International Journal of Engineering &Technology, 7 (3.12) (2018) 790 -792

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A Study on Spam Detection Methods for Safe SMS Communication

Shailee Bhatia[*]

Assistant Professor, Vivekananda Institute of Professional Studies
**Corresponding Author Email: shailee.bhatia@vips.edu*

Abstract

The electronic communication enables the instant and all type availability of user. The different form of information transition can be drawn in the form of SMS and emails. But these emails and SMS systems are also used by the individuals and firm as medium of their advertisement. Spam messages not only involves the unwanted messages but it also includes some viruses and threat to the security system. In this paper, a study to the SMS filtration methods is provided. The paper has explored the types of SMS spams, its threats and various filtration methods to detect the spam SMS.

Keywords: *Filtration; SMS; Spam.*

1. Introduction

The electronic data communication can be performed in different forms like email, SMS etc. Such communication is carried out in open environment which results the insecurity against various attacks. The easy availability of user's email and mobile number pass on the communication information to unknown individuals. These persons or firms can send useless messages for promotion, disturbance or hacking. These kinds of email and SMS communication comes under spam messages [1][2][3]. To increase the reliability of the communication system, there is the requirement to block the spam messages and enable only the genuine message communication. Most of the SMS and email gateways use the message filtration at an earlier stage. But even then, the smart spammers identified some other methods, information to deliver the spam messages. There is the requirement of spam message filtration to avoid the unwanted messages. These kinds of spam filter must be applied on communication gateways as well as on the client-side machines. In this paper, the behavior of the spam messages, spam filtration methods and the available spam filtration approaches are discussed [4][5][6][7]. The different type of SMS spam and their ration to the total spam messages is shown in figure 1. The main problem with spam message is that one cannot identify it as spam message. In first appearance, the spam message looks like genuine message. Once the message is read, the spam message can be identified and blocked. Once the spam message is increased, the complexities of handling of spam message increases. It is required to monitor the mobile devices regularly for spam messages. As a message is marked as spam, the filtration software can extract the message information to block the similar messages [9][10][11][12]. The categories of spam messages are commercial spam, charity messages, chain message and SMS service spam. It includes some promotional messages ,request messages for some charities, request messages forwarded from others or some messages from different providers to promote and advertise their schemes and updating.

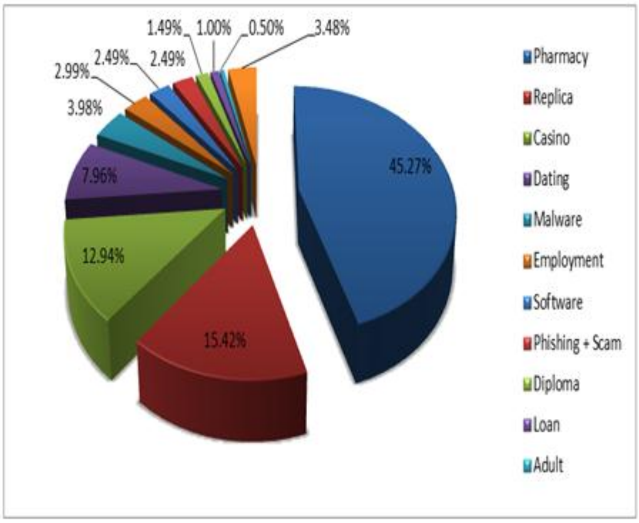

Fig. 1: Types of Spam

The categories of spam messages are listed here under

1.1 Commercial Spam

These kinds of SMS are the promotional messages that a company spread for publicity of some product. Various schemes forwarded regularly to the customers can be identified as spam messages.

1.2 Charity Messages

The request message for some donation or charity by placing some stories and problems are common as SMS spams. These messages are also passed to obtain the account information from the individuals. The direct money transfer by fooling the people is also the goal of such spams

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

1.3 Chain Message

The chain messages are the request messages forwarded from the friends. These can be some fake information, charity requests, advertisements, product publicity etc. As the messages are sent by the friends, the mobile number cannot be blocked to avoid such spams.

1.4 SMS Service Spam

The SMS service providers also send spam messages to promote their schemes, and regular updating about new plans. Even if the customer does not have the requirement, such information is communicated to the customers regularly.

2. Literature Survey

The online communication in the form of SMS and mail messages suffers from some unwanted message communication. This communication is termed as spam message communication. Lot of researchers provided different methods to locate the spam message effectively based on the information content observation. In this section, the contribution of earlier researchers is provided. Author [2] applied a feature engineering method to perform spam filtration. The performance adaptation was provided by the author to filter the SMS. The feature level derivation was provided by author to identify the constraint of spam messages. Author [3] used the behavior analysis to filter the spam and included them in blacklist. Author defined Spam Tracker tool to classify the sends, based on the spam type and block the abnormal users. The user activity, message type and the statistical information was processed collectively to identify the messages as spam messages. Author incorporated the tool on existing email server to improve the reliability of mail server. Author [4] applied a crowdsourcing based SMS spam detection system. The probabilistic learning using Bayesian network model was suggested by the author to locate the message and to generate the safe message pattern. Author [5] has applied a content-based analysis to identify the messages as spam messages. The Bayesian filter was applied by the author to block the spam emails. The spam message test collection, its size and language level analysis were applied by the author for spam identification. Author also applied the spamming method using machine learning approach. Author [6] identified the personalized challenges of spam message distribution. The scalability of spam detection method and its distribution on client and server end is provided. The user population analysis based on message type was provided by the author. Author [7] defined an email authentication system by locating the smart senders adaptively. The popular message communication and the message content analysis was performed collectively to identify the spam message and the sender. The direct and indirect effect of the message is also analyzed by the author.

Author[8] defined a work on spam filtration on web data communication. The filtration requirement, opportunities and challenges were described by the author. The message archives and the migration filter impact were analyzed by the author. Author[9] defined a spam filter message by analyzing the associated labels. The legitimate emails and messages was identified using data reduction algorithm. The consistent cluster formation and relatively the bad message identification was provided by the author. Author[10] used the similarity graph based method email spam filtration. The aspect based, user based and content-based analysis was provided by the author. The multi featured analysis was provided by the author for spam detection and to include the IP addresses in blacklist. Author[11] has used the cluster adaptive method for semi-supervised analysis for spam message detection. The email clustering-based tool was provided by the author for separately the ham and spam messages. Two semi-supervised learning methods were defined by the author as spam message detection. Author[12] used the logistic regression based spam filtration method. The naïve bays method was applied for feature space generation to generate the disjoint feature group. Author [13] used the minimum descriptor length-based spam detection approach with concern of message length and message content. The message content quality was observed by the learning method to classify the spam messages. Author[14] defined study method to identify the scope and type of various SMS spam detection methods. The result-based evaluation was provided by the author to improve the performance of message learning methods. The classifier-based evaluation was provided by the author to improve the reliability of spam message identification. Author[15] defined an information processing method for both text and image messages. Author setup an ontology-based constraint environment to customize the spam and ham messages. The message quality analysis and relative handling was provided by the author as anti-spammer system. Author[16] defined topic and user specific spam detection. The organization specific, language specific and message type specific spam detection was provided by the author.

3. Spam Filtration Methods

The implemented system aims to utilize filter-based spam detection methods and classify them as such. It uses such an approach in unison with fingerprint processing which increases efficiency and the spam. The SMS service providers also send spam messages to promote detection hit ratio. The system also makes use of multiple sources of spam reporting. These are detailed as server-side reporting, peer to peer reporting by other servers, in-house client-side reporting to SMS servers, and server-side reporting to clients. Furthermore, care should be taken not to filter legitimate messages of the clients in the haste to contain spam. The implemented system uses these approaches to optimize on the performances.

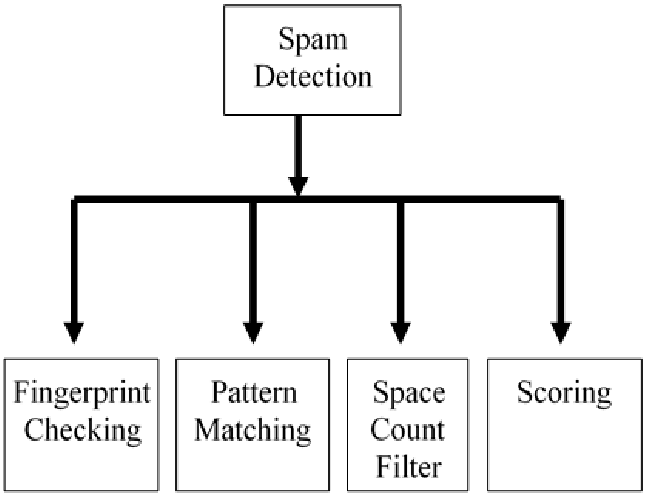

Fig. 2: Spam Detection Techniques

3.1 Pattern Matching

It works by specifying a pattern (actually a list of patterns) of text that you expect not to be found in legitimate message but common in spam messages (like "$$$$$", "Earn a lot of money" and so on).

3.2 Checking the Sender Mobile Number

Verifying if the sender of the message really exist can be a hard thing (or even impossible) and usually not done. What is much more common is verifying at least the Mobile Number. If a mobile number is sending the spam message again and again, then it can set to the spam list itself. In such case, as some message sent by the particular number, it is already taken as the spam message. This kind of check can be performed on promotional mobile numbers or the SMS service providers.

3.3 Digest Comparison

The Architectural design seeks to incorporate these factors while processing for spam. The first level filter starts with the Digest comparison. Here the process to create a Digest from the incoming message is prompted and this digest is used in an ingenious way to compare for similarities with known and reported spam messages. The system seeks to be optimistic in that it gives a measure of flexibility in which to report spam. The flexibility is not too stringent nor too lenient. The proposed system fixes this at 80% and above matches with the compared digest would result in that message as being reported as spam.

3.4 User Spam Reports

The next process relies on past user spam reports as a logical way of filtering spam. So those messages that manages to sneak past the first process are sure to be filtered in this process if it was reported as spam earlier by that client. This is client specific and does not affect the messages of the whole network in general. This is also a fairly less complex process as the spam reports are maintained and updated by the system and this dictionary of reported spams are compared with incoming messages to aid in detecting spam.

3.5 Contact List Matcher

The next process consists of the address book matching. Here this is a combination of spam sources to verify the incoming mobile number with the stored repository of user. This process also yields good results if the spam was already reported for that particular contact number can be verified.

If spam was detected in this stage then again it is filtered and the process grinds to a halt. So as the system tries its best to detect spam at each of the above-mentioned stages either independently or in union, it also is flexible to not reporting spam of ambiguous messages. This is very important else most of the messages that would even partially describe to one of the above filters would be reported as spam.

3.6 Pattern Matching

Special cases when spammer includes the space between characters of a particular string to avoid being detected as spam by dictionary checking in those cases. Eliminate the intra string spaces and form the word and compare with spam Dictionary which some unwanted words and giving individual percentage to all the words.

4. Conclusion

Spam messages are the common threat to the user in the form of continuous disturbance, space consuming, time consuming and the security threaten. In this paper, a study of the problems and challenges associated to the spam messages are identified. The paper also explored the common available methods to detect the spams in SMS system. This paper can serve as a reference in implementing spam filtering techniques based on content.

References

[1] “SMS Spam Overview — Preserving the value of SMS texting”, https://www.cloudmark.com/en/s/resources/whitepapers/sms-spam-overview

[2] Cormack, G. V., Hidalgo, J. M. G., & Sánz, E. P. (2007, July). Feature engineering for mobile (SMS) spam filtering. In Proceedings of the 30th annual international ACM SIGIR conference on Research and development in information retrieval (pp. 871-872). ACM.

[3] Ramachandran, A., Feamster, N., & Vempala, S. (2007, October). Filtering spam with behavioral blacklisting. In Proceedings of the 14th ACM conference on Computer and communications security (pp. 342-351). ACM.

[4] Yadav, K., Kumaraguru, P., Goyal, A., Gupta, A., & Naik, V. (2011, March). Smsassassin: Crowdsourcing driven mobile-based system for sms spam filtering. In Proceedings of the 12th Workshop on Mobile Computing Systems and Applications (pp. 1-6). ACM.

[5] Gómez Hidalgo, J. M., Bringas, G. C., Sánz, E. P., & García, F. C. (2006, October). Content based SMS spam filtering. In Proceedings of the 2006 ACM symposium on Document engineering (pp. 107-114). ACM.

[6] Kolcz, A., Bond, M., & Sargent, J. (2006, May). The challenges of service-side personalized spam filtering: scalability and beyond. In Proceedings of the 1st international conference on Scalable information systems (p. 21). ACM.Pattaraporn Klangpraphant," E-Mail Authentication System: A Spam Filtering for Smart Senders", ICIS 2009, November 24-26, 2009 Seoul, Korea ACM 978-1-60558-710-3/09/11

[7] Klangpraphant, P., & Bhattarakosol, P. (2009, November). E-mail authentication system: a spam filtering for smart senders. In Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human (pp. 534-538). ACM.

[8] Erdélyi, M., Benczúr, A. A., Masanés, J., & Siklósi, D. (2009, April). Web spam filtering in internet archives. In Proceedings of the 5th international workshop on Adversarial information retrieval on the web (pp. 17-20). ACM.

[9] Laorden, C., Ugarte-Pedrero, X., Santos, I., Sanz, B., & Bringas, P. G. (2011, September). Enhancing scalability in anomaly-based email spam filtering. In Proceedings of the 8th Annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference (pp. 13-22). ACM.

[10] Dasgupta, A., Gurevich, M., & Punera, K. (2011, February). Enhanced email spam filtering through combining similarity graphs. In Proceedings of the fourth ACM international conference on Web search and data mining (pp. 785-794). ACM.

[11] Whissell, J. S., & Clarke, C. L. (2011, September). Clustering for semi-supervised spam filtering. In Proceedings of the 8th Annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference (pp. 125-134). ACM.

[12] Ming-wei Chang," Partitioned Logistic Regression for Spam Filtering", KDD’08, August 24–27, 2008, Las Vegas, Nevada, USA. ACM 978-1-60558-193-4/08/08

[13] Almeida, T. A., Yamakami, A., & Almeida, J. (2010, March). Filtering spams using the minimum description length principle. In Proceedings of the 2010 ACM Symposium on Applied Computing (pp. 1854-1858). ACM.

[14] Almeida, T. A., Hidalgo, J. M. G., & Yamakami, A. (2011, September). Contributions to the study of SMS spam filtering: new collection and results. In Proceedings of the 11th ACM symposium on Document engineering (pp. 259-262). ACM.

[15] Youn, S., & McLeod, D. (2009, March). Improved spam filtering by extraction of information from text embedded image e-mail. In Proceedings of the 2009 ACM symposium on Applied Computing (pp. 1754-1755). ACM.

[16] Caruana, G., & Li, M. (2012). A survey of emerging approaches to spam filtering. ACM Computing Surveys (CSUR), 44(2), 9.

[17] Munro, R., & Manning, C. D. (2012, March). Short message communications: users, topics, and in-language processing. In Proceedings of the 2nd ACM Symposium on Computing for Development (p. 4). ACM.