Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 52 (2015) 244 – 251

Procedia Computer Science

6th International Conference on Ambient Systems, Networks and Technologies, ANT 2015

Dendritic Cell Algorithm for Mobile Phone Spam Filtering

Ali A. Al-Hasan[a], El-Sayed M. El-Alfy[b,*]

[a]*Saudi Aramco, Dhahran, Saudi Arabia*

[b]*College of Computer Sciences and Engineering, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia*

Abstract

With the revolution of mobile devices and their applications, significant improvements have been witnessed over years to support new features in addition to normal phone communication including web browsing, social networking and entertainment, mobile payment, medical and personal records, e-learning, and rich connectivity to multiple networks. As mobile devices continue to evolve, the volume of hacking activities targeting them also increases drastically. Receiving short message spam is one of the common vectors for security breaches. Besides wasting resources and being annoying to end-users, it can be used for phishing attacks and as a vehicle for other malware types such as worms, backdoors, and key loggers. The next generation of mobile technologies has more emphasis on security-related issues to protect confidentiality, integrity and availability. This paper explores a number of content-based feature sets to enhance the mobile phone text messaging services in filtering unwanted messages (a.k.a. spam). Moreover, it develops a more effective spam filtering model using a combination of most relevant features and by fusing decisions of two machine learning algorithms with the Dendritic Cell Algorithm (DCA). The performance has been evaluated empirically on two SMS spam datasets. The results showed that significant improvements can be achieved in the overall accuracy, recall and precision of spam and legitimate messages due to the application of the proposed DCA-based model.

Peer-review under responsibility of the Conference Program Chairs

Keywords: Mobile Technology; Smartphones; Short Message Service (SMS); Dendritic Cell Algorithm (DCA); Spam Detection and Filtering; Application Security.

1. Introduction

Nowadays, with the advances in mobile technology, end users are accessing their emails, surfing the world-wide web, making video & voice calls, using text chatting, gaming and more through their smartphones. The number of mobile users is increasing significantly over time with almost seven billion cellular subscriptions worldwide[1]. Mobile devices are now likely to contain personal and confidential information such as credit card numbers, contact lists, emails, medical records and other sensitive documents. Unlike desktop applications, effective security controls to protect mobile devices are not mature enough and is an active area of research. This can be attributed limited resources and processing power, and lack of knowledge and awareness of many end users regarding protection mechanisms. These reasons and more are making mobiles very attractive to cyber attacks. Hackers can utilize the compromised

* Corresponding author. (On leave from Tanta University, College of Engineering, Egypt).
E-mail address: alfy@kfupm.edu,sa

Peer-review under responsibility of the Conference Program Chairs
doi:10.1016/j.procs.2015.05.067

mobiles to make calls to premium numbers without the end-users' permission, stealing contact data, or participating in botnet activities.

Exchanging short text messages (SMS) among mobile phones is very convenient and frequently used for communication on a daily basis. Subsequently, the number of unwanted SMS messages (spam) is growing. In 2012, there were 350,000 variants of SMS spam globally[2]. SMS has been considered a serious security threat since early 2000s[3]. For example, hackers can send phishing attacks to collect confidential information or launch other types of attacks. The risk of SMS spam could be operational or financial loss. It is getting easier to target end users through SMS than electronic mails (emails) since the mail service is more mature, and more effective email spam fighters have been developed and deployed by service providers and users. Unfortunately, this is not the case with the SMS spam. The controls that are used by mobile phones to block SMS spam are not as effective as email anti-spammers. It is a challenging task since SMS messages have limited sizes which means less statistically-distinguishing information. Recently, several methods have been investigated to detect SMS spam, including content-based approaches[3–7]. However, the accuracy is still relatively low and further research is required to investigate new features and new ways of calculating and utilizing them.

In this paper, we analyze several feature sets and study their impact on two machine learning algorithms. Then, we combine the top two relevant feature sets and build a more effective model. Inspired by the danger theory and the immune-based systems, we propose a novel approach based on the Dendritic Cell Algorithm (DCA) for fusing the results of Naïve Bayes (NB) and Support Vector Machines (SVM). DCA is a relatively recent approach in machine learning[8]. Using two SMS datasets, we evaluate and compare the effectiveness of the individual feature sets and the proposed fused model.

The remainder of this paper is organized as follows. Section 2 describes the methodology and Section 3 presents the empirical analysis and results. Finally, Section 4 concludes the paper.

2. Methodology

The generic framework for fighting against textual SMS spam is typically treated as a document categorization problem where individual messages are preprocessed and represented by feature vectors. Then, statistical or machine learning models are built using a training corpus to determine the category for each received message to be spam or legitimate (ham). Differences among various approaches are mainly in how messages are transferred to feature vectors and how classification takes place. The details of the main phases of the proposed model are provided in the following subsections.

2.1. Corpus Analysis and Representation

2.1.1. Enrichment

To enrich the SMS, we added two types of semantic information tagging: part-of-speech (POS) and recognized entities tags. The POS tags are the linguistic categories of words. We assign the POS tags using the Penn Treebank tag set (`http://www.cis.upenn.edu/~treebank/`). Examples of the possible tags are nouns, verbs, adjectives and adverbs. We only extracted the part-of-speech tags for the first and last terms in each message as features since they describe embedded grammatical structure that is unlikely to vary for each spammer or author[9]. The other type of tags corresponds to recognized named entities using the OpenNLP model (`https://opennlp.apache.org/`). These entities include location, organization, money, date, person and time[10].

2.1.2. Preprocessing

The preprocessing phase includes the following steps. First, the SMS message is converted into lowercase characters before being passed to the next stage. Second, each SMS message is treated as a string and then divided into distinct tokens (words). Third, each word is reduced to its root by removing all suffixes and prefixes such as 'tion', 'ing' and 'er'. We used the Porter stemming algorithm to achieve this task[11].

2.1.3. Feature Extraction

Feature extraction is a very crucial task for the SMS classification. It should not require complex analysis in order not to significantly delay the messaging service. But extracted features should also be highly correlated to the message