Effective Detecting Microblog Spammers Using Big Data Fusion Algorithm

Yang Qiao [1], Huaping Zhang [1*], Yanping Zhao [2], Yu Zhang [1], Yu Min [1]
[1]School of Computer Science, Beijing Inst.of Tech., Haidian, Beijing, China
[2]School of Management & Economics, Beijing Inst.of Tech., Beijing 100081, China
qiaoyang2014@nlpir.org kevinzhang@bit.edu.cn zhaoyp@bit.edu.cn zhangyu2014@nlpir.org
yumin2014@nlpir.org

Abstract *- The Spammers spread rumors and threaten social stability to get profit while resulting a serious impact. Most of the existing studies utilize machine learning techniques to detect spammers. While new trend of the Spammers is they are getting more intelligent too, evolving to evade existing detection features including to avoid being detected by performing like normals. In this paper, we design a Big Data Fusion algorithm to investigate the combination effects of multiple factors in detecting spammers with a series of comprehensive experimental studies. We grab a large amount of microblog data on the Internet and tested for 1.1TB of spammers' data which contains Weibo Microblog message of over 800,000 accounts. The results show that our new algorithm is much more effective than the existing detectors in that it is significantly improved in both the accuracy and the FP-rate by a large margin.*

Keywords: Social media, Spammer detection, Big data fusion algorithm

1 Introduction

Statistics show that the average time spent on social network sites are far more than other sites [1]. Take Twitter as an example, every day there are at least 65 million tweets were sent [2]. Especially in China, the social media like micro blog, Weibo Microblog in Sina.com [3], is also developing much more rapidly. Spammers in social media sites have utilized micro blog as the new platform in a convenient way to get high profits and to achieve illegal purposes [4]. The social media spammers can achieve their malicious goals such as sending rumors [5], spreading malware [5], hosting botnet command and launching other underground illicit activities [6]. These malicious acts even threaten social stability and national security. In February of 2010, thousands of Twitter users, such as the Press Complaints Commission, the BBC correspondent Nick Higham and the Guardian's head of audio Matt Wells, have seen their accounts hijacked after a viral phishing attack [7]. Many researchers along with engineers have devoted themselves to keep social media a spam-free online community. The representatives such as Sina Weibo Microblog to provide microblogging zombie clean-up plug-ins [8], Zinman et. al. [9] using the method of Naive Bayesian Model and Neural Networks for spammers detection, and Amleshwaram et. al. [10] using all aspects of the user's features in integrated social network.

However, spammers are evolving to evade existing detectors. Such as spammers will switch IP frequently while reposting to evade the detecting of IP address [11]. Or using tools to 'spin' their tweets so that they can have heterogeneous tweets with the same semantic meaning [12]. What's more, some spammers imitate the behavior of normal to avoid detection.

In this paper, we plan to design new detection features to detect evasive Weibo Microblog spammers through in-depth analysis of the evasion tactics utilized by current spammers. To achieve our research goals, we use blacklist and honeypot [13]to build our dataset.

Our contributions of this paper are as follows:

1) Set up a large Weibo Microblog data set of 1.1TB. Based on the data we set up analytics to counterpart the evasion tactics.
2) We evaluate the detection rates of two existing state-of-the-art solutions on our collected dataset.
3) We design a Big Data Fusion algorithm to investigate the combination effects of multiple factors in detecting spammers. According to our evaluation, while keeping decrease false positive rate, the detection rate significantly increases to at least 80% which are better than the existing methods.

2 Related Work

Generally, users that luring others to click on illegal links, deliberately distorting the facts, spreading advertising on social network are defined as spammers [14].

To identify distinguishable spammer characteristics, Ramchandran et. al. [15] study the network properties of email spam. Their analysis reveals a correlation between

* Huaping Zhang is the Corresponding author. (E-mail: kevinzhang@bit.edu.cn)

spammers and their physical locality (geographical IP or ASN) while the study also highlights BGP hijacking used for spam attacks. [16] is an extension of ideas from [17] where the authors employ supervised learning using network-level features to distinguish spam from ham. As the work in [18] suggests, Twitter based spam differs qualitatively from email spam.

The commonly used method to detect spammers is using machine learning methods [19] [20], such as detecting the release time distribution of the message to find abnormal [21] or use the user relationship of social network in community detection [22]. Most of the existing methods can be divided into 2 categories. As the examples of the first class[23,24,25], they extract the features of the spammers and normals to train machine-learning classifier as the detector of spammers. Based on the profile features, Lee [23] et al. develop machine learning based classifiers for identifying previously unknown spammers with high precision and a low rate of false positives. Benevenuto et al [24] identify a number of characteristics related to tweet content and user social behavior, they used these characteristics as attributes of machine learning process for classifying users as either spammers or non-spammers. Second types of methods such as [26] examine whether the use of URL blacklists would help to significantly stem the spread of Twitter spam. In addition to collecting training data, [23] and [27] also use social honey pot to collect spammers message. We also use a similar approach in this paper to collect spammers message.

3 Big Data Fusion Algorithm

In this part, based on the machine learning techniques to classifying accounts as spammers or regulars we design a big data fusion algorithm using the behaviors, the profile descriptions, and the content of the users from Sina-Weibo Microblog (like Twitter) in China. In the following section, we will describe and explain how we explore them to distinguish the significant features for effective detections in details.

3.1 Feature Set

In this part, we will explore feature set and the reasons for the selections and verify their discrimination ability.

3.1.1 Behavior-feature

Behavior-feature describes the habit of a user using Weibo Microblog. For example, users are accustomed to visiting Weibo Microblog at a specific time every day or maintain a stable posting frequency and so on. We build an auxiliary data set which contains 1000 normal users and 1200 spammers to evaluate the discrimination ability of features.

Posting Frequency: According our big data statistics' investigation of spammer operators, we find the irregular time span of using Weibo Microblog: the spammers are in a very unusual frequency pattern which is distinguishable in line with the user's habits. Due to the spammers in the absence of business they are often in an idle state, or in a very long time interval to posting a Weibo Microblog.

We set up an analytics as post frequency F_{post} of user v, computed by Eq. (1) to calculate the users posts per hour in some pre-assigned time slot (e.g. the last 2 months):

$$F_{post} = \frac{N_{post-dura}(v)}{|T_{dura}|} \quad (1)$$

where T_{dura} donates the time slot that needed to calculate posting frequency, $N_{post-dura}$ donate the number of the Weibo Microblogs posted in the time slot. To better show the distinguishable pattern between normals and spammers we draw the distributions of the F_{post}s in Fig 1.

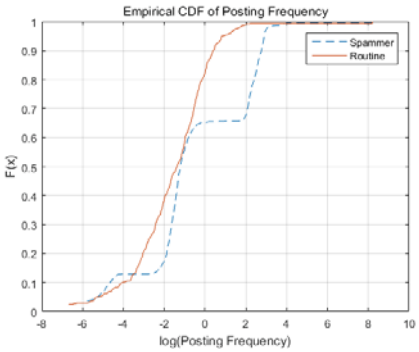

Fig. 1: the distributions of F_{post}

From Fig. 1 we can see that the distribution of spammers is a ladder shape curve(blue) which means spammers' posting frequency distributed in a few lengths of time spans. By comparison, the curve of normals is more smooth in line with the user's human habits. If the spammer still wants to evade, he needs to pay more by posting much more with limited financial support.

Ways to access Weibo Microblog(*Number of ways to post repost*): People have a lot of ways to access Weibo Microblog such as webpage or mobile client. In Fig. 2: we show some common ways

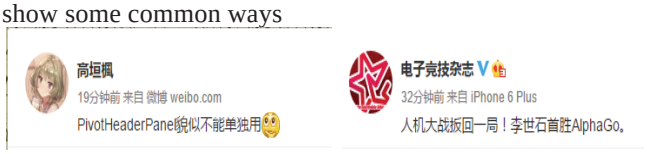

Fig. 2: ways to access Weibo Microblog

We define that *Ways to access Weibo Microblog* as the total number of the ways a user used to post original Weibo Microblog and Number of the ways to repost.

Because spammers need to post a large number of similar Weibo Microblogs in a given time period for some purposes, they need to use API or Weibo Microblog-repeater to release. In contrast, normals have a variety of ways to access Weibo Microblog but not the spammers. We draw the distributions of two:

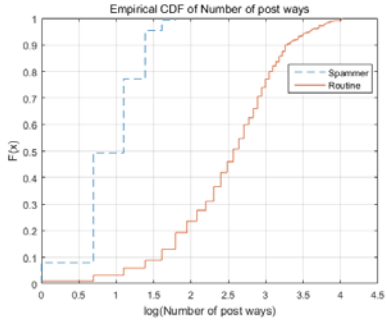

Fig. 3(a): *Ways to access Weibo Microblog(for post)*

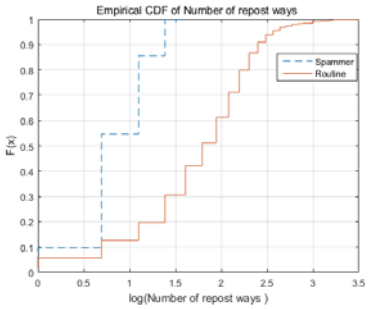

Fig. 3(b): *Ways to access Weibo Microblog(for repost)*

From Fig. 3 we can see that normals use more different ways to access Weibo Microblog than spammers.

Whether to participate in hot Weibo Microblog: Firstly, we define hot Weibo Microblog as having minimum of 100 reposts or comments on record. For spammers, the most common ways they used to make a profit is to repost or comment a target Weibo Microblog much more frequently. We get the evidence through social investigation and find that the purchase fee for a spammer account has the minimum committed consumption standard such as at least 100 times repost! That means spammers participate in hot Weibo Microblog more likely, because it comes to the core of their business, it's hard to avoid.

3.1.2 Content-based feature

In order to avoid the high computational complexity of the semantic analysis of every Weibo Microblog, we selected the following three content-based features as big data analytics.

Ratio of Original and Repost: Firstly, we define a user's total number of Weibo Microblog as N_{all}, the number of original Weibo Microblog is N_{ori}, the number of repost Weibo Microblog is N_{rp}.Then we calculate a user's ratio of Original and that of Repost:

$$R_{ori} = \frac{N_{ori}}{N_{all}}, R_{rp} = \frac{N_{rp}}{N_{all}} \quad (2)$$

Through big data analysis of spammers content we found spammers usually got lower ratio of Original Weibo Microblog and higher one of Repost than normals. As shown in Fig. 4.

We explain two main reasons for this situation: 1) Spammers are often assigned a target Weibo Microblog to be reposted so spammers' reposts are much more. 2)Posting original Weibo Microblogs needs more efforts so that less profit for spammers, and it will increase the probability of being detected if a spammer posts too often.

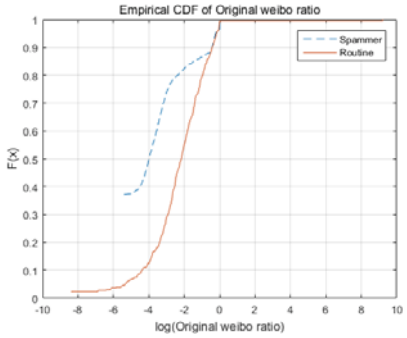

Fig. 4(a): Comparison the Ratio of Original

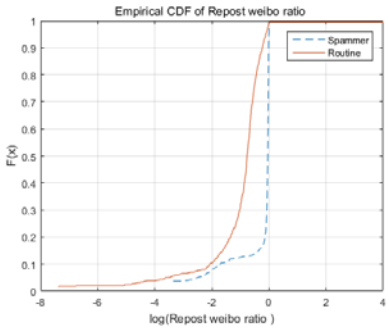

Fig. 4(b): Comparison the ratio of Repost

If spammers try to evade these two detection features, they will have to pay a high price. For example, spammers use websites like spin-bot to convert the target Weibo Microblog to a variety of forms like original Weibo Microblogs, they will pay a high time cost.

Average of @mention: @mention presents the public interaction between Weibo Microblog users, or the multiple layer repost feature of some users. According to our investigation, most of spammers' Weibo Microblogs only contain one @mention, which means their target Weibo Microblog are original. We define user v's Average of @mention as $A_{rp-at}(v)$:

$$A_{rp-at}(v) = \frac{1}{|N_{rp}(v)|} \cdot \sum_{u \in RP(v)} N_{rp-at}(u) \quad (3)$$

Where $N_{rp}(v)$ is the total number of user v's reposts, $RP(v)$ is the set of user u's repost, N_{rp-at} is the number of @mentions per repost of user v. We also draw the curve of the *Average number of @mention* distribution as Fig. 5 We can see that there are obvious differences in the curve of distributions between normals and spammers. As for evasion tactics, spammers can randomly @someone while reposting to evade detection, but that may also cause accusation and lead to accounts suspended.

3.1.3 Profile-based Feature

Profile features describe the basic user information. Due to the different purposes of using Weibo Microblog account, we choose the following profile-based features.

Total of Fans and Followings: Fans number and Followings number describe a user's popularity or level of attraction, which also show a user's level of activity in Weibo Microblog. We randomly select spammers and normals each of the 1000 people from the annotated corpus. We use the distribution in Fig. 6(a)(b) to show the difference between spammers and normals in this feature.

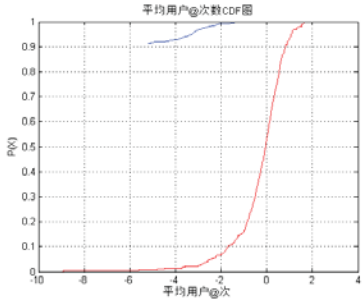

Fig. 5: Average of @ mentions

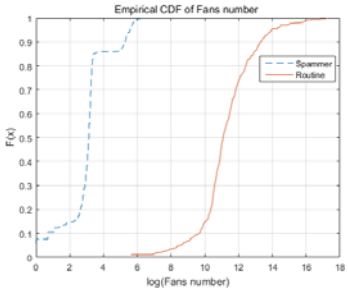

Fig. 6(a): Fans number

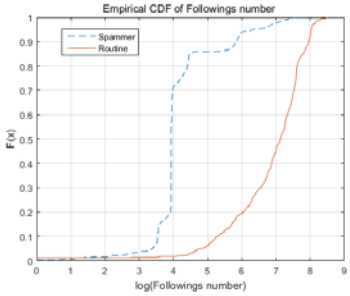

Fig. 6(b): Followings number

We can see that although the owner of spammers can raise the number of fans or followings by follow other spammers, there are still obvious difference between spammers and normals. Normal often get higher number than spammers both in fans number and followings number. This is also a good reflection of the difference between the account activity.

Ratio of fans number and followings number: Firstly, we use N_{fans} and $N_{follows}$ represent the Fans number and Followings number of a Weibo Microblog user. Then a user's ratio of fans number and followings number R_{fafo} can be calculated with the following formula:

$$R_{fafo} = \frac{N_{fans}}{N_{follows}} \quad (4)$$

The same as the last part, we draw the distribution of this feature in Fig. 7. We can see that most of the spammers' Ratio of fans number and followings number are less than 1, and normals are the opposite. We think this is because spammers sometimes are used to follow other account to making profit.

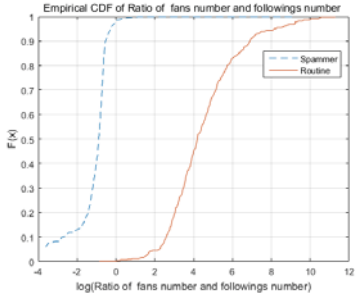

Fig. 7: Ratio of fans number and followings number

3.1.4 Big data Infusion Approach

We setup a big data infusion approach by incorporating our analytics and tactics to the existing state-of-the-art algorithms or methods, to improve the whole classifying or detecting efficacy.

4 Experiment and Evaluation

In this part, we will verify the validity of our new feature set through the experimental method. Based on this, we will analyze the impact of the classification model and the type of feature set on the detection results.

4.1 Experimental Data Preparation

We wrote a Sina Weibo Microblog crawler crawling users information and Weibo Microblog message for our experiment. In the process of collection, we use key words and posting time to identify a arousal event. In this way, we selected 10 arousal event that may contain spammers for crawling. Details about the crawling information can be seen in Table 1.

Table 1: Weibo Microblog accounts crawling information

CATEGORY	AMOUNT
TOTAL OF WEIBO ACCOUNTS	853,041
TOTAL OF WEIBO POSTS	142,304,427
TOTAL OF FANS' ACCOUNTS	130,334,187
TOTAL OF FOLLOWINGS' ACCOUNTS	115,675,345

Then, we need to identify Sina Weibo spammers from our crawled dataset. We randomly selected 10% of the accounts from each weibo arousal event and tag every account manually. What's more, we also bought spammers account on Internet authorities and collected their Sina Weibo information. Finally, we collect 20,000 spammers(15,000 through purchasing) and 20,000 normals to build each of our cross-validation test data set.

4.2 Evaluation of Big data Infused technique in Different Classifier

For the comparison the performance of the big data features infused classifiers, we selected 4 popular machine learning classifiers, including Logistic Regression[28],

SMO[29], AD tree[30] and Random Forest[31]. For each classifier we use 10-fold cross-validation to conduct evaluation.

In order to simulate the real situation, considering spammers detection is a imbalanced classes problem, we randomly selected 700,000 weibo posts from 720 normal accounts and 480 spammer accounts to build experiment dataset. In Fig. 7, we show the detection result of different classifiers:

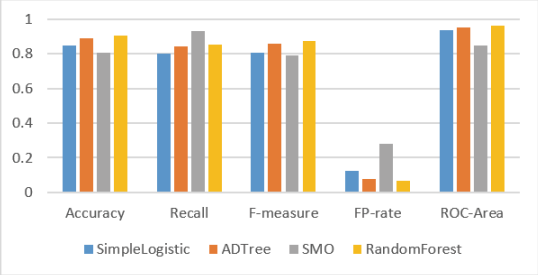

Fig. 7: Detection result of different classifiers

As shown in Fig. 7 and details in Table 2, the bigdata infused classifier based on Random Forest has the highest detection accuracy of 90.08% which means the best performance in distinguishing spammers from normals. The highest recall rate of 0.931 was obtained based on the SMO method, so we can use SMO to detect more spammers. In addition, the SMO algorithm leads to a much higher FP-rate of 0.279 than the other methods. According to the ROC-Area mesure of overall performance, the detector using Random Forest got the best performance. Since it detects more spammers than other method.

In order to facilitate the comparison, we use Table 2 for further analysis:

Table 2: Detection result of different classifiers

分类器	Accuracy	Recall	F-Measure	Precision	FP-rate	ROC Area
Simple Logistic	84.83%	0.804	0.809	0.814	0.122	0.804
AD Tree	88.08%	0.844	0.861	0.879	0.078	0.953
SMO	80.50%	0.931	0.793	0.690	0.279	0.826
Random Forest	90.08%	0.856	0.874	0.892	0.069	0.962

By observing Table 2 we can find that:

1) *Low model accuracy does not mean that no use.* We can see from the ROC-Area column in Table 2 that detector using SMO get the lowest value. That is to say its classification result is the worst. But when we do not consider the classification accuracy and consider only to find more spammers, wo should also choose SMO. Because it get the highest recall rate.

2) *Decision trees are suitable for our feature sets.* The method based on decision tree (AD Tree and Random Forest) is superior to the other two methods in classification accuracy. So we think decision tree is more suitable for our feature set under normal circumstances.

3) *The effect of the algorithm in class unbalanced problem.* Threshold shift and Composition Technologies are two commonly used methods to improve the accuracy of the class imbalance problem. Simple Logistic and Random Forest belong to these two kinds of methods respectively. Therefore the two methods have higher accuracy.

In order to refine the analysis of the results, we study the cross relationship between the classification results of each classifier, the results are shown in Fig. 8:

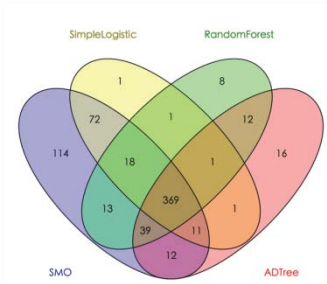

Table 3: Proportion of cross section

Classifier	Coincidence ratio
SMO	56.94%
Simple Logistic	77.84%
Random Forest	80.04%
AD Tree	80.04%

Fig. 8: cross relationship

Fig. 8 shows that the SMO algorithm and the other three algorithm results have obvious differences in the detection. What's more, 80% account are wrong classified by in the 114 account only detected by SMO. We also studied the accounts that were detected by the four methods, only 5 (1.4%)of them were identified as wrong classification. From Table 3 we see that the proportion of the coincidence part of all four algorithm is about 80% except SMO. So Using a variety of methods voting to determine the results is also a method to improve the accuracy of classification.

4.3 Comparison with Existing Strategies

In this part we implement two existing effective detection schemes [32, 33] and compare with our method. we also used the experiment dataset in 4.1. In order to ensure the fairness of the comparison, we choose the big data infused Logistic Regression method which was used both in [32] and [33]. Assuming that our proposed method is A, [32] is B, [33] is C. The comparison results are shown in Fig. 9.

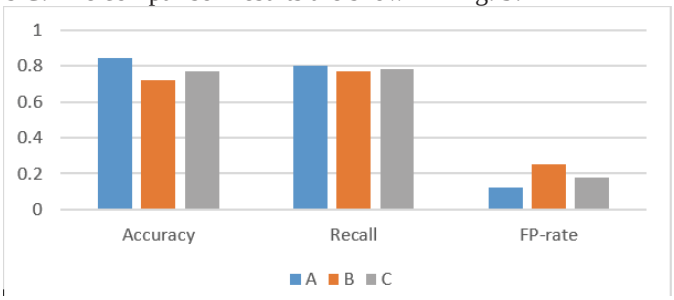

Fig. 9: Comparison of different detection methods

Compared with the method B and method C, our method improves the accuracy of 12% and 7% respectively. And there are also 1% and 4% optimizations on the recall rate. We think what we have in our ascension is:

1) Our feature set is *more abundant*, so higher accuracy can be obtained.

2) Feature *Bilateral Friend Ratio* in B can be evade by spammers by following other spammers easily, so it will lead to wrong classification.

3) Feature *Maximum number of Reposting* in C is an outdated detection feature. Through our investigation, the owner of

spammers control a large number of Weibo Microblog account so a spammer's *Maximum number of Reposting* is 1.A spammer don't need to repost a Weibo Microblog many times.So, this feature doesn't seem to work very well now.

4.4 Analysis and Evaluation of the Feature

In this part, we split and combine the feature subsets to analyze the detection results of different kinds of features. We define Behavior-features as feature set A, Content-features as feature set B, Profile-features as feature set C. In the following experiments, we tested the six feature sets: A, B, C, A+B, B+C, and A+C in Logistic Regression. Results are shown in the Fig. 10.

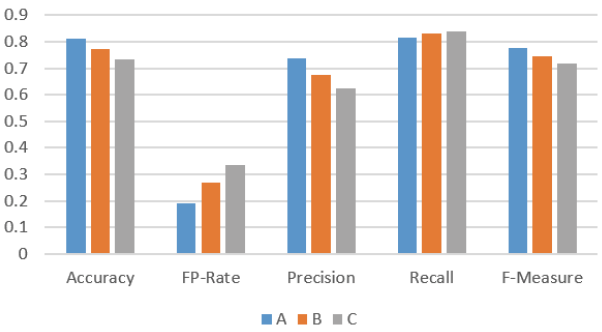

Fig. 10 (a): Comparison of different feature set

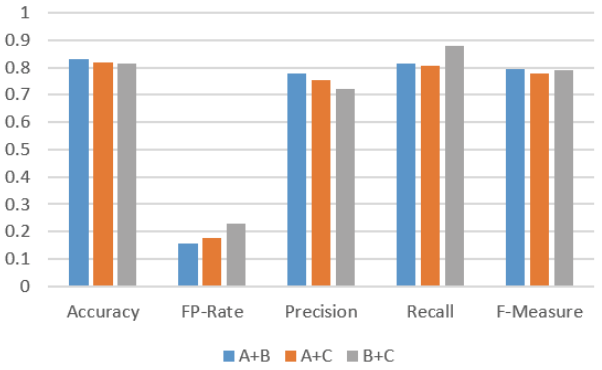

Fig. 10 (b): Comparison of different feature set

Firstly, we analyze the result in Table Fig. 10 (a), it compares the differences between different types of features:

1) The accuracy is decreased with the order of Behavior-features, Content-features, and Profile-features and the magnitude of the decline is even about 4%. On the other hand, it is also the most difficult to avoid the Behavior-features through our investigation. So we think that Behavior-features is more effective than other features in distinguishing between spammers and normals.

2) We can see from the Fig. 10 that the use of Profile-features can get a higher recall rate. But when we improved the recall about 1% using Profile-features only FP-Rate also increased by about 8%. This is the loss outweighs the gain. So we believe Profile-features should be combined with other features.

3) Same as accuracy, the F-Measure is also decreased with the order of Behavior-features, Content-features, and Profile-features. So we think as a whole Behavior-features is superior to Content-features and Profile-features on the detection of spammers.

Then, we analyze the detection result of two kinds of features in Fig. 10 (a). By comparing the Fig. 10 (a) and table 5(b) we can see:

1) By incorporating two kinds of features, the accuracy is increased by about 5%. At the same time, the recall rate is only decreased by 2% with the combination of Behavior-features and Profile-features.

2) By combine different kind of features we also get higher F-Measure, so it is very necessary to use a variety of features.

By comparing Fig. 10 and the result of our whole feature set we find that the accuracy is promoted most by adding Behavior-features followed by Content-features. This is also verified from one side that Behavior-features is superior to Content-features and Profile-features on the detection of spammers.

4.5 The promotion of new features

In order to further verify the correctness of the new big data analytics we propose, we analysed the detection result of the following two feature sets. The first set contains analytics we used that are also used in some of the previous studies including: *Original weibo ratio, Repost weibo ratio, Fans and Followings Ratio* The second set is our whole analytics set. The experimental results are shown in the following Table 4:

Table 4: The promotion of new features

	Without our Features			All Features		
Classifier	Accuracy	FP-Rate	F-Measure	Accuracy	FP-Rate	F-Measure
Simple Logistic	73.75%	0.356	0.728	84.83%	0.122	0.809
AD Tree	83.66%	0.116	0.834	89.08%	0.078	0.861
SMO	63.08%	0.161	0.409	80.50%	0.279	0.793
Random Forest	85.5%	0.095	0.843	90.08%	0.069	0.874

From the table 6, we can see that after adding the new analytics, the accuracy of each algorithm are improved at least 5%. At the same time, the FP-Rate are also improved. This observation implies that the improvement of the detection performance is indeed proportional to our newly designed big data infused analytics rather than the combination of several existing features.

5 Conclusion

In this paper, we design a novel big data infusion algorithm to detect Weibo spammers based on an in-depth analysis of the new evasion tactics utilized by social spammers. We collected a large amount of spammer data on the Internet and do the examination of two state-of-the-art solutions. Through the analysis of those evasion tactics and existing research design a multi-features fusion algorithm to detect spammers. According to our evaluation, while keeping an even lower false positive rate, the detection rate by using our new method increases over 10% than all existing detectors under four different prevalent machine learning classifiers. Finally, depending on the demand, we can choose different classification models or feature subsets in practical application.

6 References

[1] http://www.businessinsider.com

[2] Costolo: Twitter Now Has 190 Million Users Tweeting 65 Million Times A Day.

[3] https://en.wikipedia.org/wiki/Microblogging_in_China

[4] Biao Li, MN Zheng. Study on effect of online water army in the Communication of Network Opinion in the Era of Micro-blog[J]. CJC, 2012(10):30-36

[5] Yang C, Harkreader R C, Gu G. Die Free or Live Hard? Empirical Evaluation and New Design for Fighting Evolving Twitter Spammers[J]. IEEE Transactions on Information Forensics & Security, 2011, 8(8):1280 - 1293.

[6] http://xueshu.baidu.com/

[7] Twitter phishing hack hits BBC, Guardian and cabinet minister.

[8] http://app.Weibo Microblog.com/detail/776yQ

[9] Zinman A, Donath J. Is britney spears spam. In: Proc. of the 4th Conf. on Email and Anti-Spam (CEAS 2007). 2007. 1−10.http://ceas.cc/2007/

[10] Amleshwaram A A, Reddy N, Yadav S, et al. CATS: Characterizing automation of Twitter spammers[C]// Communication Systems and Networks (COMSNETS), 2013 Fifth International Conference on. IEEE, 2013:1-10.

[11] http://tech.qq.com/a/20101126/000325.htm

[12] https://spinbot.com/

[13] http://www.projecthoneypot.org/about_us.php

[14] GF Deng, GW tang. Network communication and social impact studies rumor [J]. Seeker, 2005, (10):88-90.

[15] Tseng CY, Sung PC, Chen MS. Cosdes: A collaborative spam detection system with a novel e-mail abstraction scheme. IEEE Trans. on Knowledge and Data Engineering, 2011,23(5):669−682. [doi: 10.1109/TKDE.2010.147]

[16] Kan Cheng, Liang Chen, Peidong Zhu. Interaction based on method for spam detection in online social networks [J]. Journal on Communications, 2015, 36(7):120-128.

[17] Sathawane KS, Tuteja RR. A robust spam detection system using a collaborative approach with an E-mail abstraction scheme and spam tree data structure. Int'l Journal of Computer Science and Applications, 2013,6(2):293−298.

[18] Hayati P, Chai K, Potdar V, Talevski A. HoneySpam 2.0: Profiling Web spambot behaviour. In: Proc. of the Principles of Practicein Multi-Agent Systems. Heidelberg: Springer-Verlag, 2009. 335−344. [doi: 10.1007/978-3-642-11161-7_23]

[19] https://en.wikipedia.org/wiki/Machine_learning

[20] MO Qian, YANG Ke. Overview of Web Spammer Detection[J]. Ruan Jian Xue Bao/ Journal of Software, 2014, 25(7): 1505-1526.http://www.jos.org.cn/1000-9825/4617.html.

[21] Hayati P, Chai K, Potdar V, Talevski A. Behaviour-Based Web spambot detection by utilising action time and action frequency. In:Taniar D, Gervasi O, Murgante B, Pardede E, Apduhan BO, eds. Proc. of the Computational Science and Its Applications (ICCSA2010). Heidelberg: Springer-Verlag, 2010. 351−360. [doi: 10.1007/978-3-642-12165-4_28]

[22] Hayati P, Potdar V, Talevski A, Chai K. Characterisation of Web spambots using self organising maps. Int ' l Journal of ComputerSystems Science & Engineering, 2011,26(2):87−96.

[23] Lee K, Caverlee J, Webb S. Uncovering social spammers: social honeypots machine learning[C]// Proceedings of the 33rd international ACM SIGIR conference on Research and development in information retrieval. ACM, 2010:435-442.

[24] F. Benevenuto, G. Magno, T. Rodrigues, and V. Almeida. Detecting Spammers on Twitter. InCollaboration, Electronic messaging, Anti-Abuse and Spam Confference (CEAS), 2010.

[25] Wang A H. Don't follow me: Spam detection in Twitter[C]. Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on. IEEE, 2010:1 – 10.

[26] Grier C, Thomas K, Paxson V, et al. @spam: the underground on 140 characters or less[C]// In Ccs. ACM, 2010:27-37.

[27] Stringhini G, Kruegel C, Vigna G. Detecting spammers on social networks[C]. Computer Security Applications Conference. 2010:1-9.

[28] https://en.wikipedia.org/wiki/Logistic_regression

[29] https://en.wikipedia.org/wiki/Sequential_minimal_optimization

[30] https://en.wikipedia.org/wiki/Alternating_decision_tree

[31] https://en.wikipedia.org/wiki/Random_forest

[32] Wang K, Xiao Y, Xiao Z. Detection of Internet water army in social network[C]//Proc. of the 2014 Int'l Conf. on Computer, Communications and Information Technology (CCIT 2014). Amsterdam: Atlantis Press. 2014: 189-192.

[33] Lin C, He J, Zhou Y, et al. Analysis and identification of spamming behaviors in sina Weibo Microblog microblog[C]//Proceedings of the 7th Workshop on Social Network Mining and Analysis. ACM, 2013: 5.