Neurocomputing 159 (2015) 27–34

Contents lists available at ScienceDirect

Neurocomputing

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

Detecting spammers on social networks

Xianghan Zheng [a,b], Zhipeng Zeng [a,b], Zheyi Chen [c], Yuanlong Yu [a,b,*], Chunming Rong [d]

[a] College of Mathematics and Computer Science, Fuzhou University, Fuzhou, China
[b] Fujian Key Laboratory of Network Computing and Intelligent Information Processing, Fuzhou, China
[c] Department of Computer Science, QingHua University, Beijing, China
[d] Department of Computer Science and Electronic Engineering, University of Stavanger, Stavanger, Norway

ARTICLE INFO

Article history:
Received 10 September 2014
Received in revised form
26 November 2014
Accepted 8 February 2015
Communicated by Huaping Liu
Available online 24 February 2015

Keywords:
Social network
Spammer
Machine learning
Support vector machine

ABSTRACT

Social network has become a very popular way for internet users to communicate and interact online. Users spend plenty of time on famous social networks (e.g., Facebook, Twitter, Sina Weibo, etc.), reading news, discussing events and posting messages. Unfortunately, this popularity also attracts a significant amount of spammers who continuously expose malicious behavior (e.g., post messages containing commercial URLs, following a larger amount of users, etc.), leading to great misunderstanding and inconvenience on users' social activities. In this paper, a supervised machine learning based solution is proposed for an effective spammer detection. The main procedure of the work is: first, collect a dataset from Sina Weibo including 30,116 users and more than 16 million messages. Then, construct a labeled dataset of users and manually classify users into spammers and non-spammers. Afterwards, extract a set of feature from message content and users' social behavior, and apply into SVM (Support Vector Machines) based spammer detection algorithm. The experiment shows that the proposed solution is capable to provide excellent performance with true positive rate of spammers and non-spammers reaching 99.1% and 99.9% respectively.

1. Introduction

Within the past few years, online social network, such as Facebook, Twitter, Weibo, etc., has become one of the major way for internet users to keep communications with their friends [1–3]. According to Statista report [4], the number of social network users has reached 1.61 billion until late 2013, and is estimated to be around 2.33 billion users globe, until the end of 2017.

However, along with great technical and commercial success, social network platform also provides a large amount of opportunities for broadcasting spammers, which spreads malicious messages and behavior. According to Nexgate's report [5], during the first half of 2013, the growth of social spam has been 355%, much faster than the growth rate of accounts and messages on most branded social networks.

The impact of social spam is already significant. A social spam message is potentially seen by all the followers and recipients' friends. Even worse, it might cause misdirection and misunderstanding in public and trending topic discussions. For example, trending topics are always abused by spammers to publish comments with URLs, misdirecting all kinds of users to completely unrelated websites. Because most social networks provide shorten service on URLs inside message, it is difficult to identify the content without visiting the site.

There has been a few proposals from industry and academia, discussing possible solutions for spam detection and filtering (described in Section 2). However, they are either ineffective or based on too much considered conditions (e.g., a lot of content and behavior feature, etc.). This paper investigates social spammer content and behavior issues, and proposes an effective machine learning model for spammer detection. The paper contains the following four main contributions:

- The paper adopts the spammer feature to detect spammer and test the results over Sina Weibo, the biggest social network site in China. Under the Weibo API, a specific dataset crawler is developed to extract any unauthorized users' public messages inside the Weibo platform. This is the first step for data analysis.
- The major novelty of the paper is to study a set of most important features related to message content and user behavior and apply them on the SVM based classification algorithm for spammer detection. The experiment and comparison work shows that the proposed solution enables to provide higher accuracy.
- Through feature selection algorithms and experiment testing, ten most important feature and the weight of these feature are identified. The experiment results further validate the selected

* Corresponding author.

http://dx.doi.org/10.1016/j.neucom.2015.02.047

spammer feature (manually classified) and also explain why the proposed solution could achieve excellent performance.
- The paper also develops a prototype software that is capable to distinguish any Weibo user (spammer or non-spammer). With friendly user interface, efficient and accurate classification result, ordinary users are capable to distinguish any Weibo users with simple operation. The software has been published in Sourceforge [6].

It should be mentioned that although the proposed approach is currently tested specifically in the Sina Weibo social network, it is applicable to all other existing social sites (e.g., Twitter, Facebook, etc.) with few revisions. The rest of the paper is organized as follows. Section 2 presents the background of the Weibo social network and displays some related works about spammer detection. Section 3 introduces the method how we collect the dataset and extract feature. Section 4 describes the spammer detection model, experiments and corresponding evaluation. Finally, the conclusion and future works are given in Section 5.

2. Releated works

2.1. The Sina Weibo social network

According to [3], the number of Sina Weibo site users has reached over 500 million. Statistics show that Weibo is consistently among the top 25 most frequently visited websites during the past few years [7]. As one of the largest social networks in China, Weibo attracts millions of users online every day.

Weibo application is similar to Twitter, where users post messages, interact with friends, talk about news and share interesting topics via social network services. It is designed as a microblogging website where users post short messages no more than 140 characters. The posted messages will be delivered to followers immediately. Each user is identified by a unique username and could start following another user in order to receive friends' latest messages on homepage. The user who is followed could either accept the request to follow back, or just reject. Fig. 1 describes a simple following graph, in which user A is following user B, and user B and user C are following each other.

There are a number of expressions in Weibo, allowing users to interact with others in a better way, including mention, repost and hashtag.

2.1.1. Mention

A Weibo message containing a series of keywords like @username, meaning that the message sender is willing to share something with the user mentioned. As a consequence, Weibo will automatically notify the user mentioned with the message in his/her homepage.

Example: @Bob wann'a go for a coffee?

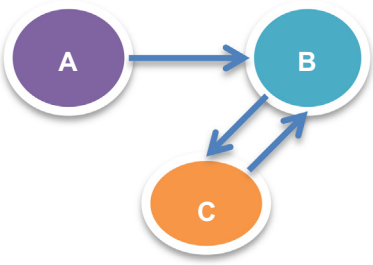

Fig. 1. A simple following graph.

2.1.2. Repost

Repost is another way to send message. User always reposts the other users' message that is interested. The reposted message will also be received by the user's followers.

2.1.3. Hashtag

Weibo users could post message containing hashtags () to identify a specific topic. If enough users pick up this topic, it will appear in the list of trending topics.

Example: happy birthday to Alice hello Alice.

2.2. Existing research

In the past ten years, email spam detection and filtering mechanisms have been widely implemented. The main work could be summarized into two categories: the content-based model and the identity-based model. In the first model, a series of machine learning approaches [8,9] are implemented for content parsing according to the keywords and patterns that are spam potential. In the identity-based model, the most commonly used approach is that each user maintains a whitelist and a blacklist of email addresses that should and should not be blocked by anti-spam mechanism [10,11]. More recent work is to leverage social network into email spam identification according to the Bayesian probability [12]. The concept is to use social relationship between sender and receiver to decide closeness and trust value, and then increase or decrease Bayesian probability according to these value.

With the rapid development of social networks, social spam has attracted a lot of attention from both industry and academia. In industry, Facebook proposes an EdgeRank algorithm [13] that assigns each post with a score generated from a few feature (e.g., number of likes, number of comments, number of reposts, etc.). Therefore, the higher EdgeRank score, the less possibility to be a spammer. The disadvantage of this approach is that spammers could join their networks and continuously like and comment each other in order to achieve a high EdgeRank score.

In academia, Yardi et al. [14] studies the behavior of a small part of spammers in Twitter, and find that the behavior of spammers is different from legitimate users in the field of posting tweets, followers, following friends and so on. Stringhini et al. [15] further investigates spammer feature via creating a number of honey-profiles in three large social network sites (Facebook, Twitter and Myspace) and identifies five common features (followee-to-follower, URL ratio, message similarity, message sent, friend number, etc.) potential for spammer detection. However, although both of two approaches introduce convincible framework for spammer detection, they lack of detailed approaches specification and prototype evaluation.

Wang [16] proposes a naïve Bayesian based spammer classification algorithm to distinguish suspicious behavior from normal ones in Twitter, with the precision result (*F*-measure value) of 89%. Gao et al. [17] adopts a set of novel feature for effectively reconstructing spam messages into campaigns rather than examining them individually (with precision value over 80%). The disadvantage of these two approaches is that they are not precise enough.

Benevenuto et al. [18] collects a large dataset from Twitter and identify 62 feature related to tweet content and user social behavior. These characteristics are regarded as attributes in a machine learning process for classifying users as either spammers or non-spammers. Zhu et al. [19] proposes a matrix factorization based spam classification model to collaboratively induce a succinct set of latent feature (over 1000 items) learned through social relationship for each user in RenRen site (www.renren.com). However, these two approaches are based on a large amount of selected feature that might consume heavy computing capability and spend much time in model training.

In Sina Weibo field, literature [20] investigates three types of spammer behavior (aggressive advertisement, duplicate reposting and aggressive following) and extracts three separated sets of feature. Different from the main approach with all feature used by one spammer classifier, this proposal is based on a group of classifiers, each using three generated feature sets and working jointly as a spammer classifier to detect spammer. The concept of combining several spamming classifiers together is expected to improve detection performance. However, because that each separated feature set might not contain enough feature items (8 at most), the computation result might be inaccurate (precise rate reaches only 82.06%).

Generally, this paper follows similar concept with previous works, however, with a few distinguished points:

1. Our proposed SVM-based classification model considers only 18 feature items and achieve the best performance result, with *F*-measure value reaching over 99%. This is the best result ever achieved (although different collected datasets with different contents might cause a bit deviation in result computation, a big improvement of result is still comparable and significant).
2. The importance of each selected feature is studied and verified through the Weka [21], a data mining software upon Java tool. The combination usage of these feature also explains why the proposed approach is capable to achieve much higher precision rate than other existing works.
3. Instead of pure experiment upon specific dataset, a prototype software is specifically developed and opened for public usage, helping any user to distinguish spammer on the Sina Weibo network environment. The accuracy of prototype further proves the efficiency of proposed solution.

3. Dataset collection and analysis

3.1. Dataset and feature collection

Similar as most social media platforms, the public Weibo developer API (specifically, user_timeline API) only provides the downloading functionality on the recent messages of authorized users. This is considered as an obstacle to the process of data collection. To solve this problem, specific data crawler and feature collection mechanism are developed, as described in the following steps (see Fig. 2):

1. 100 normal users (from celebrity, company, and government that post/repost/comment frequently) and 50 spammer users (who expose malicious behavior frequently) are manually selected as data source.
2. Two types of data crawlers are developed for ordinary user and spammer respectively. The ordinary user crawler is for extracting normal user's list of followees, which are also considered as normal users because most of the normal users are unlikely to follow spammers in reality (also validated through analysis in Section 3.2.2); spammer crawler is for extracting the list of spammers behind spammers' specific reposted messages. Finally, 30,116 Weibo users are extracted.
3. For each user, we crawl corresponding information inside 500 recent messages, with Step1: the basic user information (e.g., the number of followees, number of followers, created days, etc.) could be achieved via Weibo API; Step 2: through the username, it is capable to crawl a set of message ID, through which the message attributes (e.g., the number of reposts, the number of comments, the number of likes, etc.) could be obtained with help of the Weibo API. Finally, more than 16 million messages are crawled from 25th, Feb, 2014 to 1st, May, 2014.

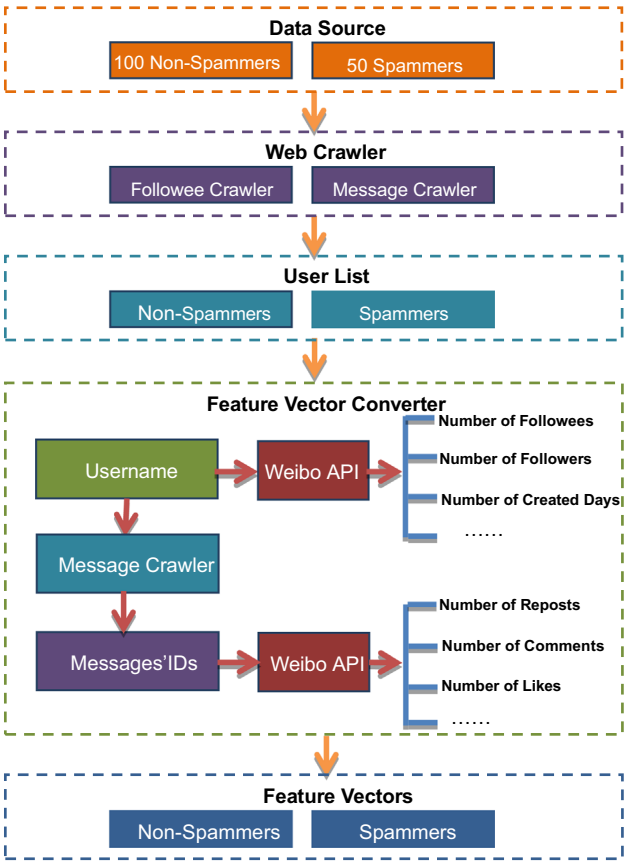

Fig. 2. Dataset and feature collection procedure.

4. For each user, a feature vector is constructed according to crawled user and message information described above.

After that, our work labels collected users as spammers or non-spammers. We develop a mechanism to help three volunteers analyze each collected user manually and independently based on the recent messages. The majority voting is introduced to decide which class the user belongs to if one user is labeled to different classes. However, a user labeling process depends on human judgment, and might lead to inevitable human error. Therefore, we ignore and discard the users whose class is difficult to decide. In total, 11488 spammers and 17646 non-spammers are labeled. Finally, 80% spammers and non-spammers from labeled dataset are randomly selected as the training data, leaving the rest as testing data.

3.2. Feature analysis

Unlike normal Weibo users, spammers usually aim at the commercial intent such as advertisement spreading. In this section, we analyze the difference between spammers and non-spammers from both content and behavior point of view according to dataset collected.

3.2.1. Content-based feature

From Dataset, we randomly select 300 spam and 300 non-spam messages, each of which assigned by a random integer identity value ranged from 1 to 300. Besides, the maximum number of reposts, comments and likes is set to 100.

From statistics point of view, three most obvious and important featuresof spam messages could be achieved. Fig. 3(a) shows the repost number distribution, inside which more than 90% of spam messages have a repost counts lower than 10. Similarly, the number of

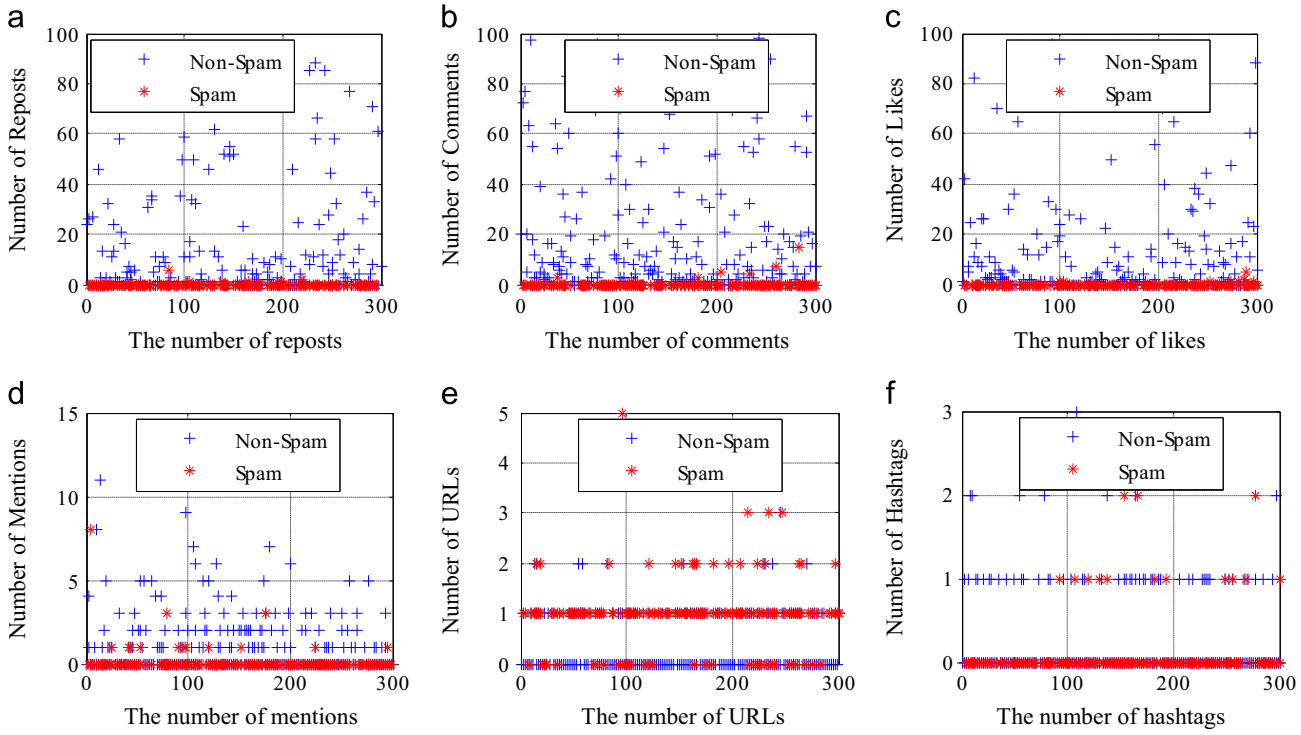

Fig. 3. Distribution of content-based feature.

comments and likes is also quite small, as shown in Fig. 3(b) and (c). This may be explained that most normal users pay litter attention to spam messages.

Fig. 3(d) indicates the number of mentions in each message. As expected, most spam messages do not contain any mention because most spammers only aim at advertising, and spend few time on interacting with other users. Fig. 3(e) indicates that most spams contain at least one URLs linking to advertisement pages. The number of hashtags analyzed in Fig. 3(f) shows that spammers sometimes post messages so as to be retrieved by search engine.

3.2.2. *User-based feature*

In the following, cumulative distribution function (CDF) is introduced to study the feature of spammers, as shown in Fig. 4.

Fig. 4(a) analyzes the number of followees for each user. Normally, spammers try to follow a multitude of legitimate users so as to be followed back. However, it does not work for most time, as shown in Fig. 4(b). This type of behavior makes the fraction of followees per followers very large in comparison with non-spammers, as illustrated in Fig. 4(c).

Analysis in the number of created days (See Fig. 4(d)) indicates that spammers have to create new accounts frequently. This might be because of anti-spam mechanism that would eventually detect and automatically clean spammer accounts.

After that, the fraction of messages per day is illustrated in Fig. 4(e). Spammer accounts usually act as a “Robot” to post messages automatically. After calculating the average number of messages per day for both spammers and non-spammers, it is found that the number of messages posted by spammers per day is approximately three times higher than non-spammers (with mean value of spammers and non-spammer 15.19 and 3.62 respectively).

Finally, Fig. 4(f) analyzes the number of average URLs in each user's recent messages. It shows that most spammers have at least one URL in each message. However, the result indicates that some normal users also include URLs in many of their messages. After manually checking, the reason is that some companies create official accounts to promote their products with URLs linking to specific websites.

4. Spammer detection

Based on dataset and feature collection described in the previous section, a supervised machine learning model is introduced for spammers identification. Supervised learning [22] is the machine learning task of inferring a function from labeled training data that consists of a set of training examples. Inside supervised learning, each example is a pair consisting of an input object (typically a vector) and a desired output value (also called supervisory signal). Through analysis of the training data, supervised learning solution produces a classification model for predicting new examples.

4.1. *SVM based spammer detection model*

Fig. 5 illustrates the basic concept of proposed spammer detection model. In this solution, training data is converted to a series of feature vectors that consist of a set of values for attributes. These vectors construct the input of supervised machine learning algorithm. After training, a classification model is applied to distinguish whether the specific user belongs to normal user or spammer.

Because spammers and non-spammers have different social behavior, through analyzing content feature and user behavior, it is capable to distinguish abnormal behavior from legitimate ones. In this paper, we set 18 feature listed in the following: the number of followees, the number of followers, the number of messages, the number of friends following each other, the number of favorites, the number of created days, fraction of followees per followers, fraction of original messages, number of messages per day, the average number of reposts, the average number of comments, average number of likes, the average number of URLs, the average number of pictures, the average number of hashtags, the average number of user mentioned, fraction of messages containing URLs, fraction of messages containing pictures.

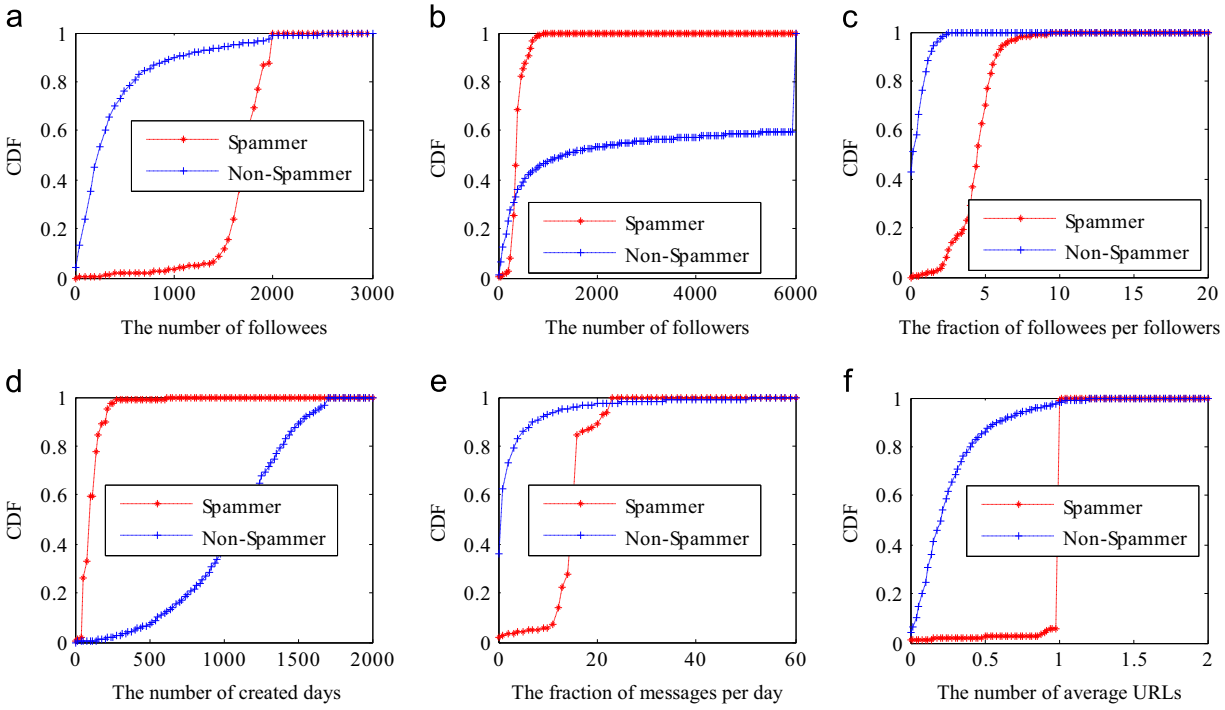

Fig. 4. Cumulative distribution function of user-based feature.

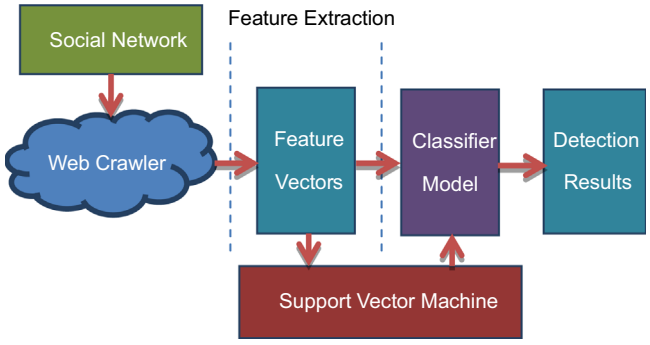

Fig. 5. Overview of spammer detection model.

4.2. SVM classifier

The spammer detection solution is based on a non-linear support vector machine (SVM) classifier [23] with the Radial Basis Function (RBF) kernel. This could be achieved through the implementation provided by libSVM [24], an integrated software for supporting vector classification, regression and distribution estimation.

The SVM with RBF kernel function has two such training parameters: *C* controls overfitting of the model; and *gamma* controls the degree of nonlinearity. In the experiment, we apply a parameter selection tool provided by libSVM to select parameters automatically with a 5-fold cross-validation. This tool uses grid search policy to find highest classification accuracy through computation from different values of *C* and *gamma* pair. Finally, a most suitable pair that *C* and *gamma* equal with 128 and 0.03125 respectively is generated and selected for our specific training dataset.

4.3. Evaluation metrics

In the evaluation, we consider a confusion matrix illustrated in Table 1, where *a* represents the number of spammers correctly classified, *b* refers to the number of spammers misclassified as non-spammers, *c* expresses the number of non-spammers misclassified as spammers, and *d* is the number of non-spammers correctly classified. According to the confusion matrix, a set of metrics commonly evaluated in machine learning field are introduced: *precision*, *recall* and *F-measure*.

Table 1
Example of confusion matrix.

		Predicted	
		Spammer	Non-spammer
True	Spammer	*a*	*b*
	Non-spammer	*c*	*d*

Precision (P) is the ratio of number of instances correctly classified to the total number of instances and is expressed by formula $P=a/(a+c)$. *Recall* (R) is the ratio of the number of instances correctly classified to the total number of predicted instances and is expressed with formula $R=a/(a+b)$. *F-measure* is the harmonic mean between precision and recall, and is defined as $F=2PR/(P+R)$. For evaluation of classifiers' performance, *F-measure* value is more precise because it is a combination value with summarizing of both precision and recall.

4.4. Ratio of spammer to non-spammer

Firstly, we use complete training dataset for testing work and achieve *F-measure* value of spammer and non-spammer as 91.6% and 93.2% respectively. This might not be the optimized result. In order to achieve higher spammer detection accuracy, the ratio of spammer to non-spammer in the training dataset is changed as follows: 10:1, 8:1, 6:1 4:1, 2:1, 1:2, 1:4, 1:6, 1:8 and 1:10, with corresponding classification accuracy result illustrated in Fig. 6. It shows that *F-measure* value of both spammer and non-spammer grows simultaneously when the ratio of spammer decreases, and reaches the highest accuracy of about 99.5% and 99.9% when the ratio is set to 1:2. After that, the accuracy drops quickly while the ratio of non-spammer rises. On the other hand, it is obvious that an

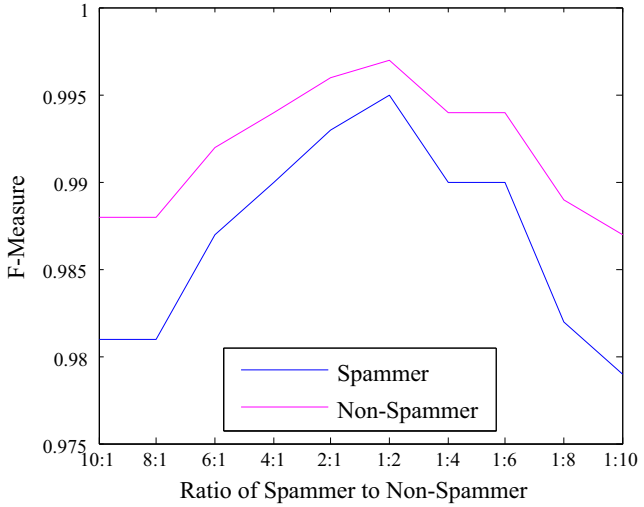

Fig. 6. Classification accuracy with different ratios of spammer to non-spammer in training dataset.

Table 2
Confusion matrix.

		Predicted	
		Spammer	Non-spammer
True	Spammer	99.1%	0.9%
	Non-spammer	0.1%	99.9%

appropriate ratio of spammer to non-spammer is important since a large quantitative difference (i.e. 10:1 or 1:10) would result in lower accuracy. This is because that a large ratio of spammer indicates a large probability to misclassify normal user to spammer, and vice versa. Therefore, in the following experiment, the ratio of spammer to non-spammer is set to be 1:2.

4.5. Classification result and comparison

Table 2 illustrates confusion matrix obtained by SVM classifier. It shows that our proposed solution is quite efficient, with 99.1% spammers and 99.9% non-spammers correctly classified, leaving only a small fraction of spammers and non-spammers misclassified. Table 3 describes the value of evaluation metrics, in which *precision*, *recall* and *F-measure* are calculated for spammer and non-spammer respectively.

Besides, we also compare the proposed approach with other classifiers: Decision Tree, Naïve Bayes and Bayes Network, with implementation provided by Weka. For each classifier, the same evaluation metrics (*precision*, *recall* and *F-measure*) are calculated for both spammers and non-spammers, with the result illustrated in Table 4. It is obvious that SVM classifier is capable to achieve best accuracy. This indicates that the hyperplane calculated by SVM could separate training data into two parts with a maximum margin. Besides, it is shown that the other three classifiers also achieve good accuracy. This is because that the suitable feature (including content and user behavior) selected are capable to distinguish spammers from non-spammers effectively.

4.6. Importance of the attributes and user suggestions

After that, two well-known feature selection methods (information gain and Chi Squared available on Weka) are applied to find the ranking of importance of these selected attributes. Specifically, we evaluate the relative power of each selected attribute and distinguish one user class from the others by applying these two methods respectively. The result listed in Table 5 indicates that the most 10 important attributes taken from the two methods are quite similar.

Additionally, we notice that the top two most important attributes are the number of created days and the average number of comments, which are also easy to be identified from the normal user point of view. These two attributes also highlight the behavior feature that spammers usually create new accounts to avoid being detected, and receive little feedback from legitimate users. Therefore, for normal users, ignore Weibo messages from very new account with little comment could be a good strategy to avoid spam.

Furthermore, we verify the importance of the top 10 attributes via dividing 18 attributes into 10 subsets (each of which represents all attributes minus *i*-th attribute). We calculate *F-measure* value of both spammer and non-spammer inside each subset according to approaches described in Section 4. In Fig. 7, the result indicates that (1) the accuracy result indeed decreases slightly when any attribute is removed; (2) generally (ignore the column of All-10), the more importance of the specific attribute, the less accuracy result will be (See All-1 column for example); (3) the miss of a single attribute does not influence much on result (with the worst accuracy value reaching 98.6%). This could be explained that most spammers are related to multi-feature and could be clearly classified even one important feature is missing.

Table 3
Classification evaluation.

	Precision	Recall	*F*-measure
Spammer	0.999	0.991	0.995
Non-spammer	0.995	0.999	0.997

Table 4
Comparison between SVM and other classifiers.

Classifier	Precision		Recall		*F*-measure	
	Spammer	Non-spammer	Spammer	Non-spammer	Spammer	Non-spammer
SVM	0.999	0.995	0.991	0.999	0.995	0.997
Decision Tree	0.942	0.95	0.953	0.958	0.947	0.954
Naïve Bayes	0.939	0.96	0.922	0.966	0.93	0.963
Bayes Network	0.946	0.915	0.907	0.956	0.926	0.935

4.7. Prototype implementation

Instead of relying only on the experiment of specific training and testing dataset, we further develop a prototype software for the purpose of distinguishing Weibo users in real environment. The work is described in the following steps:

1. Based on developed data crawler, the prototype software contains an user interface that accepts an username or trending topic as input.
2. We randomly select a trending topic, called Jeremy Lin joined the Lakers (initiated in July 25, 2014), which has attracted 2562 participating users by Aug 25, 2014.
3. Each participating user in this topic is analyzed according to content and behavior feature, and classified as spammer or

Table 5
Attributes Ranking list Top 10.

Rank	Information gain	Chi squared
1	Number of created days	Number of created days
2	Average number of comments	Average number of comments
3	Fraction of followees per followers	Average number of URLs
4	Average number of URLs	Fraction of followees per followers
5	Fraction of messages containing URLs	Average number of user mentioned
6	Average number of user mentioned	Fraction of messages containing URLs
7	Fraction of original messages	Average number of pictures
8	Average number of pictures	Fraction of original messages
9	Number of messages per day	Number of messages per day
10	Number of followees	Number of followees

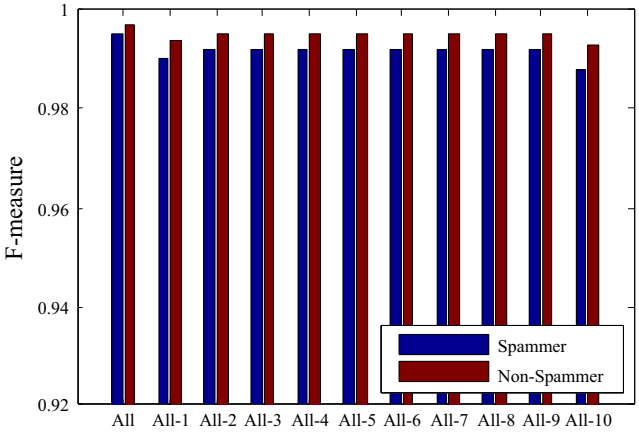

Fig. 7. Classification results with different feature subsets.

Table 6
Spammer detection in trending topic.

Trending topic	Jeremy Lin joined the Lakers
Total users	2562
Detected spammers	14
Real spammer accounts	13
False alarms	1
Accuracy	92.9%

non-spammer based on proposed classification model. Finally, 14 users are labeled as spammer.

4. We analyze these 14 users' recent messages manually and find that 13 users are spammer account, with only one user misclassified (as illustrated in Table 6). The testing result further proves feasibility, efficiency and reliability of our proposed solution. Note that developed software is open for public usage in Sourceforge site.

5. Conclusion and future works

In this paper, we have introduced a machine learning based spammer detection solution for social networks. The solution considers the user's content and behavior feature, and apply them into SVM based algorithm for spammer classification. Through a multitude of analysis, experiment, evaluation and prototype implementation work, we have shown that proposed solution is feasible and is capable to reach much better classification result than the other existing approaches.

However, two open issues are still waiting for urgent answer. On one hand, although the proposed approach could achieve precise classification result, it takes over one hour in a process of model training. Therefore, one open issue includes online spammer detection that contains the capability of real-time data and feature collection, lower training time with high accuracy. Extreme Learning Machine (ELM) [25,26], a new learning scheme of feedforward neural networks that provide much lower training time and similar accuracy, could be one possible solution.

On the other hand, feature extracted in our proposed solution (also existing approaches) is based on statistical analysis and manual selection. However, In the era of big data with huge data volume and convenient access [27], feature extraction mechanism in our solution might be low adaptive and costive. Therefore, how to import the concept of artificial intelligence technology (e.g. deep learning algorithms [28–30]) into automatic feature learning and extraction has become an important question.

Acknowledgments

The authors would like to thank the support of the Technology Innovation Platform Project of Fujian Province under Grant no. 2009J1007, the Program of Fujian Key Project under Grant no. 2013H6011, and the Natural Science Foundation of Fujian Province under Grant no. 2013J01228.

The authors would like to thank Prof. Yuanlong Yu from Fuzhou University for his invaluable expert advice that makes this paper successfully completed.

References

[1] Facebook, ⟨http://www.facebook.com/⟩.
[2] Welcome to Twitter, ⟨http://twitter.com/⟩.
[3] Weibo – SINA, ⟨http://english.sina.com/weibo/⟩.
[4] Statista, ⟨http://www.statista.com/⟩.
[5] Nexgate. 2013 State of Social Media Spam, ⟨http://nexgate.com/wp-content/uploads/2013/09/Nexgate-2013-State-of-Social-Media-Spam-Research-Report.pdf⟩, 2013.
[6] Weibocrawler, ⟨http://weibocrawler.sourceforge.net/⟩.
[7] Alexa Top 500 Global Sites, ⟨http://www.alexa.com/topsites⟩.
[8] M. Uemura, T. Tabata, Design and evaluation of a Bayesian-filter-based image spam filtering method, in: Proceedings of the International Conference on Information Security and Assurance (ISA), IEEE, 2008, pp. 46–51.
[9] B. Zhou, Y. Yao, J. Luo, Cost-sensitive three-way email spam filtering, J. Intell. Inf. Syst. 42 (1) (2013) 19–45.
[10] J. Jung, E. Sit, An empirical study of spam traffic and the use of DNS black Lists, in: Proceedings of the 4th ACM SIGCOMM Conference on Internet Measurement, ACM, 2004, pp. 370–375.
[11] M. Antonakakis, R. Perdisci, D. Dagon, W. Lee, N. Feamster, Building a dynamic reputation system for DNS, in: Proceedings of the Third USENIX Workshop on Large-scale Exploits and Emergent Threats (LEET), 2010.
[12] Trust evaluation based content filtering in social interactive data, in: Proceedings of the 2013 International Conference on Cloud Computing and Big Data (CloudCom-Asia), IEEE, 2013, pp. 538–542.
[13] J. Kincaird, Edgerank: the secret sauce that makes Facebook's news feed tick, TechCrunch, 2010, ⟨http://techcrunch.com/2010/04/22/facebook-edgeran⟩.
[14] S. Yardi, D. Romero, G. Schoenebeck, Detecting spam in a Twitter network, First Monday 15 (1) (2009).
[15] G. Stringhini, C. Kruegel, G. Vigna, Detecting spammers on social networks, in: Proceedings of the 26th Annual Computer Security Applications Conference, ACM, 2010, pp. 1–9.

[16] A.H. Wang, Don't follow me: spam detection in Twitter, Security and Cryptography (SECRYPT), in: Proceedings of the 2010 International Conference on. IEEE, 2010, pp. 1–10.
[17] H. Gao, Y. Chen, K. Lee, D. Palsetia, A. Choudhary, Towards online spam filtering in social networks, in: Proceedings of the Symposium on Network and Distributed System Security (NDSS), 2012.
[18] F. Benevenuto, G. Magno, T. Rodrigues, V. Almeida, Detecting spammers on Twitter, in: Proceedings of the Seventh Annual Collaboration, Electronic messaging, Anti-abuse and Spam Conference (CEAS), 2010.
[19] Y. Zhu, X. Wang, E. Zhong, N.N. Liu, H. Li, Q. Yang, Discovering spammers in social networks, in: Proceedings of the Twenty-Sixth AAAI Conference on Artificial Intelligence (AAAI), 2012.
[20] X. Hu, J. Tang, Y. Zhang, H. Liu, Social spammer detection in microblogging, in: Proceedings of the Twenty-Third International Joint Conference on Artificial Intelligence, ACM, 2013, pp. 2633–2639.
[21] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, I.H. Witten, The WEKA data mining software: an update, ACM SIGKDD Explor. Newsl. 11 (1) (2009) 10–18.
[22] F. Wang, C. Zhang, Robust self-tuning semi-supervised learning, Neurocomputing 70 (16) (2007) 2931–2939.
[23] C. Cortes, V. Vapnik, Support-vector networks, Mach. learn. 20 (3) (1995) 273–297.
[24] LIBSVM – A Library for Support Vector Machines, ⟨http://www.csie.ntu.edu.tw/∼cjlin/libsvm/⟩.
[25] G.-B. Huang, Q.-Y. Zhu, C.-K. Siew, Extreme learning machine: theory and applications, Neurocomputing 70 (1) (2006) 489–501.
[26] G.-B. Huang, H. Zhou, R. Zhang, Extreme learning machine for regression and multiclass classification, IEEE Trans. Syst., Man, Cybern. 42 (2) (2012) 513–529.
[27] X. Zheng, N. Chen, Z. Chen, C. Rong, G. Chen, W. Guo, Mobile cloud based framework for remote-resident multimedia discovery and access, J. Internet Technol. 15 (6) (2014) 1043–1050.
[28] G.E. Hinton, Learning multiple layers of representation, Trends. Cogn. Sci. 11 (10) (2007) 428–434.
[29] Y. Bengio, Scaling up deep learning, in: Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, ACM, 2014, p. 1966.
[30] S. Zhou, Q. Chen, X. Wang, Active deep learning method for semi-supervised sentiment classification, Neurocomputing 120 (2013) 536–546.

Xianghan Zheng is associate professor in the College of Mathematics and Computer Sciences, Fuzhou University, China. He received his MSc of Distributed System (2007) and Ph.D. of Information Communication Technology (2011) from University of Agder, Norway. His current research interests include New Generation Network with special focus on Cloud Computing Services and Applications, Big Data Processing and Security.

Zhipeng Zeng (zhipeng.zeng@fzu.edu.cn) is currently working toward his M.S. Degree in College of Mathematics and Computer Science at Fuzhou University. His current research interests mainly focus on Big Data Analysis, especially on Social Network Analysis, Machine Learning, etc.

Zheyi Chen (zheyi.chen@yahoo.cn) is currently working toward his M.S. degree in College of Information Science and Technology at QingHua University. His current research interests mainly focus on New Generation Network, especially on Cloud Computing and Applications.

Yuanlong Yu (yu.yuanlong@fzu.edu.cn) is currently professor in the College of Mathematics and Computer Sciences, Fuzhou University, China. He received the B. Eng. degree in automatic control from the Beijing Institute of Technology, Beijing, China (2000), the M. Eng. degree in computer applied technology from Tsinghua University, Beijing, China (2003), and the Ph.D. degree in electrical engineering from the Memorial University of Newfoundland, St. John's, NL, Canada (2010). His current research interests mainly focus on machine learning, computer vision and cognitive robotics.

Chunming Rong (chunming.rong@uis.no) is Professor of the University of Stavanger and head of the Center for IP-based Service Innovation (CIPSI) at the University of Stavanger (UiS) in Norway. The CIPSI has the mission to promote cross-fertilization between several research fields to facilitate design and delivery of large-scale and complex IP-based services required by many application areas. Chunming's research interests include cloud computing, big data analysis, security and privacy.