How to Fight against SMS-Spam: Structural Approach and Results

Giseop Noh

Abstract—**Although the number of different uses for mobile-data networks has grown rapidly, short message service (SMS) remains the primary message-exchange method; in addition, SMS is still necessary since it provides several advantages including the small monetary cost that is incurred per transmission, greater security compared to online social networks (OSNs). Due to the popular status of SMS, SMS spam is a form of communication that can be used to pursue malicious economic intents such as phishing and illegal advertising, or to widely distribute unwanted messages to numerous phone users. In this paper, we explore the effectiveness of using social structural approach. To this end, we introduce a methodology that shows how to expand SMS networks from small SMS datasets to social networks based on real-world datasets and possible SMS-spam attack. Also, we verify the detection effectiveness of our approach by conducting experiments.**

Index Terms—**Spam detection, social structural approach, spam attacks.**

I. Introduction

The short-message service (SMS) is a communication method that sends messages of a limited size and is mostly transmitted over mobile networks (e.g., mobile phones). As the widespread use of mobile phones has expanded globally, the cost of SMS continues to decrease. As a result of the ease and low cost of using SMS, it has become the most widely-used communication service, followed by voice communications. According to the International Telecommunication Union (ITU), 5.3 billion active mobile cellular users around the world sent 1.8 trillion SMS messages (approximately 200,000 SMS messages per second) in 2010 [1]; the worldwide penetration of mobile broadband services [2] is further stimulating the use of SMS; also, 18.7 billion texts are sent worldwide every day (not including app-to-app messaging) in 2017 [3]. Even though email and mobile messengers such as Twitter are commonly used in everyday life due to the explosive growth of smart-device use, SMS is still a major method for mobile communication. From a research perspective, SMS has not been sufficiently investigated relative to similar Internet messaging services (e.g., Twitter and email); nevertheless, as is discussed in [4], Twitter comprises less than 1 % of the world's communications, but accounts for more than 75 % of the research regarding short-message communications.

Spam refers to unsolicited and/or unwanted messages that are transmitted to a large number of recipients with a malicious intent [4], [5] including economic motives, phishing, and scamming. Spam frequently appears in various online communications including email, online social networks, SMS, blogs, and online guest rooms. SMS spam is effective from the attacker's perspective for the following reasons: (i) SMS spam is not cost-prohibitive because the increase in the use of SMS leads to a reduction in message costs (below USD $0.001 in China and a cost-free service in other countries) [6]. (ii) SMS messages are often personal, privileged, and private when compared to other online short-message services [7], whereby users tend to trust incoming SMS messages and are therefore more likely to open messages compared with email or other online communications. (iii) SMS spammers can more easily acquire target accounts—the targeted telephone numbers—as they simply need to enumerate all of the numbers from a finite phone-number space, or search for phone information on the Internet; specifically, 20 % to 30 % of SMS traffic in China and India is SMS spam [8], while 30 % of SMS messages in the Asia region have been classified as spam [6]. (iv) People tend to use acronyms when writing SMS messages, so the abbreviations used by SMS users are not standard for their language; this could represent a problem because the use of fewer words indicates that there is less information to work with, and such linguistic variability provides a greater amount of terms or features with a more sparse representation [9].

So far, methods to detect email spam have been the center of attention for the research community, whereas SMS spam has rarely been considered. The available defense approaches against email spam include blacklisting, address management, and content-based filtering. A content-based approach has been proven to be an effective solution [10], and several corresponding research papers have been published [9]-[13]. The challenge of SMS-spam filtering in comparison with email-spam filtering, however, is the nature of SMS text, whereby the length is brief, informal characters are used, and less header information is available.

Recent studies have explored more advanced spam filtering methods on online social networks (OSNs). OSNs reflect real social interactions between users and have a unique structure that includes small-world behavior, clustering, and sparse cuts between the clusters.

In addition to content-based methods, spam filtering through the use of network structures has also received much attention; however, spam filtering based on the OSN

Manuscript received October 29, 2018; revised July 18, 2019. This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government(MSIT) (No. NRF-2018R1C1B5083091).

Giseop Noh is with the Cheongju University, Cheongju-si, Chungcheongbuk-do, South Korea, 28503 (e-mail: kafa46@gmail.com).

doi: 10.18178/ijmlc.2020.10.1.917

structure also faces difficulties as a result of the limited network information for SMS due to the highly private nature of SMS activity. S. J. Delany *et al.* summarized possible spam-filtering approaches in [8], whereby a great amount of attention is paid to content-based SMS-spam filtering.

SMS-spam filtering has not been fully explored, and it is challenging to design effective spam filters since it is difficult to collect SMS datasets to analyze their graphical structures. We therefore believe that the use of social networks provides a meaningful solution. In this paper, we explore reasonable methodologies to address the question, "Can we fully exploit the advantages of the nature of social networks to detect SMS spam?" To answer this question, we propose an approach to configure and expand a social-network-based SMS dataset by structural approach. The main contributions of this paper are summarized as follows:

- First, we created a social network for SMS messages and SMS spammers to analyze the characteristics of the network using a real-world dataset and sociology theory. Through our SMS-network-building approach, we provide a framework to build and configure SMS networks as one of the guidelines.
- Secondly, we propose a social network based spam detection approach. We believe that our approach can be the first trial and can serve as a baseline concept to improve social-network-based SMS detection.

The remainder of this paper is organized as follows: We review previous works related to SMS spam-detection methodologies in Section II including content-based and social-network-based approaches; in Section III, we present the manner in which we built the SMS network and tackled the privacy obstacle regarding SMS datasets; in Section IV, we propose our spam detection approach that includes a social-network-based detector and provide possible SMS spam attack (called One2N); in Section V, we explain how the proposed approach works by providing the results of experiments; and Section VI concludes our paper.

II. Related Works

A. Spam Filtering

Much of the existing research on spam filtering has focused on the protection techniques regarding email [14], Twitter [4], [15]-[20], Facebook [21], and the Internet [22] including white and black listings; the digital signature, postage control; address management; collaborative, content-based filtering [23]; and social-network-based filtering. Specifically, most of the spam- or spammer-detection approaches for social networks involve the content-based approach [21].

From email spam to SNS spam, a user's information is treated as the most valuable feature for spam filtering. The Naïve Bayesian filter and SVM (Support Vector Machine) are popular approaches in spam-filtering research, as they are common, well-known machine-learning algorithms and have shown a superior performance compared to other approaches.

The authors of [15] suggested graph-based features such as the in-degree, out-degree, and user-reputation level for a micro-blogging service like Twitter that has content-based features such as duplicate tweets, HTTP links, replies and mentions, and topics. For the online voting systems, Benevenuto *et al.* explored YouTube.com to detect spammers who try to increase the reputations of malicious movies by posting a series of responses, and they exploited video attributes (ratings), user attributes (activities), and social-network metrics (clustering coefficient and betweenness) [24]. To enhance the performance of spam detection, several approaches build social-network-based approaches on top of content-based schemes [14, 25, 26]. Using the network spam-filter features (in- and out-link, cross-link, etc.) from 12 million Web pages, the authors of [22] tested various network features for an improved classification performance.

However, the previously mentioned social-network-based approaches, unlike our trial, do not address SMS-spam filtering at all.

B. SMS-Spam Filtering

SMS-spam filtering is a relatively new task that inherits many issues and solutions from email-spam filtering; however, it poses its own specific challenges due to the brief length of the messages. The Naive Bayesian's algorithm, pattern-matching algorithms, evolutionary algorithms, Logistic Regression (LR), Dynamic Markov Compression (DMC), and SVM, among others, can be used in the SMS-spam-detection field, but traditional content-based filters may have their performance seriously degraded while the level of ambiguity is increased. Since SMS messages are fairly short with only 160 characters and their text is generally rife with idioms and abbreviations [6], it is difficult to adopt traditional email-spam filters without any kind of modification.

The authors of [9] first studied the possibility of applying Bayesian filtering techniques to the problem of SMS-spam filtering, whereby the Bayesian filtering techniques that are used to block email spam were extended. Qian Xu *et al.* also utilized SVM-classifier and *k-nearest-neighbor* (k-NN) algorithms with content-less features for SMS-spam detection. They show that temporal features and network features including the number of recipients and the CC can be effective compared to conventional static features [10].

Ref. [27] considered the problem of content-based spam filtering, whereby the technique checks enough features in short spam messages (i.e., mobile (SMS) communication, blog comments, and email-summary information) to distinguish them from non-spam messages in a low bandwidth client. Their purpose is to examine the transferability of successful email filtering techniques to very short messages.

Liu and Wang first considered an effective online SMS-spam filtering application based on each individual classifier with the same weight; however, the authors partially used Chinese SMS volunteers [28], and they extracted email-body text to split it into sentences for pseudo SMS (PSMS) collection. Ningning Wu *et al.*, implemented mobile, parallel real-time monitoring and filtering with a multi-core software platform for SMS. They combined Pinyin Fuzzed Keyword Matching Technology with a dynamic adjustment of the user's credit grade based on the keyword dictionary of Bayesian Learning [29].

III. Construction of SMS Network

A. How to Overcome the Difficulty of SMS Networks

Unlike OSNs like Twitter and Facebook, SMS messages have the following two key differences [7]: (i) SMS is typically a private communication between two (or more than two) persons who trust each other. (ii) Although SMS and Twitter messages ("tweets") are similar in terms of their message length, SMS messages are more likely to be brief.

Unlike Twitter's open API that provides access to the platform's public messages, SMS communication is highly private. Due to SMS privacy issues, it is difficult to collect datasets from users. One possible approach is to collect SMS messages from volunteers; however, the senders of the volunteers' received messages have not given their consent in this case. A publicly released dataset can therefore only contain those SMS messages sent by the volunteers, which leads only restricted message contents and sender-receiver networks.

There are several research studies for which SMS datasets were collected. In our paper, we exploit the SMS network that was gathered and publicly released by National University of Singapore (NUS). The NUS dataset contains 42,140 English and 31,205 Chinese SMS messages from a collection period between 2004 and April 2014; this dataset appeared in [7], [30], [31], but unfortunately, it does not distinguish the spam messages. To explore the possibility of spam detection using social networks, we needed to adopt another dataset for which the spam SMS messages have been clearly classified. We subsequently cover the details of overcoming this obstacle in a step-by-step manner.

Due to the difficulty of obtaining SMS datasets, we first used the real-world (NUS) dataset as a seed structure for constructing an SMS-message network using social-network theories that are as realistic as possible. We believe that the proposed artificial construction of an SMS network is one of the best solutions to explore the unseen structure of the unknown SMS world. From the seed structure, we needed to expand the SMS network; however, we did not have any clues as to what the exact nature of the SMS network was. To tackle this problem, we selected and analyzed the most similar structure among the different social networks. We selected the Twitter dataset since Twitter resembles SMS technology in terms of message length. In summary, we generated SMS networks according to the following steps:

Step 1. Select a baseline network:

Select one real-world SMS dataset (NUS dataset in this paper) as a seed network (structure). The seed network is required to expand its network size (the number of nodes and edges) according to network-expansion rules.

Step 2. Analyze a reference network:

Analyze a known message-exchange network as a reference network to expand the seed network. We selected a Twitter message network as the reference network due to the commonality regarding the message-length limit. We derived the expansion rules from analyzing the reference network. In this paper, we use the power law exponent as an expansion rule.

Step 3. Expand the baseline network:

Expand the SMS network by exploiting the characteristics of the reference network.

We elaborated on the baseline SMS networks by using the details in the following three sub-sections.

B. Selecting a Baseline Network (Step 1)

As we discussed in the previous sub-section, we selected the NUS dataset as our seed network. In terms of basic characteristics, the NUS dataset contains 51,654 English SMS messages with the corresponding time stamp, country, phone model, source ID, destination ID, message body (text), and message profile. We selected and gathered the information regarding the source ID, destination ID, and message body, as these data are essential for the construction of our baseline SMS network; we filtered out the messages without a source ID. For brevity, let the source ID, destination ID, and message body be *sender*, *receiver*, and *text*, respectively, in the remainder of this paper. Lastly, we extracted the sender, receiver, and text from the original NUS dataset, resulting in 40,077 messages comprised of 60 senders and 2,409 receivers.

C. Analyzing a Reference Network (Step 2)

Since we do not know the complete structure of the SMS social network, and given that a sound term representation is one of the most important parts, we need to accept that SMS messages do not have the same structure and characteristics as those of email or other previous short-message formats; therefore, we first analyzed the Twitter network including spam messages.

In terms of the shared message-length brevity between Twitter and SMS, the character limitations of both are 140 and 160, respectively [7]; we selected the Twitter dataset because of this similarity. In our paper, we focus on the characteristics of an expanded SMS network that met the following two conditions: (i) A large and popular social network that embeds a function of the message exchange and contain a portion of spam messages. (ii) Similarity with the large and popular social networks to reflect the real world as much as possible. Lastly, we believe that the Twitter social network is one of the clues for inferring an SMS network through an analysis of the network characteristics.

We choose a Twitter dataset (http://twitter.mpi-sws.org/links-anon.txt.gz) for use in this paper that was generated by M. Cha *et al*. and contains 1,963,263,821 social links [17]. With reference to SMS spam, the list of spammers in the Twitter dataset was provided by S. Ghosh *et al*. in [18] and contains 41,352 spammer accounts; also, Kwak *et al*. conducted a quantitative study with a very large Twitter network (41.7 million users, 1.47 billion social links, and 106 million tweets) [19]. Java *et al.* showed that the out-degree exponent of their Twitter dataset is 2.4, and that OSNs and human-contact networks are "scale-free networks" that show a "small-world phenomenon" [20]. It has been proven that social links (degree distribution) follow a power-law distribution [32]-[34]. Additionally, Meng Jiang *et al.* focused on Twitter attacks in [35], whereby they searched for groups of accounts (spammers) that were used to unfairly bolster the popularity of their customers.

D. Expanding the Baseline Network (Step 3)

Using the baseline network (NUS dataset), we generated a unidirectional social link if an SMS record existed between a sender and receiver (refer to the upper-left graph in Fig. 1)

Since the baseline network is not enough to reflect the complete nature of the entire SMS network, we expanded the baseline network. From Step 2 (“Analyzing a reference network”), we choose the value of the power law exponent as our expansion rule.

Since we only have sender messages from the research volunteers, the generation of the SMS-message network was not relevant. To overcome this shortcoming, however, we exploited the observations from the spammed Twitter network. We expanded the original NUS SMS network by increasing the edges via two methods (random and preferential attachments [34]). In the random attachment, we added edges in the following manner: (i) Randomly choose a number between 0.0 and 1.0. (ii) Select the number of nodes (by looking up Table I) to be connected for each node. (iii) Connect all of the nodes to their selected nodes. From our experiment on the random attachment, 2,586 edges were added. Additionally, we generated edges based on the preferential attachment (PA) model [36]. We set the power law distribution with an exponent of 2.4 since we realized that the out-degree exponent of the Twitter dataset is 2.4 from Step 2, and generated the number of edges for each randomly chosen node, whereby we borrowed the idea of edge generation from [37]. The SMS network generated via the PA model is reported in the upper-right figure of Fig. 1.

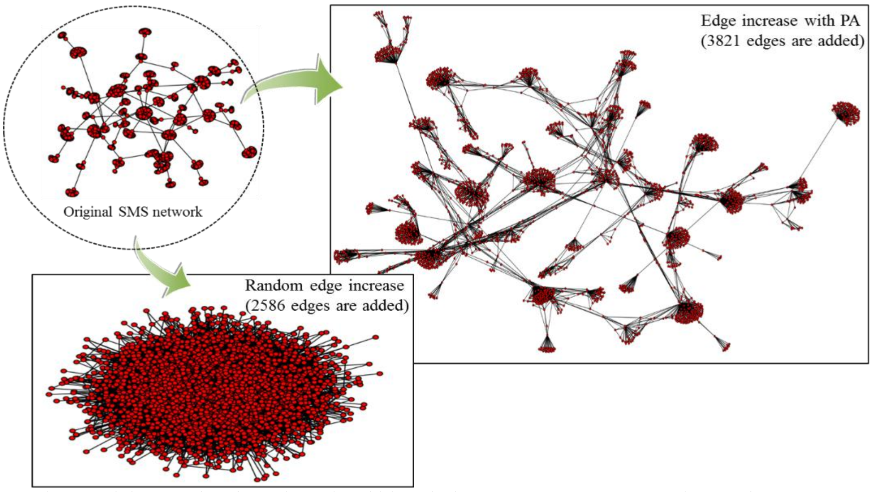

Fig. 1. Twitter social network, where the red and blue circles represent spammers and normal users, respectively.

TABLE I: THE PROBABILITY OF GENERATING THE NUMBER OF EDGES

Prob. with power law exponent (= 2.4)		0.223	0.191	0.161	0.131	0.104	0.079	0.055	0.035	0.017	0.004
No. of edges to be added	PA*	1	2	3	4	5	6	7	8	9	10
	Random	0	0	1	1	2	2	3	3	4	5

*PA: Preferential Attachment is the way of generating networks. In this paper, we followed the network generation using [34]

IV. SPAM DETECTION

A. Detection Metric

To exploit the social-network characteristics, we explored the network metrics. The possible metrics that exist include betweenness centrality (BC), in-degree, and out-degree; BC is given by [38]. Another metric is to represent a graph by using the clustering coefficient (CC). CC is the fraction of the pairs of node *n*'s friends that are connected to each other by edges. In this paper, we use CC as our basic social-network metric since CC is reported as a possible metric in spam-filtering techniques [16], [39]. We leave the exploration of other metrics for our future works.

The CC of the specific node *n* is given by [40] in (1).

$$CC(n) = \frac{2e_n}{deg(n)(deg(n)-1)} \tag{1}$$

where e_n and $deg(n)$ are the number of real edges between the neighbors of node *n* and the number of neighbor edges, respectively.

Therefore, for the global structure analysis, the average CC can be computed as (2).

$$CC_{ave} = \frac{1}{|V|}\sum_{i}^{|V|} CC(i) \tag{2}$$

In this paper, we use CC as our basic social-network metric since *CC* is reported as a possible metric in spam-filtering techniques [15], [23]. We leave the exploration of other metrics for our future works.

B. Spammer Characteristics

Reference [16] founds that spammers have a low CC in an email network because spammers send emails to randomly selected recipients. We believe the finding of [16] that posits that spammers have a lower CC than normal SMS users from adopting social theories such as those of [41]. Since a spammer has less social relations than normal users, the CC of the spammer is also lower than those of normal users.

C. Spam Detection

From using CC values for detecting spam, we devised the detection approach based on the mean and the upper and lower thresholds. After our detection decides that a message is spam and that the corresponding sender is a spammer, it provides an “attack” notice to users. The spam decision rules are as follows:

```
Input:
$\mu$: the mean CC of receivers from a sender
$\gamma$: the mean CC of the rest of the receivers
$\alpha$: the threshold value

Decision:
If $\gamma$ is in the range of $[\mu (1-\alpha), \mu (1+\alpha)]$,
    the messages are normal
    (the sender is a normal message sender).
Otherwise, the messages are spam
    (the sender is a spammer).
```

V. Simulation and Analysis

A. Attack Scenarios

We hold two assumptions regarding the construction of the attack type: (i) If a spammer sends a single message to multiple receivers, the possibility of detection by defenders is greater. (ii) A spammer knows the various spam-detection algorithms (even though nearly all of the detection approaches are only valid for email networks) such as the varying of either the number of SMS messages or the number of spammers. We define a spammer's spam strategy as follows:

1 to N (One2N) spam: A spammer sends SMS spam to N receivers via a sender. The spammer selects N receivers at random and only one type of spam message is sent.

One of the main features of spammers is that they have a large number of message receivers; however, it is also possible for normal users to send a large, or "heavy," SMS load. For instance, the organizer of a business conference will send a large number of SMS messages to the attendee list. In this case, the organizer's behavior is similar to that of a spammer in terms of SMS-message quantity. We applied the term "normal heavy sender" (NHS) for this type of non-spam heavy message sender who has many receivers.

Let the NHS set be n^h, so that $n^h = \{n_i \mid n_i \geq 100\}$, where n_i is the number of the edges of node n. We assign the level of randomness using R and it is defined as follows:

R = a ratio allocating the fraction of the receiver's sent-message number from n^h.

Let the set of randomly selected receivers be n^r. Let the total number of nodes in the SMS be N, and let the number of receiver nodes from n^h be $\left|n^h\right|$; for example, if R = 0.1, the number of randomly selected receivers is $\left\|\left|n^h\right| \times R\right\|$, where $\|\cdots\|$ is the nearest integer function. The number of $\left\|\left|n^h\right| \times R\right\|$ nodes among all of the receiver nodes is substituted by n^r.

B. Experiments on One2N attack

An example of a One2N attack is portrayed in Fig. 3. The color coding follows Table II, and these color rules are applied to all graphical representations of the attack scenario (One2N). To compare a situation wherein normal messages are sent from NHSs, we generated a graph where the number of NHS = 1 and R = 1.0. As we can see from Fig. 2 and Fig. 3, the forming patterns of the edges are different from each other, whereby One2N attacks form edges into different local communities; however, the NHS edges belong to one community that an NHS belongs to as well. In other words, NHSs send SMSs to known people; spammer send messages to unknown members from various communities.

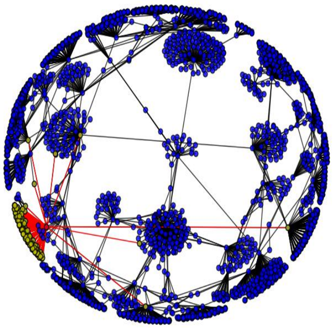

Fig. 2. Example of HNS where randomness = 1.0, NHS no. = 1, receiver no. = 139, and no. of other local NHS-connected communities = 6.

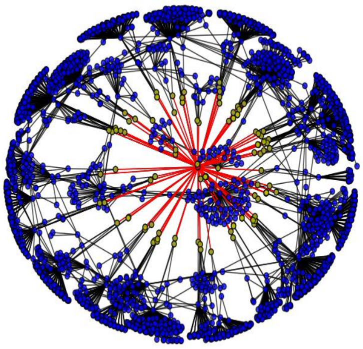

Fig. 3. Graphical representation of One2N attack where receivers = 100.

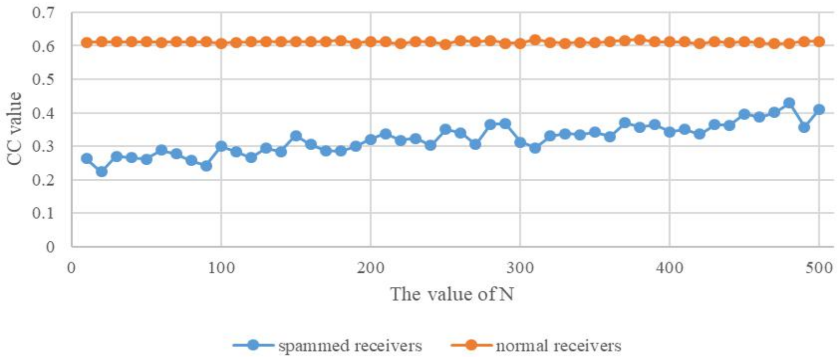

Fig. 4. Averaged CC distribution for varying N under One2N attack.

We conducted experiments with 8 HNSs whose neighbor (receiver) numbers are greater than or equal to 50. Our spam detection rule (SDR) classified all of the 8 NHSs as normal nodes with $\alpha = 0.35$. Note that α is the controlling parameter that indicates how much variation can be allowed around the mean value of the non-spamming receivers (refer to Section IV-C).

To monitor the robustness of SDR on spam attacks, we simulated the One2N attack using different N values, where $10 \leq N \leq 500$ and the interval resolution is 10; note that N represents the number of spammed receivers. We calculated the average CCs of the spammed nodes and normal nodes, and the average results are 0.323 for the former and 0.612 for the latter. The averaged CC distribution of the One2N attack is portrayed in Fig. 4. As we can see in Fig. 4, the CC values that sent spam to receivers from one spammer are increased as N grows. However, the CC values of the normal receivers are stable. The SDR identified all of the One2N cases as attacks regardless of the N value.

VI. Conclusions

From the outset of this study, we continuously tried to answer the question, "Can we fully exploit the advantages of the nature of social networks to detect SMS spam?" To answer our question, we proposed an approach for generating a reasonable social network to test SMS-spam detectors. We also proposed the social-network-based SMS-spam-detection approach; additionally, we introduced possible type of SMS-spam attack (called One2N) that include the random nature of spammers. After simulation using social network-based spam detection against spam attacks with various number of receivers, our approach can detect all spam messages. Therefore, we argue that the answer to our previously mentioned question is "Yes," since spam detection is notable and meaningful enough to be compared under normal conditions.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Giseop Noh conducted all research, writing the paper, analyzed results, and had approved the final version.

Acknowledgment

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. NRF-2018R1C1B5083091).

References

[1] ITU. (April 25, 2014). *The World in 2010: ICT Facts and Figures*. [Online]. Available: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2010

[2] T. Almeida, J. M. G. Hidalgo, and T. P. Silva, "Towards sms spam filtering: Results under a new dataset," *International Journal of Information Security Science,* vol. 2, pp. 1-18, 2013.

[3] TextRequest.com. (Oct. 17, 2018). *73 Texting Statistics That Answer All Your Questions*. [Online]. Available: https://www.textrequest.com/blog/texting-statistics-answer-questions/

[4] R. Munro and C. D. Manning, "Short message communications: users, topics, and in-language processing," in *Proc. the 2nd ACM Symposium on Computing for Development*, 2012, p. 4.

[5] T. M. Mahmoud and A. M. Mahfouz, "SMS spam filtering technique based on artificial immune system," *International Journal of Computer Science Issues (IJCSI),* vol. 9, 2012.

[6] T. A. Almeida, J. M. G. Hidalgo, and A. Yamakami, "Contributions to the study of SMS spam filtering: new collection and results," in *Proc. the 11th ACM symposium on Document engineering*, 2011, pp. 259-262.

[7] T. Chen and M.-Y. Kan, "Creating a live, public short message service corpus: The NUS SMS corpus," *Language Resources and Evaluation,* vol. 47, pp. 299-335, 2013.

[8] S. J. Delany, M. Buckley, and D. Greene, "SMS spam filtering: Methods and data," *Expert Systems with Applications,* vol. 39, pp. 9899-9908, 2012.

[9] J. M. Gómez Hidalgo, G. C. Bringas, E. P. Sánz, and F. C. García, "Content based SMS spam filtering," in *Proc. the 2006 ACM symposium on Document engineering*, 2006, pp. 107-114.

[10] Q. Xu, E. W. Xiang, Q. Yang, J. Du, and J. Zhong, "Sms spam detection using noncontent features," *IEEE Intelligent Systems,* pp. 44-51, 2012.

[11] I. Androutsopoulos, J. Koutsias, K. V. Chandrinos, and C. D. Spyropoulos, "An experimental comparison of naive Bayesian and keyword-based anti-spam filtering with personal e-mail messages," in *Proc. the 23rd Annual International ACM SIGIR Conference on Research and Development in Information Retrieval*, 2000, pp. 160-167.

[12] A. Bratko, B. Filipič, G. V. Cormack, T. R. Lynam, and B. Zupan, "Spam filtering using statistical data compression models," *The Journal of Machine Learning Research,* vol. 7, pp. 2673-2698, 2006.

[13] V. Metsis, I. Androutsopoulos, and G. Paliouras, "Spam filtering with naive bayes-which naive bayes?" in *Proc. CEAS*, 2006, pp. 27-28.

[14] F. Li and M.-H. Hsieh, "An empirical study of clustering behavior of spammers and group-based anti-spam strategies," in *Proc. CEAS*, 2006.

[15] A. H. Wang, "Don't follow me: Spam detection in twitter," in *Proc. the 2010 International Conference on Security and Cryptography (SECRYPT)*, 2010, pp. 1-10.

[16] P. Oscar and V. Roychowdbury, "Leveraging social networks to fight spam," *IEEE Computer,* vol. 38, pp. 61-68, 2005.

[17] M. Cha, H. Haddadi, F. Benevenuto, and P. K. Gummadi, "Measuring user influence in twitter: the million follower fallacy," *ICWSM,* vol. 10, pp. 10-17, 2010.

[18] S. Ghosh, B. Viswanath, F. Kooti, N. K. Sharma, G. Korlam, F. Benevenuto *et al.*, "Understanding and combating link farming in the twitter social network," in *Proc. the 21st International Conference on World Wide Web*, 2012, pp. 61-70.

[19] H. Kwak, C. Lee, H. Park, and S. Moon, "What is Twitter, a social network or a news media?" in *Proc. the 19th International Conference on World Wide Web*, 2010, pp. 591-600.

[20] A. Java, X. Song, T. Finin, and B. Tseng, "Why we twitter: understanding microblogging usage and communities," in *Proc. the 9th WebKDD and 1st SNA-KDD 2007 Workshop on Web Mining and Social Network Analysis*, 2007, pp. 56-65.

[21] S. Y. Bhat and M. Abulaish, "Community-based features for identifying spammers in online social networks," in *Proc. the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, 2013, pp. 100-107.

[22] Q. Gan and T. Suel, "Improving web spam classifiers using link structure," in *Proc. the 3rd International Workshop on Adversarial Information Retrieval on the web*, 2007, pp. 17-20.

[23] J. W. Yoon, H. Kim, and J. H. Huh, "Hybrid spam filtering for mobile communication," *Computers & Security,* vol. 29, pp. 446-459, 2010.

[24] F. Benevenuto, T. Rodrigues, V. Almeida, J. Almeida, and M. Gonçalves, "Detecting spammers and content promoters in online video social networks, in *Proc. the 32nd international ACM SIGIR Conference on Research and Development in Information Retrieval*, 2009, pp. 620-627.

[25] F. J. Ortega, C. Macdonald, J. A. Troyano, and F. Cruz, "Spam detection with a content-based random-walk algorithm," in *Proc. the 2nd International Workshop on Search and Mining User-Generated Contents*, 2010, pp. 45-52.

[26] C. Castillo, D. Donato, A. Gionis, V. Murdock, and F. Silvestri, "Know your neighbors: Web spam detection using the web topology," in *Proc. the 30th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval*, 2007, pp. 423-430.

[27] G. V. Cormack, J. M. Gómez Hidalgo, and E. P. Sánz, "Spam filtering for short messages," in *Proc. the Sixteenth ACM Conference on Information and Knowledge Management*, 2007, pp. 313-320.

[28] W. Liu and T. Wang, "Index-based online text classification for sms spam filtering," *Journal of Computers,* vol. 5, pp. 844-851, 2010.

[29] N. Wu, M. Wu, and S. Chen, "Real-time monitoring and filtering system for mobile SMS," in *Proc. ICIEA 2008. 3rd IEEE Conference on Industrial Electronics and Applications*, 2008, pp. 1319-1324.

[30] H. Y. Jue, "Analysis of SMS efficiency," PhD Thesis National University of Singapore, 2004.

[31] C. Bach and J. Gunnarsson, "Extraction of trends is SMS text," Master's thesis, Lund University, 2010.

[32] A. Broder, R. Kumar, F. Maghoul, P. Raghavan, S. Rajagopalan, R. Stata *et al.*, "Graph structure in the web," *Computer Networks,* vol. 33, pp. 309-320, 2000.

[33] R. Kumar, P. Raghavan, S. Rajagopalan, and A. Tomkins, "Trawling the web for emerging cyber-communities," *Computer Networks*, vol. 31, pp. 1481-1493, 1999.

[34] X. Shi, B. Tseng, and L. Adamic, "Looking at the blogosphere topology through different lenses," *Ann Arbor*, vol. 1001, p. 48109, 2007.

[35] M. Jiang, P. Cui, A. Beutel, C. Faloutsos, and S. Yang, "CatchSync: catching synchronized behavior in large directed graphs," in *Proc. the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2014, pp. 941-950.

[36] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, pp. 509-512, 1999.

[37] H.-Y. Lam and D.-Y. Yeung, *A Learning Approach to Spam Detection Based on Social Networks*, Hong Kong University of Science and Technology, 2007.

[38] Y. Boshmaf, K. Beznosov, and M. Ripeanu, "Graph-based Sybil detection in social and information systems," in *Proc. the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, 2013, pp. 466-473.

[39] P. O. Boykin and V. Roychowdhury, "Personal email networks: An effective anti-spam tool," *arXiv preprint cond-mat/0402143,* 2004.

[40] P. G. Lind, M. C. Gonzalez, and H. J. Herrmann, "Cycles and clustering in bipartite networks," *Physical Review E,* vol. 72, p. 056127, 2005.

[41] M. McPherson, L. Smith-Lovin, and J. M. Cook, "Birds of a feather: Homophily in social networks," *Annual Review of Sociology*, pp. 415-444, 2001.

Giseop Noh is currently working as an assistant professor in the Department of Software Convergence, College of Engineering, Cheongju University. He received his B.E. in industrial engineering, R.O.K Air Force Academy, M.S. in computer science from University of Colorado, and Ph.D in electrical & computer engineering from Seoul National University. His current research interests are recommender systems, social network analysis, and information life cycle analysis.