Applied Soft Computing 22 (2014) 11–27

Contents lists available at ScienceDirect

Applied Soft Computing

journal homepage: www.elsevier.com/locate/asoc

Improved email spam detection model with negative selection algorithm and particle swarm optimization

Ismaila Idris*, Ali Selamat[1]

UTM-IRDA Digital Media COE, Office of Research Alliance & Faculty of Computing, Universiti Teknologi Malaysia,
81310 UTM Johor Bahru, Johor, Malaysia

ARTICLE INFO

Article history:
Received 13 May 2013
Received in revised form 17 February 2014
Accepted 2 May 2014
Available online 14 May 2014

Keywords:
Negative selection algorithm
Particle swarm optimization
Email
Spam
Non-spam
Detector generation

ABSTRACT

The adaptive nature of unsolicited email by the use of huge mailing tools prompts the need for spam detection. Implementation of different spam detection methods based on machine learning techniques was proposed to solve the problem of numerous email spam ravaging the system. Previous algorithm used in email spam detection compares each email message with spam and non-spam data before generating detectors while our proposed system inspired by the artificial immune system model with the adaptive nature of negative selection algorithm uses special features to generate detectors to cover the spam space. To cope with the trend of email spam, a novel model that improves the random generation of a detector in negative selection algorithm (NSA) with the use of stochastic distribution to model the data point using particle swarm optimization (PSO) was implemented. Local outlier factor is introduced as the fitness function to determine the local best (Pbest) of the candidate detector that gives the optimum solution. Distance measure is employed to enhance the distinctiveness between the non-spam and spam candidate detector. The detector generation process was terminated when the expected spam coverage is reached. The theoretical analysis and the experimental result show that the detection rate of NSA–PSO is higher than the standard negative selection algorithm. Accuracy for 2000 generated detectors with threshold value of 0.4 was compared. Negative selection algorithm is 68.86% and the proposed hybrid negative selection algorithm with particle swarm optimization is 91.22%.

1. Introduction

Email is now part of millions of people's life in the world today. It has changed the way man collaborates and works by being the most cheapest, popular and fastest means of communication [1]. Though, it recorded success in a lot of human activities, improving group communications, its impact was felt on the growth of business and also leads national development in a positive path. It is one of the technologies that has a direct impact on human life. The major short-coming of this technology is the increase in unsolicited email messages that a recipient receives. One significant and growing task that resulted from unsolicited email is the classification of email. This poses a problem among cooperate organizations and individuals trying to solve this menace called email spam. The task of email classification is shared into sub-tasks. The initial task is the collection of data and email message representation. Second task is the selection of a email feature and dimensional reduction of features [2], and the final task is the mapping of both training and testing set for classification of email. The essence of classification is to distinguish between spam and non-spam email. The problem of email spam is a global issue and is often encountered by all email users. It is defined as an unwanted junk email delivered to services on Internet mail. The amount of email spam has skyrocketed due to bulk mailing tools, this annoyed the receivers the more and the Internet service providers (ISP) are constantly under great pressure and complain on the problem of unsolicited email messages. Different techniques has been proposed in dealing with unsolicited email spam; the very first step in tackling spam is to detect spam email, this brought about the constant development of spam detection models; the models has two main approaches: the statistical and the non-statistical techniques. The statistical approach is a lot more effective than the non-statistical approach. Most of the statistical models in existence normally search for a specific keyword pattern in emails.

Quite a lot of machine learning techniques for email spam detection model have been proposed with little work on the negative

* Corresponding author. Tel.: +60 143813540.
E-mail addresses: ismi_idris@yahoo.co.uk (I. Idris), aselamat@utm.my (A. Selamat).

[1] Tel.: +60 7 5531008; fax: +60 7 5530160.

http://dx.doi.org/10.1016/j.asoc.2014.05.002
1568-4946/© 2014 Elsevier B.V. All rights reserved.

selection algorithm. Research on the negative selection algorithm mainly focuses on anomaly detection, fault detection, malware detection and intrusion detection. Most work on negative selection algorithm (NSA) and particle swarm optimization (PSO) solves the problems of anomaly detection and intrusion detection. The implementation of particle swarm optimization with negative selection algorithm to maximize the coverage of the non-self space was proposed by Wang et al. [3] to solve the problem in anomaly detection. The research of Gao et al. [4] focuses on non-overlapping detectors with fixed sizes to achieve maximal coverage of non-self space; this is initiated after the generation of detectors by negative selection algorithm. There are few researches on the construction of email spam detection model with mammalian immune system functions; though, several immune system models are applied to virus detection [5], intrusion detection [6], anomaly detection [7] and malware detection [8]. If considerable effort is not made to find a technological solution to the menace of spam, the Internet email is in danger as an important medium of communication; in same way that the virus tried to disable the revolution of personal computers. The understanding of the artificial immune system based on the mammalian immune system is very vital in this study. The main goal of the immune system is to distinguish between non-self and self-element which is the basis for our implementation with negative selection algorithm, one amongst the algorithm of artificial immune system (AIS). This research will replace self in the mammalian immune system as non-spam in our system and non-self in the mammalian immune system as spam in our system. Details of negative selection algorithm (NSA) and its implementation will be discussed in Section 3. A battle against spam is a very difficult one; therefore, it makes for all a lot of sense to fight an adaptive pathogen with an adaptive system. This brought about the study of negative selection algorithm which is an adaptive algorithm in the fight against spam. The adaptive nature of the negative selection algorithm makes it able to supersede every other algorithm for email spam detection. The algorithm is able to learn from a previous attack, which is used to protect the system against the same attack in the future. Most models make emphasis on applying and designing computational algorithm and techniques with the use of simplified models of different immunological processes [9,10]. A review of machine learning approach for email spam classification was presented by Guzella et al. [11], the work discusses most of the techniques adopted in email spam classification like naïve Bayes (NB), support vector machine (SVM), artificial neural network (ANN), logistic regression (LR), lazy learning (LL), artificial immune system (AIS), boosting ensembles and other related approach. This paper proposes an improved solution for email spam detection inspired by the artificial immune system by the adoption of spam detection generation techniques with negative selection algorithm and particle swarm optimization. The particle swarm optimization (PSO) was implemented to generate detectors for training of negative selection algorithm to cover the spam space instead of the original random generation of detector use by negative selection algorithm. The paper is organized in to six sections. Section 1 is the introduction. Section 2 discusses the related work in negative selection algorithm. The proposed improved model and its constituent framework are discussed in Section 3. Empirical studies, results and discussion are in Section 4 and Section 5 discusses the experimental results. Model implementation and its advantages are presented in Section 6. Conclusion and recommendation is in Section 7.

2. Related work

Artificial immune system (AIS) is a new mechanism implemented for the control of email spam [12], it uses pattern matching in representing detectors as regular expression in the analysis of message. A weight is assigned to the detector which was decremented or incremented when observing the expression in the spam message with the classification of the message based on the threshold sum of the weight of matching detectors. The system is meant to be corrected by either increasing or decreasing all the matching detector weights with a 1000 detector generated from spam-assassin heuristic and personal corpus. The results were acceptable on the basis of the few number of detectors used. A comparison of the two techniques to determine message classification using spam-assassin corpus with 100 detectors was also proposed by [13]. This approach is like the previous techniques but the difference is the increment of weight where there is recognition of pattern in the spam messages. Random generation of the detector does not help in solving the problem of the best-selected features; though, feature weights are updated during and after the matching process of the generated detectors. The weighting of features complicates the performance of the matching process. In conclusion, the present techniques are better than the previous due to their classification accuracy and slightly improved false positive rate. More experimentation was performed by [14] with the use of spam-assassin corpus and Bayesian combination of the detector weight. Messages were scored by the simple sum of the message that was matched by each non-spam in the detector space and also by the use of Bayes scores. Words from the dictionary and patterns extracted from a set of messages are considered in detector generation besides the commonly used filters in order to be assured of the message classification. It was finally observed that the best results emerged when the heuristic was used with similar performance of the other two techniques. The approach of scoring features or feature weighting during and after the matching process does not help in the selection of important features for spam detection due to its computational cost.

Artificial immune system (AIS) collaborative filter that seems to learn the signature of a typical pattern of spam message with the aim of sampling words randomly from a message while removing words that exist in the non-spam message was proposed by [15]. This resulted in a robust system of obfuscation with respect to random words. Signatures that are to be distributed to other agents were selected with care in other to avoid the use of unreliable features. Spam-assassin corpus was used for the implementation of the experiment with promise of good result when there are few collaborated servers. Supervised real valued antibody network (SRABNET) that evolves detector population was also proposed by Bezerra et al. [16]. The sizes of the network are adjusted dynamically based on training data with the use of total cost ratio (TCR) as the training stopping criteria. The representation of messages are a bag of words (BoW) with features in binary, with a process of taking away words that appears below 5% in excess of 95% in all messages. The experiment adopts PU1 corpus with a 10 fold cross-validation. A genetic optimized spam detection using AIS algorithm was proposed by Mohammad and Zitar [17]. The genetic algorithm optimized AIS to cull old lymphocytes (replacing the old lymphocyte with new ones) and also to check for new interest for users in a way that is similar. In updating intervals such as the number of received messages, the interval is updated with respect to time, user request and so on; many choices were used in selecting the update intervals which was the aim of using the genetic algorithm. The experiment was implemented with spam-assassin corpus with 4147 non-spam messages and 1764 spam messages. The implementation of different pattern recognition scheme inspired by the biological immune system in order to identify uncommon situations like the email spam [17–20], unfortunately, has not been able to produce outstanding result.

It is quiet desirable to determine quantitatively the coverage of certain negative selection algorithm or make a conclusion on how detectors are distributed and their coverage in the spam space. The