send GET EURO STOP to 83222.

Figure 1. Sample of SMS spam and ham from SMS spam collection

The idea proposed here for dealing with the SMS spam problem is based on variant DE algorithms. Up to the best of our knowledge, this is the first time to use DE algorithms as clustering for SMS spam. The SMS spam detection task is to identify whether s_i is SMS spam or ham using clustering is $\mathbb{C}: s_i \rightarrow \{SMS\ spam, ham\}$. Detecting distinctive features that have high discriminatory power to distinguish between SMS spam and ham to be crucial in SMS spam detection. To support the clustering a set of n features $F = \{f_1, f_2, \dots, f_n\}$ should be extracted from $\mathbb{S}$.

This research investigates the challenge of SMS spam detection that is how the distinctive features F are identified to classify the spam SMS messages. In this, the features of the ham and SMS spam messages are extracted to form features set representing a sign for the corresponding message. These features are used to train DE for identifying the centroids of the SMS spam and ham. Then, the trained centroids are given to the testing stage to detect SMS spam or ham.

The first stage of the proposed SMS spam detection model is preproccessing. After retrieving the SMS message from a data source, text preprocessing that is very important is applied to make the messages to be analyzed. Several steps are involved in preprocessing in order to prepare the message to an SMS spam detection. Firstly, the message is converted to lowercase to evade differentiation between the same words that are different in case. Secondly, the punctuation is removed. After that, the messages are tokenized based on delimited whites-pace to identify the tokens. Then, stop words are excluded from the set of tokens recognized in the former step to obtain a message as a list of keywords. Finally, the tokens are stemmed to recognize their roots.

Once applying preprocessing to the collection of messages**,** the message representation stage should be performed to represent the message by distinct terms. Each term then is involved a weight calculated using term-frequency inverse-sentence-frequency. Afterword, each message is represented as a vector of weights of terms. In addition, some features are extracted from the raw data to further improve the message representation as explained in what follows:

- The length of the message is considered one feature to be added to represent the message since SMS spams length tends to be longer than ham.
- The presence of a number is considered as one feature to be added to represent the message since the spammer prefers using the phone number to claim a lottery or prize.

The extracted feature set can be used by the DE to define the centroid of each cluster. The proposed DE SMS spam detection consists of two stages: training and testing stages. The goal of the training stage is to tune the value of two centroid vectors according to a set $F = \{f_1, f_2, \dots, f_n\}$ of training messages. While the goal of the testing stage is to classify the incoming message into SMS spam or ham based on the two centroid vectors produced from the training stage. The following subsections illustrate how DE is utilized for the clustering purpose based on the extracted features.

2.1. DE based clustering for SMS spam detection

After extracting the message features set, an optimization model based on DE that uses these features to identify the centroids for clustering of SMS spam and ham is proposed. Three differential evolution variants namely DE/rand/1, jDE/rand/1, jDE/best/1 are utilized. The detailed explanation of the main characteristic components of the proposed models is provided in what follows.

2.2.1. Individual representation and population initialization

In the proposed models, cluster centroids are encoded in the individual. Each individual I is represented as a vector of n genes that corresponds to the 2 cluster centroids. The mathematical formulation of the individual is as follows:

$$I = \{i_1, i_2, \dots, i_n\},$$

$$\forall j \in \{1, \dots, n\}, i_j \in [min_j, max_j]$$

min_j : is the minimum value feature j can get, and
max_j: is the maximum value feature j can get.

DE is a population-based optimization algorithm and starts with a population $\mathbb{P}$ of N solutions. Formally speaking, $\mathbb{P}$ can be formulated as follows:

$$\mathbb{P} = \{I_1, I_2, \dots, I_N\}$$

where N is the population size.

2.2.2. Mutation and crossover operations

This operation is considered as the main operation that is responsible for maintaining the population diversity in evolution. The mutation equations for DE/rand/1, jDE/rand/1 and jDE/best/1 are in (1), (2), and (3) respectively [18-20].

DE/rand/1 $V_i = I_{r1} + F(I_{r2} - I_{r3})$ (1)

jDE/rand/1 $V_i = I_{r1} + F_i(I_{r2} - I_{r3})$ (2)

jDE/best/1 $V_i = I_{best} + F_i(I_{r1} - I_{r2})$ (3)

where r_1, r_2 and r_3 are random numbers in [1,N] and they are mutually different, $best$ is the individual in the current population. F is a random number in (0,1) and

$$F_i = F_l + F_u \times rand \qquad if\ r < T_1$$

F_l is lower bound of mutation.
F_u is upper bound of mutation.
T_1 is the probability to alter F factor.

The crossover operation aim is to combine the target I vector with the donor vector V to produce the trial vector U. Equation (4) [21] illustrates the crossover operation for DE/rand/1 and (5) [22] demonstrates the crossover operation for jDE/rand/1 and jDE/best/1.

$$U_{i,j} = \begin{cases} V_{i,j}\ if\ r_1 \le CR\ or\ j = I_{i,r_2} \\ I_{i,j}\ if\ r_1 > CR\ and\ j \ne I_{i,r_2} \end{cases} \quad (4)$$

$$U_{i,j} = \begin{cases} V_{i,j}\ if\ r_1 \le CR_i\ or\ j = I_{i,r_2} \\ I_{i,j}\ if\ r_1 > CR_i\ and\ j \ne I_{i,r_2} \end{cases} \quad (5)$$

where
CR is a random number in (0,1] that determines the value of the trial vector U which is inherited from the donor V.
r_1 is a random numbers in (0,1]
r_2 is a random numbers in [1,n]
and

$$CR_i = rand \qquad if\ r < T_2$$

T_2 is the probability to alter *CR* factor.

2.2.3. Evaluation DE selection operation

According to the SMS spam problem, the formulation of the objective function requires maximizing the accuracy that means the number of messages that are correctly detected as SMS spam (TP) and the number of messages are correctly classified as ham(TN) should be maximized. In other words the number of messages that are misclassified as SMS spam (FP) and the number of messages are misclassified as ham (FN) should be minimized. Each individual is evaluated using the objective function as in (6). The computation of the objective function for each individual is as follows. First, the centroids, $\mathbb{C} = \{SMS\ spam, ham\}$ encoded in the individual are extracted and the clusters are formed. Then, the cluster is attained by assigning the messages s_i to a cluster corresponding to the closest centroid. Euclidean squared distance metric is adopted for the computation of the distance between a message and the centroid.

$$Maximize\ \ ObjFun(I) = \frac{TP+TN}{TP+TN+FN+FP} \quad (6)$$

After evaluation the individuals, DE selection operation is applied as shown in (7), the resultant vector from this operation is the vector with the higher objective function that will be passed to the next generation.

$$I_i = \begin{cases} U_i\ \ if\ ObjFun(U_i) > \ ObjFun(I_i) \\ I_i \qquad\qquad\qquad\qquad otherwise \end{cases} \quad (7)$$

3. EXPERIMENTAL RESULTS AND DISCUSSION

SMS Spam Collection [17c] is a public dataset collected for SMS spam research that contains 5,574 English, real and non-encoded messages. Each message is labeled to indicate whether a given message is a legitimate (ham) or SMS spam. It contains about 86.67% of ham and 13.33% of SMS spam. Evaluation metrics represented by accuracy(Acc) [23], false negative rate (FNR) [24] and false positive rate (FPR) [25] are used for assessing the proposed SMS spam. Evaluation of the proposed SMS spam detection model is performed by applying the k-fold cross-validation approach. In this paper, 3- fold cross-validation approach and 2-fold cross-validation are adopted to show the impact of training and testing dataset on the performance of the proposed model. The evaluation is presented in terms of average accuracy(Acc), false negative rate (FNR) and false positive rate (FPR) over k-fold. Table 1 reports the setting parameters of DE models. Tables 2 and 3 present the results of the proposed approach under 3-fold and 2-fold for various classification. From those two tables, which present the average performance of the three variant DE algorithms DE/rand/1, jDE/rand/1, jDE/best/1 against k-means baseline method in terms of Acc, FNR and FNR over ten different runs, it is clear that the three variant DE models have successfully clustered the messages into SMS spam and ham for the different k-fold approaches against k-means through reducing FNR and FPR and increasing the accuracy. Also, it can be observed that the jDE/best/1 produces the best result over other variant DE models.

Table 1. DE parameters setting

Parameter	Value
Population size, N	100
Maximum number of generations	100
Crossover probability, CR	0.9
Mutation probability, F	0.5
Lower bound of mutation, F	0.1
Upper bound of mutation, F	0.9
probability to alter F, T_1	0.1
probability to alter CR, T_2	0.1

Table 2. Comparative results obtained over 10 independent runs fort he proposed model against K-means regarding 3-fold

Model	*Acc*	*FNR*	*FPR*
DE/rand/1	0.9641	0.0116	0.1925
jDE/rand/1	0.9660	0.0122	0.1742
jDE/best/1	0.9667	0.0116	0.1738
k-means	0.8600	0.0682	0.6024

Table 3. Comparative results obtained over 10 independent runs for the proposed model against K-means regarding 2-fold

Model	*Acc*	*FNR*	*FPR*
DE/rand/1	0.9648	0.0128	0.1801
jDE/rand/1	0.9652	0.0120	0.1814
jDE/best/1	0.9671	0.0107	0.1756
k-means	0.8290	0.0991	0.6350

4. CONCLUSION

In this paper, the problem of SMS spam detection was addressed as a clustering analysis. Finding the clustering structures that provide high discrimination between SMS spam and ham has been considered as NP-hard which needs a metaheuristic algorithm. Three DE variants were utilized to distinguish incoming messages into SMS spam and ham. Experimental results reveal that the DE/best/1 surpasses other variants and k-means in terms of accuracy, false-negative rate, and false-positive rate. Future work should include an investigation to consider multi-objective evolutionary algorithms that may produce better results.

REFERENCES

[1] S. M. Abdulhamid, et al., "A Review on Mobile SMS Spam Filtering Techniques," in *IEEE Access*, vol. 5, pp. 15650-15666, 2017.
[2] G. Rawashdeh, et al., "Comparative Between Optimization Feature Selection by Using Classifiers Algorithms on Spam Email," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 6, pp. 5479-5485, 2019.
[3] N. Desai and M. Narvekar, "Normalization of Noisy Text Data," *Procedia Computer Science*, vol. 45, pp. 127-132, 2015.
[4] N. Jiang, et al., "Understanding SMS Spam in Large Cellular Network: Characteristics, Strategies and Defenses," *International Workshop on Recent Advances in Intrusion Detection*, pp. 328-347, 2013.
[5] H. Sajedi, et al., "SMS Spam Filtering Using Machine Learning Techniques: A Survey," *Machine Learning Research*, vol. 1, no. 1, pp. 1-14, 2016.

[6] T. M. Mahmoud and A. M. Mahfouz, "SMS Spam Filtering Technique Based on Artificial Immune System," *International Journal of Computer Science Issues*, vol. 9, no. 2, pp. 589-597, 2012.
[7] N. Sjarif, et al., "SMS Spam Message Detection Using Term Frequency-Inverse Document Frequency and Random Forest Algorithm," *Procedia Computer Science*, vol. 161, pp. 509-515, 2019.
[8] X. Qian, "SMS Spam Detection Using Noncontent Features," *IEEE Intelligent Systems*, vol. 27, no. 6, pp. 44-51, 2012.
[9] A. Karami and L. Zhou, "Improving Static SMS Spam Detection by Using New Content-based Features," *The 20th Americas Conference on Information Systems (AMCIS)*, 2014.
[10] K. Zainal and M. Z. Jali, "A Review of Feature Extraction Optimization in SMS Spam Messages Classification," in Berry M., et al. (eds), "Soft Computing in Data Science (SCDS)," *Communications in Computer and Information Science*, vol. 652, pp. 158-170, 2016.
[11] Y. Kaya and O. F. Ertuğrul, "A Novel Feature Extraction Approach in SMS Spam filtering for Mobile Communication: One-Dimensional Ternary Patterns," *Security and communication networks*, 2016.
[12] N. F. Sulaiman and M. Z. Jali, "A New SMS Spam Detection Method Using both Content-Based and Non Content-Based Features," *Advanced Computer and Communication Engineering Technology*, pp. 505-514, 2016.
[13] N. Choudhary and A. K. Jain, "Towards Filtering of SMS Spam Messages Using Machine Learning Based Technique," in Singh D., et al., (eds), "Advanced Informatics for Computing Research," *Communications in Computer and Information Science*, vol. 712, pp. 18-30, 2017.
[14] R. K. Kaliyar, et al., "SMS Spam Filtering on Multiple Background Datasets Using Machine Learning Techniques: A Novel Approach," *2018 IEEE 8th International Advance Computing Conference (IACC)*, pp. 59-65, 2018.
[15] A. Sharaff, "Spam Detection in SMS Based on Feature Selection Techniques," in Abraham A., et al., (eds), "Emerging Technologies in Data Mining and Information Security," *Advances in Intelligent Systems and Computing*, vol. 813, pp. 555-563, 2019.
[16] A. A. Ojugo and A. O. Eboka, "Memetic Algorithm for Short Messaging Service Spam Filter Using Text Normalization and Semantic Approach," *International Journal of Informatics and Communication Technology (IJ-ICT)*, vol. 9, no.1, pp. 9-18, 2020.
[17] T. A. Almeida, et al., "Contributions to the Study of SMS Spam filtering: New Collection and Results," in *Proceedings of the 2011 ACM Symposium on Document Engineering (DOCENG'11)*, pp. 259-262, 2011.
[18] M. Georgioudakis, et al., "On the Performance of Differential Evolution Variants in Constrained Structural Optimization," *Procedia Manufacturing*, vol. 44, pp. 371-378, 2020.
[19] T. Eltaeib and A. Mahmood, "Differential Evolution: A Survey and Analysis," *Applied Sciences*, vol. 7, p. 1945, 2018.
[20] M. Georgioudakisa and V. Plevris, "On the Performance of Differential Evolution Variants in Constrained Structural Optimization," *Procedia Manufacturing*, vol. 44, pp. 371-378, 2020.
[21] S. Das and P. N. Suganthan, "Differential Evolution: A Survey of the State-of-the-Art," *IEEE Transactions on Evolutionary Computation*, vol. 15, pp. 4-31, 2011.
[22] J. Brest, et al., "Dynamic optimization using Self-Adaptive Differential Evolution," *2009 IEEE Congress on Evolutionary Computation*, Trondheim, pp. 415-422, 2009.
[23] K. S. Reddy and E. S. Reddy, "Integrated Approach to Detect Spam in Social Media Networks Using Hybrid Features," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 1, pp. 562-569, 2019.
[24] A. Boukhalfa, et al., "LSTM Deep Learning Method for Network Intrusion Detection System," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 3, pp. 3315-3322, 2020.
[25] S. Sheikhi, et al., "An Effective Model for SMS Spam Detection Using Content-based Features and Averaged Neural Network," *International Journal of Engineering, Transactions B: Applications*, vol. 33, no. 2, pp. 221-228, 2020.

BIOGRAPHY OF AUTHOR

Sarab M. Hameed received B.Sc. degree in computer science from university of Baghdad, in 1992, M. Sc. from university of Baghdad, in 1999 and Ph. D. from university of technology in 2005. She is currently assitant professor at department of computer science, university of Baghdad. Her research interest includes computer and data security and soft computing in the security field.