Spamming in Short Message Service (SMS)

Taofeek-Ibrahim, Fatimoh Abidemi & Abikoye, Oluwakemi Christiana (Ph.D)
Computer Science Department, The Federal Polytechnic, Offa, Kwara State, Nigeria
Computer Science Department, University of Ilorin Kwara State, Nigeria
E-maills: fatty_fatty2@yahoo.com.au; kemi_adeoye@yahoo.com

ABSTRACT

Spamming is very common because of the economics. Spam advertisers have little to no operating costs and so need only a minute response rate to make a profit. Short Message Service (SMS) spamming gained popularity over other spamming approaches like Electronic-mail (E-mail) and due to the increasing popularity of SMS communication. It has become a major nuisance to the mobile subscribers given its pervasive nature. Spam SMS detection is more challenging than E-mail spam detection because of the restricted length of SMS, use of regional content, abbreviations and shortcut words, and limited header information. Moreover, the abbreviations used by SMS users are not standard for a language, they depend on the users communities. Such language variability provides more terms or features, and a more sparse representation. This paper presents a review of SMS spam; compares SMS and E-mail, some commonly used SMS spam detection techniques were also discussed.

Keywords: Spamming, Electronic-mail (E-mail), Short Message Service (SMS), Spam, Features, Representation.

iSTEAMS Conference Proceedings Paper Citation Format
Taofeek-Ibrahim, Fatimoh Abidemi & Abikoye, Oluwakemi Christiana (2018) Spamming in Short Message Service (SMS). Proceedings of the 14th iSTEAMS International Multidisciplinary Conference, AlHikmah University, Ilorin, Nigeria, Vol. 14, Pp 201-214

1. INTRODUCTION

Mobile and wireless technologies have evolved beyond recognition since the first radio signals were transmitted in the late nineteenth century (Urbas & Krone, 2006). Mobile technology has since been advancing at a rapid pace. This technology makes it even easier to communicate, do business and learn on your mobile device. Many technology enthusiasts dream of an “all-in-one” portable device, which can handle all their communication and entertainment needs. Short Message Service (SMS) or text messaging, has become one of the world’s most popular and practical forms of communication. According to Syniverse Technologies (2016), it is the world No. 1 form of electronic communication. Globally, almost 6 billion people use it. And in just 2011 alone, it was used to send more than 7 trillion communications. In a fragmented mobile world of multiple devices, operating systems and service providers, messaging remains the one constant that offers a singular ubiquitous channel through which all end users can communicate with each other. SMS grows beyond traditional texting and is now being used in authentication (e.g. mobile banking, one time password delivery etc), information retrieval systems (e.g., TV shows), smart phone configuration Over-The-Air (OTA) configuration and social web site alerts (e.g., Facebook, Twitter, etc) (Andrew, 2008).

According to Syniverse Technologies (2016), not only is messaging the most widely used form of communication, it is also one of the most trusted. As long as you have a mobile phone and service plan, SMS is available. This makes its global reach soar as there are no pre-existing connections required, such as accepting friend requests, requiring two parties to download the service app. The technology for sending and receiving SMS is not reliant on high speed internet, essentially making anyone in modern society reachable. Messaging is communication associated with close acquaintances, personal topics and private conversations, making it more highly trusted than other channels like E-mail and because it is such an omnipresent and trustworthy communication channel, messaging has become a prime target of fraudulent activity. This high trust along with the sheer volume of text messages-SMS reached 8.7 trillion messages worldwide in 2015, up from over 5 trillion messages in 2010, according to informa-has made messaging platform attractive to spammers looking to abuse end-user confidence (Andrew, 2008).

According to International Telecommunication Union (ITU), Spam is an unsolicited electronic message which includes but it is not limited to emails, short message service (SMS),Voice over Internet Protocol (VoIP), instant messages from chats. Spam is usually sent in bulk for commercial or other purposes and indiscriminately. SMS spamming gained popularity over other spamming approaches like email and due to the increasing popularity of SMS communication. It has become a major nuisance to the mobile subscribers given its pervasive nature. It incurs substantial cost in terms of lost productivity, network bandwidth usage, management and raid of personal privacy. Mobile Spam frustrate the mobile phone users just like email spam, they cause new societal frictions to mobile handset devices. The gravity of problem can be analyzed by a survey report, which shows that the number of spam SMS exceeds more than 50% of the total received SMS. Alone in UK, 66% of mobile phone users received spam text messages. It is however worth to note that a large volume of spam SMS originates from cellular companies themselves containing information related to new offers and deals (Rafique & Abulaish, 2012).

Spam SMS detection is more challenging than E-mail spam detection because of the restricted length of SMS, use of regional content, abbreviations and shortcut words, and limited header information. Only 160 characters are allowed in a standard SMS text, and that could be a problem because using fewer words means less information to work with. Due to this constraint, people tend to use acronyms when writing SMS. For instance, Instead of expressing “How are you” the users generally type only “how r u”. Moreover, the abbreviations used by SMS users are not standard for a language, but they depend on the users communities. Such language variability provides more terms or features, and a more sparse representation (Lutfun & Mainul, 2017).

The amount of text that is generated every day is increasing dramatically. This tremendous volume of mostly unstructured text cannot be simply processed and perceived by computers. Therefore, efficient and effective techniques and algorithms are required to discover useful pattern (Allahyari, Safaei, Pouriyeh, Trippe, Kochut, Assefi, & Guttierrez, 2017).Furthermore, since a vast majority of messaging traffic is legitimate, highly accurate content analysis and filtering is required to remove spam but at the same time ensure that a reliable delivery of legitimate messages is maintained (“Protecting the last refuge of spam- free communication”, 2016).

There are different categories of SMS spam filtering such as List-Based Filters (white list and black list), Legislation approaches, Heuristic approaches and Machine-learning approaches. The techniques are used in client side, server side or in both client and server sides. Machine learning provides better protective mechanisms that are able to control spam (Subramaniam, Jalab & Taqa, 2010). Naïve Bayes, Multinomial Naïve Bayes, Support Vector Machine (SVM), Logistic Regression, Decision Trees, K-Nearest Neighbor are used to classify between Spam and legitimate SMSes named Ham. Unfortunately, none of these techniques seem to solve the challenges of use of abbreviated words (Lutfun & Mainul, 2017).

2. SHORT MESSAGING SERVICE (SMS)

SMS has been in existence since the second generation (2G) to the present fourth generation (4G) mobile phone (Pereira & Sousa, 2004). This GSM data service has established itself as the simplest and easiest means of personalized one-to-one communication; it has been the longest and the most popular messaging service. Consequently, the low cost of SMS and network reliability has made sending of SMS messages an economical option for GSM subscribers (Duksu, et al., 2010). Short Messaging Service (SMS) refers to a wireless, radio-based service for transferring short alphanumeric messages among mobile phones on the Global System for Mobile (GSM) communications and Universal Mobile Telecommunication Systems (UMTS) cellular networks. It was introduced in the wireless networks and was included in the GSM standards in 199. It is a two way transmission service that makes use an SMS Center (SMSC) that acts as a store-and-forward unit for messages. The sender can receive a notification for a success or failure of the transmission thus providing a guaranteed delivery to the receiver. Moreover, a mobile handset is able to receive or send a message any time, even when an active call is in progress. If some failures occur, the message is kept in the network until the destination is available. It also has special features of out-of-band packet delivery and low-bandwidth transferring of message. An SMS is formatted as a byte array that contains a message header and body. The header section can be used to attach different details that need to be sent along with the message while the body contains the actual message. The message length is up to 160 alphanumeric characters and can be converted to 70 ASCII characters using Base64 encoding. SMS service can be used to provide some additional services for mobile information services. This includes mobile electronic commerce, mobile transactions, news, sports, and entertainment services (Nyamtiga, Sam & Laizer, 2013).

2.1Categories of SMS
SMS may be categorized as shown in Figure 1.

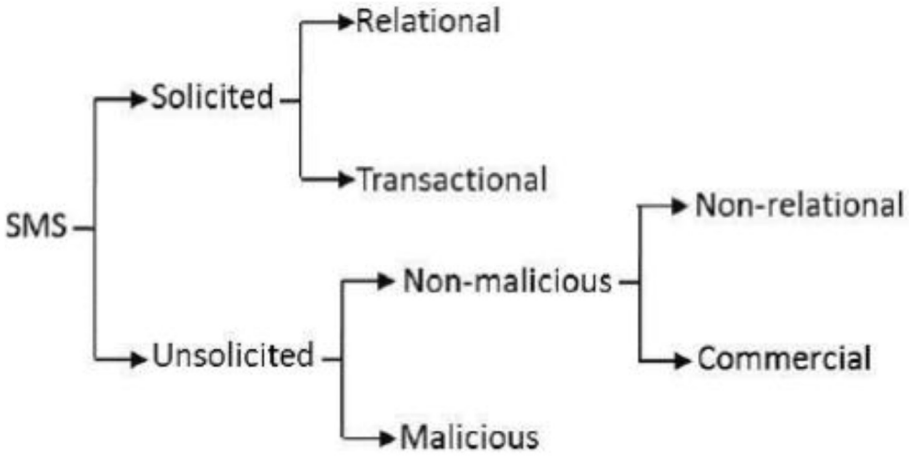

Figure 1: Categories of SMS (Osho, et al., 2014)

Every SMS can broadly be categorized as either solicited or unsolicited. Solicited short messages often contain relational messages, sent by an entity with personal relationship with the subscriber. The message could also be transactional, containing information from organizations whose services the recipient have subscribed to. Financial alerts, ticket or reservation booking information, mobile message response to enquiries, to mention but few, are instances of transactional messages. On the other hand, unsolicited short messages will usually convey either malicious or non-malicious contents. Most unsolicited non-malicious short messages emanate from senders without personal relationship with the subscriber. The sender may have obtained the phone number of the subscriber from a relation, friend, or through other sources. Also in this group of unsolicited non-malicious messages are commercial messages sent by mobile network operators, value-added service providers, and telemarketers. These constitute the bulk of spam short messages. Unsolicited malicious messages would normally come from senders who spoof the names of legitimate organizations, taking advantage of mobile users' subscription to transactional communications. This malicious intent forms the basis for identity theft. The header of the message is structured to assume the identity of a legitimate entity. Unsuspecting SMS subscribers often fall prey to this type of message (Osho, et al., 2014)

2.2 Differences between SMS and E-mail

- Short Messaging Service (SMS) is a text communication service in the world of mobile communications system. It involves using communications protocols to exchange short messages between fixed lines or handheld devices, but most commonly used in cell phones. Electronic mail (e-mail) is a way of exchanging digital messages or text communication in the world of internet and computer networks. It involves using Transmission Control Protocol – Internet Protocol (TCP-IP) to send messages in the form of packets to the users over computing devices with internet facility.
- For sending SMS, one needs to have a cell phone with short messaging service application (which is very common) and a working Subscriber Identity Module (SIM) from a telecommunication service provider. For sending an e-mail, one needs to have a computing device (pc or laptop), an internet connection, and an e-mail address from the internet service provider.
- In SMS, there is a word limit of around 160 characters for which the user is charged a certain price. Going over that limit (for the next 160 characters), the user is charged twice and so on. Moreover, most cell phones do not have the option of going over 1000 characters. In e-mailing, there is no such word limit and the user can send right from a short message to a long descriptive one.

- SMS do not carry with themselves the additional benefits of attaching multimedia files or using colorful and different fonts. E-mailing is bundled with the benefits of attaching multimedia files like pictures, songs, other files. E-mails also have an option to use a different sized, colored fonts, colored backgrounds, and themes.
- SMS captures over the precious memory because they automatically store themselves up in either the phone memory or in any external memory objects like memory cards, hence reducing the amount of memory needed for other stuff. E-mails do not require the memory of your pc or laptop but utilize the server's memory to store themselves.
- SMS are preferred over e-mails when it comes to having quick and long hours of conversation. Whereas, e-mails are preferred if the message to be delivered is long and there is no cell phone connectivity between the two persons involved or the user doesn"t want to spend money on international SMS (Osho, et al., 2014). Both come in handy in different situations and both have their own individual charm that makes them two of the most used applications in the world ("sms vs email", n.d.).

3. SPAM

In one sense, the history of spam is the history of the Internet. It is a history of hackers who have constantly probed the limits of the Net's capabilities to enable the medium to do their bidding in delivering all manner of electronic junk messaging. And it is also a tale of the scientists who have fought a constantly losing battle to try to stop them and, in the course of doing so, have helped shape the evolution of the Internet as a commercial medium (**"**Spam: A Shadow History of the Internet**",** 2013). More than half of inbound business email traffic was spam in 2015, despite a gradual decline over recent years. In 2015, spam reached its lowest level since 2003 ("Internet Security Threat Report", 2016). However, the spam problem is not going away. Spammers are finding other ways to reach their audiences, including the use of social networking and instant messaging, two of the most popular types of applications found on mobile devices. In exploiting them in addition to email, spammers continually seek to evolve their tactics ("Social media, scams and email threats", 2015).Today's IT administrations face the challenging task of managing the countless amount of mobile devices that connect to enterprise networks every day (Sullivan, 2012). Spam is an unsolicited electronic message which includes but it is not limited to emails, short message service (SMS), Voice over Internet Protocol (VoIP), instant messages from chats. Spam exist in different media such as email spam, mobile (SMS) spam, Instant message spam (SPIM), Usenet newsgroup spam, social network spam, spam dexing (Spam in search engines) and internet telephony spam. The technical difference between all these spam media makes spam in general too complex for one overview. Thus, there is a need to briefly discuss the spamming in other media as well (Osho, et al., 2015).

3.1 Email Spam

Email is the most common form of spamming on the internet. It involves sending unsolicited messages to a large number of recipients. Spammers obtain e-mail addresses by a number of means: harvesting addresses from Usenet postings, DNS listings or Web pages; guessing common names at known domains (Osho, et al., 2015).

3.2 SPIM (Instant Message Spam)

SPIM is spam delivered through instant messaging (IM) instead of through e-mail messaging. Although less ubiquitous than its e-mail counterpart, spim is reaching more users all the time. According to a report from Ferris Research, 500 million IM spam were sent in 2003, twice the level of 2002. As it becomes more prevalent, spim could impact the business community similarly to the way that spam does now, by consuming corporate resources and creating security problems ("techtarget-spim", 2006).

3.3 Spam Dexing

Spam dexing, which is a word derived from "spam" and "indexing," refers to the practice of search engine spamming. It is a form of SEO spamming. SEO is an abbreviation for Search Engine Optimization, which is the art of having your website optimized, or attractive, to the major search engines for optimal indexing. Spam dexing is the practice of creating websites that will be illegitimately indexed with a high position in the search engines. Sometimes, spam dexing is used to try and manipulate a search engine's understanding of a category. The goal of a web designer is to create a web page that will find favorable rankings in the search engines, and they create their pages according the standards that they believe will help – unfortunately, some of them resort to spam dexing, unbeknown to the person who hired them ("web spam- SEO spam", 2018)

3.4 Mobile Phone Spam

Mobile phone spam, also known as **SMS spam** is directed to the text messaging services of a mobile phone. It is a subset of spam that involves unsolicited advertising text messages sent to mobile phones users through the SMS. Everybody everywhere knows that email providers have spam filters but most people do not know the cell phone company has spam filters for SMS messages as well. When you are receiving SMS spam, it means that those messages got through the filters and made it to your phone.

1. **Definition of SMS Spam**

   SMS spam (sometimes called cell phone spam) is any junk message delivered to a mobile phone as text messaging through the Short Message Service (SMS) (whatis.com).It is understood as the unsolicited or undesired messages received on mobile phones. SMS Spam is classified as 32.3% annoying, 24.8% time wasting and (21.3%) violating personal privacy (Nuruzzaman et al., 2012). For example, Zain, a GSM operator in Nigeria would send an average of five (5) text messages a week to a subscriber advertising their numerous products, while in countries like India, an estimate of over 100 million SMS spam is received per day (Yadav et al., 2011). Skudlark (2014) described SMS spam as annoying and also incurring significant cost on both the Mobile Network Operators and the customers as well. SMS spammers can easily reach their victims by simply enumerating all numbers from the finite phone number space unlike the email spam, where the number of possible email addresses is unlimited. This type of spam appears to breach the privacy and electronic communication regulations because they are sent to the subscribers without prior consent from the sender Chaminda, Dayaratne, Amarasinghe & Jayakody (2013), hereby allowing users fall victims of fraudulent activities such as phishing, identity theft and fraud. In dealing with SMS spam, sometimes one can be spammed by a single number, but often it comes from all over the place.

   Once one replies with “STOP” as directed by the spammer, sure, the spam may eventually stop, but it lets the spammer know that they got a real person. For most phone providers, it is unlikely to work the way you think. You end up getting more Mobile users have become increasingly concerned regarding the security of their client confidentiality. This is mainly due to the fact that mobile market remains intrusive to the personal freedom of the subscriber. SMS Spamming has become a major nuisance to the mobile subscribers given its pervasive nature. It incurs substantial cost in terms of lost productivity, network bandwidth usage, management, and raid of personal privacy. Thus in short spamming threatens the profit of the service providers (Wang, et al., 2010 ; Reaves, et al., 2016).Mobile SMS spams frustrate the mobile phone users, and just like e-mail spam, they cause new societal frictions to mobile handset devices(Yamakami, 2003). Email spam is sent or received via the World Wide Web, while the SMS mobile spam is typically broadcasted via a mobile network. Filtering SMS spam is complicated by several factors, including the lower rate of SMS spam (compared to more abused services such as internet email), which allowed many users and service providers to ignore the issue, and the limited availability of mobile phone spam filtering software (“Mobile phone spam”, 2018).

2. **Electronic-mail (E-mail) and SMS spam Detection**

   Detection of SMS spam messages is actually a subset of spam e-mail detection problem. While an e-mail may contain text, graphics, hyperlinks, and even attached files, an SMS message contains only text limited with only 160 characters according to European Telecommunications Standards Institute (1992). Consequently, detection of spam messages corresponds to a 2-class text classification problem where the classes are defined as “spam” and “legitimate” (Uysal, 2013). The (at least superficial) similarity of SMS spam filtering to email spam filtering suggests that proven technologies in email spam filtering may be useful in combating SMS spam. The content-based technologies used in email spam filtering that are candidates for SMS spam filtering include both direct content filtering and collaborative content filtering techniques (Delany, et al., 2012). The direct content filtering technologies search or use the direct textual content of the message and vary from the simplistic keyword filtering to the more varied Spam Assassin-type rule sets, to the more complex automatic text classification approaches (Delany, et al., 2012). Automatic text classification uses supervised machine learning algorithms to train a model on a set of examples of spam and legitimate messages which are labeled appropriately. This set is known as the training set and should be representative of typical spam and legitimate messages. The model learns from this training set how to distinguish spam from non-spam and is used to predict whether new messages are spam or not.

Automatic text classification requires a representation of each message; typically an n-dimensional vector where each dimension represents a characteristic or feature that is predictive of the text classification problem. The features are identified by parsing and tokenisation of the textual content. A typical tokenisation can be word-based or n-gram character-based.

The value of each feature in the vector representation of a message is normally representative of the frequency of occurrence of that feature in the message. Collaborative content filtering techniques allow a group of users to share information on spam messages. A successful approach is to generate a signature (sometimes known as a fingerprint) from the content of a known spam message and this is distributed and shared with a group of users. A signature is generated for all incoming messages and checked against the known spam signatures, and matches are labelled as spam messages. A well-known example is Vipul's Razor, an un-disclosed variation of which is used by the email spam filtering company Cloudmark. Collaborative filtering techniques rely heavily on the quality and amount of user-reporting of spam, which can be difficult in the mobile world as smart mobile devices and appropriate software technology are necessary to support user-reporting functionality (Delany, et al., 2012). The fact that many of the same issues apply across both filtering domains supports using proven email filtering technologies. Both domains have the technical issues of efficiency of filtering in real-time and have to decide between client-side and/or server-side filtering. More significantly, the characteristics of email spam filtering that make it a challenging filtering problem transfer also to the mobile space. The legitimate SMS messages that are incorrectly classified as spam by the filter are as apparent in SMS spam filtering as in email spam filtering. In addition the issue of handling concept drift, the constant change in spam in order to bypass filters, is also a key challenge.

There is already strong evidence of concept drift in current SMS spam with spammers using low volumes to avoid volume filters. As SMS spam becomes more prevalent and the filtering becomes more sophisticated in response, concept drift will become a significant problem in SMS spam filtering. For SMS spam however a number of additional issues arise, firstly regarding the message itself. The maximum length of an SMS message is 160 characters which means there is little material for content-based filtering. Due to the short message length available, SMS subscribers use an idiosyncratic language subset with abbreviations, phonetic contractions, bad punctuation, emoticons, etc., which is different to the more traditional written language more typically used in emails. It has also been shown that email spam filtering can be improved by including contextual information found in the email headers but SMS messages contain far less information in the headers, which offers less context to work with.

The mobile technology is also a factor. Client side solutions to spam filtering must operate on resource-constrained mobile devices. Despite the increasing use of smart phones, so-called feature phones, with only basic voice call and text functionality are still in the majority, especially in emerging markets where such phones continue to be launched and sold. Such devices also do not have the functionality to display a spam folder such as is common with email clients, so it is more difficult to tell users that messages have been blocked (Kobus et al., 2008). Furthermore, mobile devices typically do not facilitate user reporting of spam messages, unless this service is offered by the network or by a third party, e.g. via a short code, which makes collaborative content filters, which rely on user feedback, difficult to implement Unlike email, spam SMS not only intrudes the privacy of the users, but also adds to their annoyance because in most mobile phones its arrival is indicated through an alert tone (Rafique & Abulaish, 2012).

4. TAXONOMY OF EXISTING SMS SPAM FILTERS

There are different approaches of SMS spam filtering such as white listing and black listing, content-based, non-content based, collaborative approaches and challenge-response technique. The techniques are used in client side, server side or in both client and server side (Onashoga, et al., 2015). Listing Approach: This technique is a conventional way of filtering SMS and its classification depends on two features called the whitelist (legitimate sender number) and blacklist (unwanted or unsolicited sender's number). Content-based Approach: This approach is a rule based classification that uses pattern recognition algorithm such as Bayesian, Support Vector Machines (SVM), Decision Tree, Hidden Markov Model (HMM) and K-Nearest Neighbor (KNN) to distinguish between spam and Ham messages. Non-Content-based Approach: It is a behavioral-based detection system which uses the sending patterns such as temporal, static and network features of a spammer to classify SMS messages.

Collaborative Filtering Approach: Collaborative content filtering takes a server-based approach to combating SMS spam by collecting millions of messages of users around the globe or combining collective classifying power and accuracy from a community of users to form a super-classifier.

4.1 Machine learning Algorithm
Machine learning is about designing algorithms that allow a computer to learn. Learning is not necessarily involves consciousness but learning is a matter of finding statistical regularities or other patterns in the data. Thus, many machine learning algorithms will barely resemble how human might approach a learning task. However, learning algorithms can give insight into the relative difficulty of learning in different environments (Ayodele, 2010). The following are three broad types of machine learning algorithms:

4.2 Feature sets
In designing SMS spam filtering system, some features set are needed for classification and must correctly identified. According to Xu et al., (2012), such features include Bag of Words (BoW), Static, Temporal and Network (Onashoga et al., 2015).

Bag of Words (BoW) In Natural Language Processing, BoW model is used to represent documents, where all the words in the entire set are put together without regard to their order. The most frequent words can then be used as features in the term-document matrix.

Static features This category of static features uses the number of messages and the size of SMS message within a time period as a property for describing a sender. It is assumed that spammers usually send a large number of short messages simultaneously to make up for the cost, unlike normal users do not have a pattern except for special holidays such as New Year (Xu, et al., 2012).

Temporal features It uses the timing of an SMS which include number of messages during a day, size of messages during a day, and most importantly time of the day when the message was sent.

Network features This category uses the number of recipients and clustering coefficients to describe the sender. Spammers tend to send an invalid message to a large number of receivers without any measure of connectivity, while normal users usually have a limited set of familiar persons (Onashoga et al., 2015).

4.3 Spam Filtering Process
A manually classified spam and ham messages are input or training set for a spam filtering algorithm. The filtering process consists of the following steps (Hidalgo et al., 2006). **Preprocessing**: Deletion of irrelevant elements (e.g. HTML), and selection of the segments suitable of processing (e.g. headers, body, etc.).

Tokenization: Dividing the message into semantically coherent segments (e.g. words, other character strings, etc.).

Representation: Conversion of a message into an attribute-value pairs" vector, where the attributes are the previously defined tokens, and their values can be binary, (relative) frequencies, etc.

Selection: Statistical deletion of less predictive attributes (using e.g. quality metrics like Information Gain).

Learning: Automatically building a classification model (the classifier) from the collection of messages, as they have been previously represented. The shape of the classifier depends on the learning algorithm used, ranging from decision trees (C4.5), or classification rules (Ripper), to statistical linear models (Support Vector Machines, Winnow), neural networks, genetic algorithms, etc

5. RELATED WORKS

Unlike the growing and large number of articles about email spam classifiers, there are still few studies about SMS spam filtering. SMS spam detection is comparatively a new research area than email, social tags, and twitter and web Spam detection (Lutfun & Mainul, 2017). The researchers are mostly conducted after 2010. Summary review for utilization of features extraction and tools that have been studied in SMS spam filtering is presented as follows: Jialin, Yongjun, Zhijian and Bolun (2018) presented a new fine categorized SMS spam corpus which they claimed was unique and the largest one to the best of their knowledge. They proposed a classifier, which was based on the probability topic model. The classifier could alleviate feature sparse problem in the task of SMS spam filtering. They compared the approach with three typical classifiers (k-Nearest Neighbors (K-NN), Naive Bayes (NB) and the Support Vector Machine (SVM)) on the new SMS spam corpus. According to them, the experimental results showed that the proposed approach was more effective for the task of SMS spam filtering.

However, the Huaiyin Institute of Technology (HIT) SMS Spam Corpus collected was not very enough and has the problem of class-imbalance. Dewi, et al., (2018) presented an analysis and implementation of cross lingual short message service spam filtering using graph-based k-nearest neighbor. The steps performed in the research were in four phases: documents translation as needed, preprocessing, graph building, and classification using graph-based K-Nearest Neighbor (GKNN). The model was based on two languages: Indonesia language (Bahasa) and English Language with Indonesia 35 language/Bahasabeing the primary language for analysis. The computational complexity of the graph representation for text Classification is a main disadvantage of the approach (Yadav et al.,, 2011) Abdulhamid, Latiff, Shafie and Herawan (2017) in their Review on Mobile SMS Spam Filtering Techniques, showed that researchers mostly depend on SVMs and the Bayesian network for designing classifiers that filter spam SMS. According to them, those applications have some limitations: the number of support vectors (SV) is directly proportional to the size of the training dataset which forces SVMs to use unnecessary basis functions and hence, SVMs are not suitable for the prediction of class labels because they are not based on probability, it is necessary for the kernel function in SVMs to fulfill Mercer's condition which means that they must have a continuous symmetric kernel of a positive integral operator according to their study, relevance vector machine (RVM) prediction is based on probability and the sensitivity of the RVM to free parameters is lower than that of the SVMs, and the selection of arbitrary kernel functions is probabilistic. Also, fewer relevance vectors (RV) are used in RVMs compared to the SVs of a SVM.

Thus, time computational complexity (TCC) for classification using RVMs is less than that of SVMs. Based on their review observations; RVM is not common among researchers in proposing methods for the detection and classification of spam SMS. Yilmaz & Omar (2016) developed a feature extraction approach in SMS spam filtering for mobile communication: one-dimensional ternary patterns. In their study, an image processing method, local ternary pattern, was improved to extract features from SMS messages in the feature extraction stage. Firstly, text message was converted to their UTF-8 values. Later, each character (its UTF-8 value) in the message was compared with its neighbors. Two different feature sets were extracted from the results of these comparisons. Finally, five machine learning methods (Bayesian network, Naïve Bayes, radial basis feed forward neural network, k nearest neighbors, and RF) were employed to classify these features. Three different SMS corpora were used. According to them, the proposed approach could be employed in any type of text such as short text and/or a text that contain abbreviations, because it was built on the UTF-8 values of the characters in the text.

Determining the optimal parameters of 1D-TP was a challenge. Al-Hasan & El-Alfy (2015) explored a number of content-based feature sets to enhance the mobile phone text messaging services in filtering unwanted messages. Moreover, they developed a spam filtering model using a combination of most relevant features and by fusing decisions of two machine learning algorithms (Support Vector Machine (SVM) and Naıve Bayes (NB)) with the Dendritic Cell Algorithm (DCA). The performance was evaluated empirically on two SMS spam datasets. Their 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 mode. The approach was not compared with other models and not tested ondifferent datasets. Dipak & Kavita (2015) used WEKA text classification technique to classify spam message. Different algorithms on SMS dataset were used and on the basis of accuracy, time and error rate a suitable algorithm for the purpose was found. The results of their evaluations presented showed that for different algorithms, accuracy and time are different.

They showed On the basis of both accuracy and time, Naïve Bayes Multinomial was best algorithm for classification of spam SMS. Because its accuracy is highest as well as time required generating model is less than other algorithms Mujtaba & Yasin (2014) in their work, described a mobile station based approach where the spam SMS would be identified and removed as soon as it is received at the mobile device. Four features were derived from each SMS message and using these features a trained machine learning algorithm could classify an unknown message to be spam or ham. These features are the size of the message and existence of frequently occurring monograms in the message, existence of frequently occurring diagrams in the message and message class. The performance of Naïve bayes algorithm was shown to be better than other algorithms explored. The other algorithms were Artificial Neural Networks and Decision Tree classifier. Optimal set of features were not found. The accuracy was 93% Uysal, et al., (2013) suggested a k -nearest neighbor (kNN) and Support Vector Machine (SVM) classification of real-time mobile application for Android based mobile phones. Different permutations of the Bag-of-Word (BoW) and structural features (SF) were fed into widely used pattern classification algorithms in order to classify the SMS messages.

The experimental results and analysis on the relevant test sets showed that the mixture of BoW and SFs (instead of BoW characteristics alone) allows for a more effective and precise performance classification on both test sets. It was also found that the efficiency of utilizing characteristics selection processes varies in each language. It may not take care of new structural features. Hooshmand (2013), in his project, used a database of real SMS Spams from UCI (University of California, Irvine) Machine Learning repository, and after preprocessing and feature extraction, 38 different machine learning techniques were applied to the database. The results were compared and the best algorithm for spam filtering for text messaging was introduced. The best classifier in the original work citing this dataset utilized SVM as the learning algorithm, which yielded overall accuracy of 97.64%. Next best classifier in their work was boosted naive Bayes with overall accuracy of 97.50%. When results of previous work were compared, the classifier reduced the overall error by more than half. Adding meaningful features such as the length of messages in number of characters, adding certain thresholds for the length, and analyzing the learning curves and misclassified data have been the factors that contributed to this improvement in result Final simulation results using 10-fold cross validation showed the best classifier in the work reduced the overall error rate of best model in original work citing the dataset by more than half.

He was able to prove from simulation results, multinomial naive Bayes with Laplace smoothing and SVM with linear kernel are among the best classifiers for SMS spam detection. Nuruzzaman et al., (2012) offered a text classification technique using Naïve Bayes and word occurrences tabling contributing to SMS spam filtering on an independent mobile phone based on Naïve Bayes and word occurrences table. Two experiments were carried out with the new technique. The first simulation depicts a scenario where the applicability is low since the user needed to have a huge amount of data during the initialization of the training data. Therefore, a second simulation is run as the subscriber needs about 10 SMS spam and 10 SMS ham as training data. The results showed that the proposed spam filtering scheme on an autonomous mobile phone achieves outstanding precision with low storage consumption and satisfactory execution time. Not all word attributes are used to filter new incoming SMS because one 39 regular word can be written in many abbreviated forms based on community agreement. Better features for SMS classification are needed to improve accuracy. Mahmoud & Mahfouz (2012) created an Artificial Immune System (AIS) SMSs classification scheme for filtering SMS spam. The AIS system uses a set of features to serve as an input spam filter. It categorizes text messages by using a trained dataset which consists of Phone Numbers, Spam Words and Detectors.

The experimental results are obtained using the iPhone Operating System (iOS). The outcome of this experiment shows that the proposed scheme is able to classify messages either as spam or non-spam with more accuracy and convergence speed than the Naive Bayesian algorithm. Texts with regional contents and short texts/text that contains abbreviation will be a challenge to this approach Uysal, et al., (2012) proposed a Bayesian-based filtering framework consisting of the features derived from the Bag of Word model together with the collection of selected features explicit to spam. The performance of the framework was experimentally assessed on a bulk message collection which includes spam and non-spam messages. The results showed that a considerably high level of precision in terms of the classification is achieved for both spam and non-spam SMSs. The performance might have been improved with the collection of selected features. Rafique & Abulaish (2012) presented a novel graph-based spam detection architecture that tokenizes SMS messages and exploits their occurrence and sequential patterns to detect spam messages on mobile devices. The proposed scheme was evaluated on two real-world datasets containing both benign and spam messages and the achieved accuracy for detecting SMS spam was very appealing.

The other important contribution of the proposed scheme lied in its real-time deplorability to classify spam messages by using well-known statistical measure, (Kullback-Leibler) KL-Divergence. The graph representation of the document is more expressive than standard bag of words representation, and consequently gives improved classification accuracy. Hidden relationships among terms in the documents can also be preserved and extracted. However, the computational complexity of the graph representation for text Classification is the main disadvantage of the approach (Yadav et al., 2011)

The review has encountered a number of feature types in SMS spam filtering which have resulted at a different level of accuracies. A content feature usually consists of spam keywords, URL links, monetary value, special characters, emotion symbols and function words. Non content features consider message metadata such as length, the number of characters, white spaces, the number of terms, date, time and location wise (Zainal & Jali, 2016).Vast amount of text classification studies make use of the bag-of-words model to represent text documents where the exact ordering of words, or terms, in the documents is ignored but the number of term occurrences is considered. Each distinct term in a document collection consequently constitutes an individual feature. Terms are assigned particular weights representing their importance in a given document. The most common weighting scheme is Term Frequency - Inverse Document Frequency (TF-IDF) that scales down the number of occurrences of a term in a document by considering the number of documents in the collection containing that term. Thus, a document is represented by multi-dimensional feature vector where each dimension of the vector corresponds to the weighted value for a distinct word within the document collection, which is also known as the vector space model. The Bag of words representation does not consider the semantic relation between words. Generally the neighbor words in a sentence should be useful for predicting the target word. Bag of words also has the curse of dimensionality issue as the total dimension is the vocabulary size. It can easily over-fit the model (Uysal, et al., 2013).

6. SUMMARY

The increase in the number of mobile phone users and thus, its dependence worldwide has unavoidably attracted spammers and caused SMS spam (unsolicited) message problem just as in the case of spam e-mails.. Spam is not only annoying but it can be a vehicle for severe security breaches and information leakage as well. SMS spam is real and growing problem primarily due to the availability of very cheap bulk pre-pay SMS packages and the fact that SMS engenders higher response rates as it is a trusted and personal service (Delany et al., 2012). Blacklisting methods, statistical methods which are built on the frequency of occurrence of words or characters, and machine learning methods have been employed in SMS spam filtering. Because punishments and legal laws are not enough to solve this problem and the Group Special Mobile number of SMS can easily be changed, a content-based approached was proposed. Content-based methods showed high success in spam e-mail filtering, but it is hard in SMS spam filtering because SMS messages are extremely short and generally contains many abbreviations.

The SMS Spam detection techniques are more challenging than Email spam detection techniques because of the regional contents, use of abbreviated words (Lutfun & Mainul, 2017). The techniques which have been used to date apply what has been used in text classification in general to SMS filtering, and not necessarily taking the specific characteristics of SMS into account (Delany, et al., 2012).

7. CONCLUSION

The abbreviations used by SMS users are not standard for a language, but they depend on the users communities. Such language variability provides more terms or features, and a more sparse representation (Lutfun & Mainul, 2017). Vast amount of text classification studies make use of the bag-of-words model to represent text documents where the exact ordering of words, or terms, in the documents is ignored but the number of term occurrences is considered (Uysal, et al., 2013). The Bag of words representation does not consider the semantic relation between words (Parseh & Baraani, 2014). Generally, the neighbor words in a sentence should be useful for predicting the target word (Chen, 2017). Bag of words also has the curse of dimensionality issue as the total dimension is the vocabulary size. It can easily over-fit the model (Zhang, 2017). Since a vast majority of messaging traffic is legitimate, highly accurate content analysis and filtering is required to remove spam but at the same time ensure that a reliable delivery of legitimate messages is maintained ("Protecting the last refuge of spam- free communication", 2016).
Yilmaz and Omer (2016) came up with a feature extraction approach for SMS spam using One-Dimensional Ternary Patterns (1D-TP). They proved the approach was effective for each type of messages such as short texts and/or texts that contain abbreviations. Determining optimal parameters of 1D-TP was however a challenge of the approach. The author of this paper is currently working to improve upon the 1D-TP feature extraction approach by developing a meta-heuristic optimization of the 1D-TP feature extraction technique for Short Message Service (SMS) spam detection system using Simulated Annealing algorithm for optimization of the extracted features.

REFERENCES

1. Abdulhamid, S.M., AbdLatiff, M. S., Chiroma, H., Osho, O., Gaddafi, A., Abdul-Salaam, G., Adamu, I.A.,&Herawan, T. (2017). A Review on Mobile SMS Spam Filtering Techniques. IEEE, 5. 15651- 15666. https://doi.org/10.1109/ACCESS.2017.266678
2. Aghdam M., Tanha J., Nagllsll-Nilchi .A., Basiri M. (2009). colony optimization and Bavesian classification for feature selection in bioinformatics dataset. J. Comput. Sci. SYS1. Bioi. 2(3), I K6-199.
3. Almeida, T. A. , Yamakami, A. and Almeida, J.(2009) "Evaluation of Approaches for Dimensionality Reduction Applied with Naive Bayes Anti-Spam Filters," in Proceedings of the 8th IEEE International Conference on Machine Learning and Applications, Miami, FL, USA, pp. 517–522.
4. Al-Hasan, A., & El-Alfy, E. (2015). Dendritic cell algorithm for mobile phone spam filtering. 6th International Conference on Ambient Systems, Networks and Technologies, ANT 2015, Procedia Computer Science, 52(1), 244-251. https://doi.org/10.1016/j.procs.2015.05.067
5. Andrew, C. (2008). Top 5 Emerging Phone Technologies. Retrieved from https://electronics.howstuffworks.com/emerging-phone-technologies.htm
6. Ayodele, T.O. (2010). Types of machine learning algorithms. In: Zhang. Y. (ed.) New Advances in Machine Learning. pp. 20-48. In-TechIndia intechweb.org
7. Azeez,N.,& Mbaike, O. (2017).SMS Spam Filtering For Modern Mobile Devices. FUTA Journal of Research in Sciences, 13 (1), 177-185
8. Chaminda, T., Dayaratne, T. T., Amarasinghe, H. K. N., & Jayakody, J.M. R. S. (2013). Content-based hybrid SMS spam filter-ing system. Proceedings of ITRU Research Symposium, University of Moratuwa, Sri Lanka, pp. 31–35.
9. Choudhury, M., Saraf, R., Jain, V., Mukherjee, A., Sarkar, S., Basu, A. (2007). Investigation and modelling of the structure of texting language. IJDAR 10:157 – 174. DOI 10.1007/s10032-007-0054-0.
10. Delany, S. J., Buckley, M., & Greene, D.(2012).SMS spam filtering: Methods and data. Expert Systems with Applications, El-Sevier. 39(10), 9899–9908.https://doi.org/10.1016/j.eswa.2012.02.053
11. Dewi,D. A, C., &Shaufiah & Asror, I. (2018).Analysis and implementation of cross lingual short message service spam Filtering using graph-based k-nearest neighbor. International Conference on Data and Information Science, IOP Conf. Series: Journal of Physics: Conference Series, 971(2018) 012042. https://doi.org/10.1088/1742-6596/971/1/012042
12. Dipak, R. K. & Kavita S. O. (2015).SMS Spam Classification using WEKA. International Journal of Electronics Communication and Computer Technology (IJECCT), 5(ICICC)
13. Duksu, K., Jae-Pil, H., Jaehyuk, H., John. K. and Sung-eui. Y. (2010). Hybrid Parallel Continuous Collision Detection using CPUs and GPUs. KAIST (Korea Advanced Institute of Science and Technology) Project URL: http://sglab.kaist.ac.kr/HPCCD. Volume xx (200y), Number z, pp. 1–10.
14. Eberhardt, J.J. (2015). Bayesian Spam Detection.Scholarly Horizons: University Minnesota, Morris undergraduate Journal, 2(1), Article 2.
15. Faez, T., and Taheri, S.M.(2016). Feature Selection Using Ant Colony Optimization (ACO): A New Method and Comparative Study in the Application of Face Recognition System. DOI 10.1007/978-3-540-73435-2_6 ISSN 0302-9743
16. Han, H., Chen, Q., & Qiao, J. (2011). An efficient self-organizing RBF neural network for water quality prediction. Neural Networks, 24(7),717-725. https://doi.org/10.1016/j.neunet.2011.04.006
17. Hidalgo, J.M.G., Bringas, G. C., Sanz, E. P.,& Gracia, F.C.(2006). Content-based SMS Spam filtering. In Proceedings of the 2006 ACM Symposium on Document Engineering(DocEng'06), 107-114. https://doi.org/10.1145/1166160.1166191
18. Houshmand, S. (2013). "SMS spam detection using machine learning approach." pg 1-4.
19. Jialin M., Yongjun Z., Zhijian Wang, Bolun C.(2018). 2018. A New Fine-grain SMS Corpus and Its Corresponding Classifier Using Probabilistic Topic Model. KSII Transactions on Internet and Information Systems, 12, 2, (2018), 604-625. DOI: 10.3837/tiis.2018.02.004.
20. Kaya, Y. & Ertugrul, O. F. (2016). ˇ A novel feature extraction approach in SMS spam filtering for mobile communication: one-dimensional ternary patterns. Security and Communication Networks, Vol. 9, No. 17, pp. 4680–4690. SCN-16-0170.R1.
21. Kobus, C., Yvon, F., & Damnati, G. (2008). Normalizing SMS: are two metaphors better than one? Proceedings of the International Conference on Computational Linguistics (Cooling 2008), pp. 441-448. Manchester, August, 2008.

22. Lutfun N. L. and Mainul B. M. H (2017). "A Systematic Literature Review on SMS Spam Detection Techniques", International Journal of Information Technology and Computer Science(IJITCS), Vol.9, No.7, pp.42-50, 2017. DOI: 10.5815/ijitcs..07.05
23. Mahmoud, T.M. & Mahfouz, A.M. (2012).SMS spam filtering technique based on artificial immune system. International Journal of Computer Science Issues, 9(2), 589-597
24. Mujtaba, G. and Yasin, M. (2014). SMS Spam Detection Using Simple Message Content Features. ISSN 2090-4304 Journal of Basic and AppliedScientific Research www.textroad.com
25. Moubayed, A., Breckon T., Matthews, P. and McGough, S. A. (2016). SMS Spam Filtering using Probabilistic Topic Modelling and Stacked Denoising Autoencoder School of Engineering and Computing Sciences, Durham University, DH1 3LE Durham, UK {noura.al-moubayed,toby.breckon, peter.matthews,stephen.mcgough}@durham.ac.uk
26. Murynets, I., and Jover, R. P.(2012): "Crime Scene Investigation: SMS Spam Data Analysis". ACM Internet Measurement Conference (IMC'12), November 2012.
27. Nagwani, N.K. (2017). A Bi-level text classification approach for SMS spam filtering and identifying priority messages . International Arab Journal of Information Technology
28. Nuruzzaman, M.T., Changmoo, L., Mohd. Abdullah, F., Choi, D. (2012). Simple SMS spam filtering on independent mobile phone. Security and Communication Networks 5(10): 1209-1220
29. Nyamtiga, B. W., Sam, A., & Laizer, L. S. (2013). Enhanced security model for mobile banking systems in Tanzania. International Journal of Technology Enhencements and Emerging Engeering Research, 1(4), 4-20.
30. Onashoga, A., Abayomi-Alli, O., Sodiya, A., & Ojo, D. (2015). An Adaptive and Collaborative Server-Side SMS Spam Filtering Scheme Using Artificial Immune System. Information Security Journal: A Global Perspective, 24(4-6), 133 - 145https://doi.org/10.1080/19393555.2015.1078017.
31. Osho, O., Ogunleke, O.Y. & Falaye, A.A. (2014). Frameworks for mitigating identity theft and spamming through bulk messaging. In Adaptive Science & Technology (ICAST), IEEE 6th International Conference.https://doi.org/10.1109/ICASTECH.2014.7068119
32. Osho, O., Yisa, V.L., Ogunleke, O.Y.,& Abdulhamid, S.I.M. (2015). Mobile spamming in Nigeria: An empirical survey. In Cyberspace (CYBER-Abuja), 2015 International Conference, 150-159.https://doi.org/10.1109/CYBER-Abuja.2015.7360503
33. Pereua, C. M., & Sousa P. (2004). A Method to Define an Enterprise Architecture us-ins the Zachman FmLllcwork.lllACM Symposinm 011 Applied Computing. Nicosla, Cyprus: ACM.
34. Rafique & Abulaish (2012). Graph-Based Learning Model for Detection of SMS Spam on Smart Phones, In Proceedings of the 8th International Wireless Communications and Mobile Computing Conference (IWCMC'12) – Trust, Privacy and Security Symposium, Limasol, Cyprus, IEEE CPS, pp. 1046-1051
35. Reaves, B., Scaife, N., Tian, D., Blue, L., Traynor, P., & Butler, K.R. (2016).Sending out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways. 2016 IEEE Symposium on Security and Privacy, 339-356. https://doi.org/10.1109/SP.2016.28
36. Renuka, D.K., Visalakshi, P., & Sankar, T. (2015).Improving E-Mail Spam Classification using Ant Colony Optimization Algorithm. International Journal of Computer Applications (0975 –8887).International Conference on Innovations in Computing Techniques (ICICT 2015). 22-26
37. Sajedi, H., Parast, G.Z.,& Akbari, F. (2016).SMS Spam Filtering Using Machine Learning Techniques: A Survey. Machine Learning Research, 1(1), 1-14. https://doi.org/10.11648/j.mlr.20160101.11
38. Skudlark, A. (2014). Characterizing SMS spam in a large cellular network via mining victim spam reports, 20th ITS Biennial Conference, Rio de Janeiro 2014: The Net and the Internet - Emerging Markets and Policies, International Telecommunications Society (ITS)
39. Sullivan, (2012) Analysis of the Global Network Access Control (NAC) Market More than just NAC. Market engineering.NE66-74
40. Urbas .G & Krone T 2006. Mobile and wireless technologies: security and risk factors. http://www.aic.gov.au/publications/tandi2/tandi329.html
41. Uysal, A. K., Gunal, S., Ergin, S., & Gunal, E.(2013). The Impact of Feature Extraction and Selection on SMS Spam Filtering. Journal Elektronika IR Elektrotechnika, KTU, Lithuania, 19(5). 67-72. https://dx.doi.org/10.5755/j01.eee.19.5.1829
42. Subramaniam T., Jalab H. A. and Taqa A. Y. (2010). Overview of textual anti-spam filtering techniques‖, International Journal of the Physical Sciences Vol. 5(12), pp. 1869-1882.

43. Wang, C., Zhang, Y., Chen, X., Liu, Z., Shi, L., &Chen, G. (2010). A Behavior-based SMS Anti-Spam System. IBM Journal of Research and Development, 54(6), 651-666. https://doi.org./10.1147/JRD.2010.2066050
44. Xu, Q. , Xiang, E., Yang, Q. , Du, J. and Zhong, J. (2012) "Sms spam detection using noncontent features," IEEE Intelligent Systems, vol. 27, no. 6, pp. 44–51.
45. Yadav, K., Kumaraguru, P., Goyal, A., Gupta, A., & Naik, V.(2011).SMS Assassin: Crowdsourcing Driven Mobile-Based System for SMS Spam Filtering. https://doi.org/10.1145/2184489.2184491.
46. Yamakami, T. (2003).Impact from mobile SPAM mail on mobile internet services. In proceedings of the 2003 International symposium on parallel and distributed processings and applications, 179-184.https://doi.org/10.1007/3-540-37619-4_19
47. Yilmaz K. and Omer F. E. (2016). Security and Communication Networks: A Novel Feature Extraction Approach in SMS Spam Filtering for Mobile Communication: One-Dimensional Ternary Pattern. https://doi.org/10.1002/sec.1660
48. Zainal, K., Sulaiman, N., & Jali, M. (2015). An analysis of various algorithms for text spam classification and clustering using Rapid Miner and Weka. International Journal of Computer Science and Information Security, 13(3), 66-74.