Hindawi
Mathematical Problems in Engineering
Volume 2021, Article ID 7682579, 11 pages
https://doi.org/10.1155/2021/7682579

Research Article

A Behavior-Driven Forum Spammer Recognition Method with Its Application in Automobile Forums

Han Su,[1] Minglun Ren,[1] Anning Wang,[1] Xiaoan Tang ,[1] Xin Ni,[2] and Zhao Fang[1,3]

[1]*School of Management, Hefei University of Technology, Hefei 230009, China*
[2]*Department of Design, Information System and Inventive Processes, INSA de Strasbourg, Strasbourg, France*
[3]*Department of Information Systems and Analytics, National University of Singapore, 13 Computing Drive, Singapore*

Correspondence should be addressed to Xiaoan Tang; sichuanshengxiaoan@163.com

Received 10 June 2021; Revised 9 August 2021; Accepted 13 August 2021; Published 31 August 2021

Academic Editor: Xin Tian

Forum comments are valuable information for enterprises to discover public preferences and market trends. However, extensive marketing and malicious attack behaviors in forums are always an obstacle for enterprises to make effective use of this information. And these forum spammers are constantly updating technology to prevent detection. Therefore, how to accurately recognize forum spammers has become an important issue. Aiming to accurately recognize forum spammers, this paper changes the research target from understanding abnormal reviews and the suspicious relationship among forum spammers to discover how they must behave (follow or be followed) to achieve their monetary goals. First, we classify forum spammers into automated forum spammers and marketing forum spammers based on different behavioral features. Then, we propose a support vector machine-based automated spammer recognition (ASR) model and a *k*-means clustering-based marketing spammer recognition (MSR) model. The experimental results on the real-world labelled dataset illustrate the effectiveness of our methods on classification spammer from common users. To the best of our knowledge, this work is among the first to construct behavior-driven recognition models according to the different behavioral patterns of forum spammers.

1. Introduction

In recent years, with the background of social media, forums have become a specific community for users who have the same interests. An increasing number of users post related reviews in forums [1]. These reviews cover a wide variety of content, ranging from breaking news, discussions on various topics, posts about one's personal life, and the sharing of activities and interests [2]. As a significant platform for the users' discussion, some forums maintain a high level of user activity. In addition, the feedback from forum users is usually an important source of information for potential consumers to access product features. Enterprises also aim to discover product defects and real users' requirements via reviews in forums.

Due to the strong negative response to the initial exposure to erroneous information, it is difficult to correct such influences later. Once a network agrees on what happened, the collective memory becomes relatively resistant to competing information [3]. Thus, fake reviews in forums are now the biggest problem for forum users and enterprises.

Lots of current studies indirectly identify fake reviews by recognizing forum spammers based on behavioral features or sentiment analysis methods [4–7]. However, forum spammers are constantly updating their technology or changing their posting methods to prevent them from being detected by the fake reviews recognition system, which makes many methods no longer useful for recognizing forum spammers. Although the forum spammers try to disguise themselves as ordinary users, this purposeful posting will eventually show different behaviors from ordinary users. Therefore, this paper changes the research target from understanding abnormal reviews and the suspicious relationship among forum spammers to discovering how they must behave (follow or be followed) to achieve their

monetary goals. Firstly, we classify forum users as automated spammers, marketing spammers, and normal users according to the different behavior patterns of forum users. Automated spammers are those forum users who are controlled by the spam software. They disguise themselves as normal users who display an intention to purchase the related product or express dissatisfaction toward a related product. Normally, automated spammers mislead forum users by posting reviews with a biased emotional tendency. Marketing spammers are real users who are hired by a spam company. In contrast to automated spammers, marketing spammers disguise themselves as leading users in forums to promote related products. They post deep, detailed, and positive reviews to overstate the quality of related products. In general, the more detailed analysis, the more useful information for forum users [8–10]. Moreover, marketing spammers, as a new but contemptible marketing mode, are emerging in many forums [11]. Then, we propose a behavior-driven automated spammer recognition (ASR) model and a marketing spammer recognition (MSR) model to recognize forum spammers based on the above three types of forum users. Final experimental results illustrate our behavior-driven recognition models are able to accurately detect forum spammers.

The paper is organized as follows: Section 2 reviews the related works. In Section 3, we define some variables to measure the behavior features of forum users. The proposed ASR and MSR models are introduced in Section 4. Subsequently, we describe the experimental dataset and discuss the main experimental results in Section 5. Finally, we conclude with a summary in Section 6.

2. Related Works

At present, the research on recognizing spammers and fake reviews is mainly focused on social media like Twitter. Some e-business websites, such as Amazon and Taobao, have also achieved more research attention. In terms of recognizing forum spammers, a few studies have been conducted in recent years, mainly focusing on the recognition of fake forums and forum spam automator tools. Some recognition methods based on abnormal text content have also been proposed by researchers. Some researchers attempt to use abnormal URL characteristics in reviews and the link structure of the graph rooted at the posted URL to recognize posts from the forum spammers [12, 13]. Additionally, contents unrelated to the target posts in the forum were used to recognize forum spammers [14]. Shin [15] discovered some features and operational mechanisms of a forum spam automator tool named XRumer. This study provided some ideas for recognizing the forum spammers who used this tool. Some researchers proposed an approach that uses features such as the submission time of replies, thread activeness, position of replies, and spamicity of a forum user's first post to construct a forum spammer recognition model [5]. The significant differences in the action time and action frequency between forum spammers and normal users were also used to construct the forum spammer recognition model [7]. The performance of the classifier in [6], with an integrated semantic analysis, was quite promising in the real-world case study, as confirmed with both supervised learning and unsupervised learning techniques by comparing a nonsemantic and semantic analysis. As demonstrated in [16], by analyzing the features of forum users, forum spammer, and forums, the authors found that every forum has many fake reviews, including some forums with good reputations.

However, our work found that the methods mentioned above are no longer working well. For instance, most users are now able to easily distinguish rough and fake websites with many advertisements, so the number of fake reviews with URLs [12, 13] has become much lower. Additionally, we found that the recognition effect of the method in [14] would be compromised if a large number of forum spammers have occupied the forums. In our study, the abnormal feature named spamicity in the first post in [5] does not work currently for recognizing forum spammers. At the same time, we found that marketing spammers have a similar abnormal behavioral feature named the submission time of replies in [5] but we cannot find the same behavioral pattern among automated spammers. In [16], the method that recognizes spam pages based on spam content features is still effective, but this method cannot efficiently recognize forum spammers who have many reviews that are similar to those of normal users. In [6], the authors mentioned that once a mission is finished, a paid spam poster normally discards the user ID and never uses it again, potential paid spam posters are not willing to continue their activities for a long time.

In recent years, research on spammers in social media and e-business websites has been increasing. Liu [17] proposed a two-stage cascading model, named ProZombie, which balanced effectiveness and accuracy well in recognizing spammers in Weibo. In [18], message content, user behavior, and social relationship information were fully used to recognize spammers in Weibo. The work by Hayati et al. [19] proposed using a self-organizing map and neural networks to determine the features of spammers on the Internet. They classified spammers into four categories based on the different behavioral patterns of spammers: content submitters, profile editors, content viewers, and mixed behavior. Radford et al. [20] constructed an unsupervised representation learning system, which reached an accuracy of 91.8% in sentiment analysis by using reviews in Amazon as training datasets. Furthermore, the authors in [12, 21] recognized fake reviews via the difference of emoticons, URLs, @ symbols, and photos in different reviews from spammers and normal users. Dewang et al. [22] proposed a spam detection framework combining the PageRank algorithm to detect the spam host of websites. In [6], the authors distinguished the fake reviews by using word segmentation for the text and calculating the emotional tendency. Jiang and Ratkiewicz [23, 24] found that spammers have a "synchronized" behavioral pattern for a particular target and that it is significantly different from that of normal users. A spam detection model called SkyNet using user social networks and the posted photos in reviews has been proposed by Sun and Kenneth Loparo [25]. In [26], the final recognition accuracy for spammers was improved by 9.73% by

integrating the social network and content information into a matrix decomposition-based learning model. The above recognition methods for spammers in social media and E-business websites are developed well. However, our work found that these methods cannot be directly used to recognize forum spammers as they are not well adapted to their special behavioral patterns.

Our work is inspired by the idea of using noncontent-based features. Furthermore, Asghar et al. [27] also illustrated the effectiveness of spam-related features on improving the performance of spam detection works. Thus, we construct behavior-driven forum spammer recognition models by understanding how forum spammers must behave (follow or be followed) for monetary purposes. To the best of our knowledge, this work is the first to construct forum spammer recognition models based on forum users' different behavioral patterns. In addition, we achieved promising experimental results on real-world forum datasets.

3. Observed Features

Automated spammers and marketing spammers often cooperate with each other to mislead forum users via the different roles they play in forums. In addition, the differences in roles they play inevitably lead to differences in the behavioral patterns they exhibit in forums. To recognize these forum spammers, in this section, the features of abnormal behaviors that are likely to be linked with the forum spammers are proposed and some variables are defined to measure these features. Subsequently, these variables can be exploited in our recognition models.

3.1. Automated Spammer Features. In this section, we perform a statistical analysis to investigate the objective features that are useful in capturing the reply behavior of automated spammers. And for each feature, we define the relevant variable. The four features of automated spammers are fully described as follows.

3.1.1. Reply Manner. The work in [6] reported that the spammers usually tend to post new comments because they do not have enough patience to read the comments and replies of others. The authors also proposed the response indicator (whether the comment is a new comment or a reply to another comment) to capture the abnormal behavior. However, automated spammers in forums never post any replies to the comments of others, and they only post new replies. To recognize this more extreme abnormal behavioral pattern in forums, we define RM_i as an indicator of whether forum user i only has new replies or has some replies to other comments (even if he only has a single reply for another comment):

$$\mathrm{RM}_i = \begin{cases} 0, & \text{never reply to another comment,} \\ 1, & \text{otherwise.} \end{cases} \quad (1)$$

As shown in Table 1, in the labelled dataset, we find 100% of automated spammers never reply to another comment, but only 1.68% of normal users have this similar behavior. On contrary, most normal users in forums not only post new replies but also post many replies to the comments of others.

3.1.2. Replies Number. Posting a large number of replies within a single minute also indicates an abnormal behavior. As shown in Table 2, in the labelled dataset, some automated spammers post more than 30 replies in a single minute, which means that they can post a reply within 2 seconds on average. To capture this abnormal behavioral pattern, we define MRN_i as the maximum replies number within a single minute of forum user i. However, relying only on the maximum replies number may cause misjudgment, because normal users may also post a large number of replies at a certain point in time. Consider that this behavior pattern is frequent for automated spammers, but occasionally for normal users. We define $\mathrm{AVG\_MRN}_i^n$ as the average value of the top n maximum replies number within a single minute of forum users i. Empirically, the value of n is set to 10.

3.1.3. Cooccurrence Frequency. To avoid being detected, automated spammers in the forum utilize different reply content from their databases frequently to reply to different original posts. The phenomenon that a forum spammer uses the same content to reply to an original post continuously has become rare now. However, currently, spam teams that are constituted by different automated spammers start to post fake replies to target posts continuously. Thus, it leads to cooccurrence behavior. This means that many automated spammers appear together at the same time or within a short time period. As shown in Table 3, in our labelled dataset, 59.14% of the automated spammers have this behavior that any two forum users post replies together with one minute more than five times. In contrast, only 3.52% of normal users have the same behavioral pattern. Therefore, we define MCF_i as the maximum cooccurrence frequency between user i and other forum users who simultaneously post a reply within one minute. Similar to the replies number, the reply time of normal users may coincide with the automated spammers. Therefore, $\mathrm{AVG\_MCF}_i^n$ is defined as the average value of the top n maximum cooccurrence frequency between user i and other forum users who simultaneously post a reply within one minute.

3.1.4. Duplicate Replies (DR). Automated spammers usually post duplicate replies under different original posts [28]. Our study finds that a few normal users also post some duplicate replies, such as "I support the original poster." However, the higher the ratio of a user's duplicate replies, the more likely he/she is an automated spammer in the forum. To capture this abnormal behavior, we define DRR_i as the duplicate replies rate of forum user i, which can be calculated by the following equation:

Table 1: Reply indicators.

RM	0 (%)	1
Automated spammers	100	0
Normal users	1.68	98.32%

Table 2: Percentage of the number of replies.

MRN ≥	10 (%)	20 (%)	30
Automated spammers	6.29	0.98	0.39%
Normal users	1.63	0.16	0

Table 3: Percentage of the cooccurrence frequency.

CF ≥	3 (%)	4 (%)	5 (%)	6 (%)	7 (%)
Automated spammers	74.26	64.44	59.14	54.42	40.47
Normal users	8.23	5.25	3.52	2.72	2.20

$$\mathrm{DRR}_i = \frac{2\sum_j^N \sum_k^N \mathrm{sim}\left(r_j, r_k\right)}{N(N+1)}, \tag{2}$$

where N denotes the total number of replies posted by user i, r_j represents the text vector of j^{th} reply, and $\mathrm{sim}(r_j, r_k)$ denotes the text similarity of j^{th} reply and k^{th} reply. In this paper, the text similarity between two replies is measured by the TF-IDF weighted word embedding. Reply R_j can be represented as

$$r_j = \sum_{t \in R_j} w_t \cdot \mathrm{TFIDF}_t, \tag{3}$$

where t denotes the word in R_j, w_t represents the word vectors of word t generated by pretrained word embedding model, and TFIDF_t denotes the TFIDF value of word t. Then, for each two replies j and k, their text similarity can be measured by the following equation:

$$\mathrm{sim}\left(r_j, r_k\right) = \frac{r_j \cdot r_k}{r_j \times r_k}. \tag{4}$$

As shown in Table 4, 55.40% of automated spammers have a duplicate replies rate of more than 0.5, but the rate for the normal users is extremely low.

3.2. Marketing Spammer Features. As discussed before, marketing spammers usually disguise themselves as the leading users in the forums. These spammers not only post replies but also publish many original posts as do normal users. In other words, they are real forum users but they do what the spammers always do. Therefore, it is difficult to recognize marketing spammers using a recognition model that is constructed based on the abnormal behavioral features of automated spammers. In this section, three abnormal behavior features are identified in terms of the posting behavior of marketing spammers.

3.2.1. Posting in Many Forums. Due to the increasing strict registration process in forums, a forum account, especially a reputable forum account, is becoming a rare resource for marketing spammers. To maximize their commercial interests, the forum accounts of marketing spammers normally work in several forums. In other words, marketing spammers may publish fake original posts for different targeted products in several forums. As shown in Table 5, in the labelled dataset, the average number of forums in which marketing spammers publish original posts is much higher than that of normal users. Therefore, the variable NF is defined as the number of forums in which a forum user posts original posts within a year.

Table 4: Percentage of the ratio of duplicate replies.

DRR ≥	0.3 (%)	0.4 (%)	0.5 (%)	0.6 (%)	0.7 (%)
Automated spammers	58.74	56.19	55.40	44.79	36.74
Normal users	15.93	8.70	3.65	1.05	0.03

3.2.2. Posting Intensity Is High and Uneven. To strengthen the performance of the marketing effort, marketing spammers usually publish a series of original posts and actively interact with other forum users during the marketing period. In this period, marketing spammers promote the targeted product via the diffusion of a large number of positive word-of-mouth recommendations that they make. Moreover, they sometimes publish many negative word-of-mouth recommendations to slander their competitors. All of these are for their marketing purpose. Therefore, once the marketing period is finished, the activity of marketing spammers will decline sharply or the users even disappear completely. Moreover, the point in time at which marketing spammers post original posts usually is highly correlated with the targeted product's marketing events. As shown in Figure 1, a new car named Tiggo7 began to sell from September 2016, and with the rising search number (yellow line), the activity of marketing spammers also began to increase. Apparently, the average number of postings of marketing spammers reached the maximum 3 months after the new car was put on the market. However, with the decline of the search numbers and the end of the marketing period, the average number of postings by marketing spammers began to decline sharply or even reached zero. Moreover, the average number of postings of normal users was always stable and low. That is, the posting and replying activities of marketing spammers show alternating or cyclical fluctuations. As such, two variables NOP and SDNP are defined to measure this difference. The former variable denotes the number of original posts published by a forum user within a year and the latter variable denotes the standard deviation of the number of posts published by a forum user over 12 months.

3.2.3. Posts with Many Words and Pictures. The more detailed a product analysis is, the more helpful it is for forums users [8]. In addition, according to the reward and punishment mechanism of forums, the level and detail of original posts are an essential evaluation criterion for the "sticky posts" in forums. The number of "sticky posts" is the determinant of the authority of forum users. Marketing

Table 5: The number of forums in which marketing spammers publish original posts.

Marketing spammer	The number of forums
MS_1	45
MS_2	33
MS_3	57
MS_4	132
MS_5	73
MS_6	35
MS_7	52
MS_8	66
MS_9	75
MS_{10}	136
MS_{11}	49
Average	**68.45**
Average (normal user)	3.56

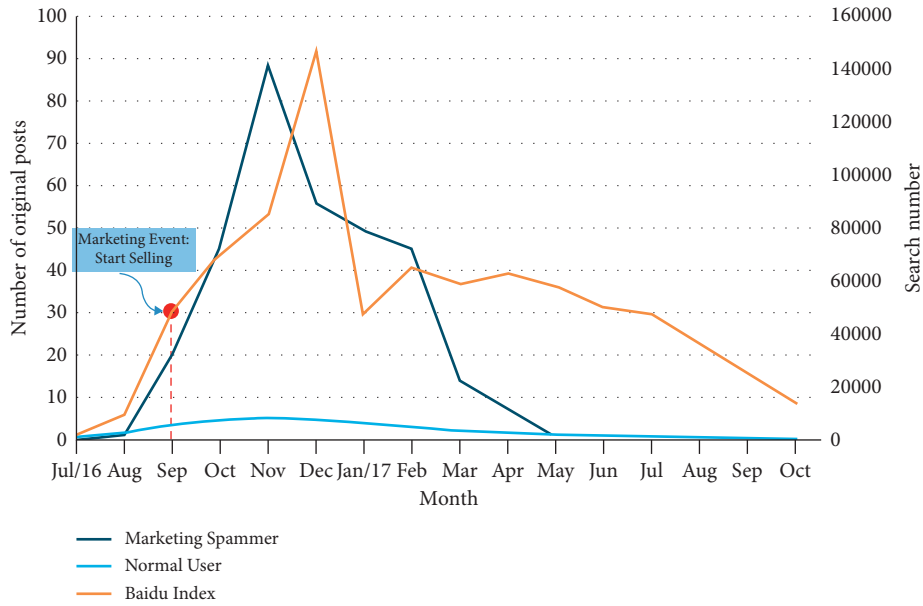

Figure 1: The average number of original posts marketing spammers posted.

spammers tend to use their authority to influence potential consumers. From Table 6, we can see that the original posts that marketing spammers published were always detailed and had many words, including a description and an analysis from every aspect of the targeted product. Therefore, as shown in Table 7, we classify the original posts into 3 levels based on the content features and find that most of the original posts of marketing spammers are Level 2 or Level 3, but most normal users' original posts are Level 1 or Level 2. Therefore, we define two variables ANW and CRL to measure this difference. The former variable denotes the average number of words for all original posts posted by a forum user within a year, and the latter variable denotes the average content richness level for all original posts posted by a forum user within a year.

Table 6: Distribution of the number of words in original posts.

	Percentage	
Word count	Marketing spammer (%)	Normal user (%)
0–500	9.10	**72.32**
500–1000	36.36	23.58
> 1000	**54.54**	4.10

4. Recognition Models

As discussed before, automated spammers and marketing spammers present obvious features in terms of the reply behaviors and post behaviors. It is difficult to identify automated spammers and marketing spammers simultaneously by one single recognition model. Therefore, a two-

Table 7: Measure of the level of detail in original posts.

	Percentage	
Level	Marketing spammer (%)	Normal user (%)
Level 1	14.32	**75.56**
Level 2	**46.80**	12.43
Level 3	38.88	12.01

Note. Level 1: no pictures, a few product features, and words. Level 2: a few images, some product features, and some sentences. Level 3: many pictures, abundant product features, and many analytical sentences.

level cascading model is adopted to improve the recognition accuracy, as shown in Figure 2. To facilitate the understanding of the proposed model, the main problem to be solved in this paper is first described.

4.1. Problem Description. Given a set of forum users $\{u_1, u_2, \ldots, u_i, \ldots, u_m\}$ and their reviews $r_i = \{r_{i1}, r_{i2}, \ldots\}$, where m denotes the number of users, this paper aims to classify each user into three types, that is, automated spammer, marketing spammer, and normal user. Specifically, the model firstly extracts the user's personal behavior features and interactive behavior features based on their reviews. Among them, the personal behavior features can be expressed as $f_k(r_i)$, where f_k denotes the feature extraction function of k^{th} feature; and the interactive behavior features can be expressed as $f_k(r_i, r_j)$. Then, the two-level model recognizes the type of each user based on the personal behavior features and interactive behavior features. The type of i^{th} user is t_i, $1 \le i \le m$, $t_i \in$ TagSet where TagSet represents the set of all user types: automated spammer and marketing spammer and normal user. Thus, the final output is $t_1, t_2, \ldots, t_m$.

4.2. The ASR Model. The first-level model (ASR model) is used to recognize automated spammers. As analyzed in Section 4.1, the six variables, reply manner (RM), maximum replies number (MRN), average of top 10 maximum replies number (AVG_MRN^{10}), maximum of cooccurrence frequency (MCF), average of top 10 maximum of cooccurrence frequency (AVG_MCF^{10}), and duplicate replies rate (DRR) are utilized to construct a support vector machines model to recognize automated spammers. The recognition model can classify the forum users into automated spammers and nonautomated spammers so that it can help us identify the majority of forum spammers among the forum users. After executing the ASR model, the automated spammers will be excluded from the forum users.

4.3. The MSR Model. The second-level model (MSR) then deals with the marketing spammers using a clustering method, which is built using the forum users streaming down from the first level. Compared to a large number of automated spammers, the number of marketing spammers is small and they are usually distributed in different forums. It is difficult to manually label many marketing spammers as an annotated dataset to construct a supervised machine learning model. Therefore, the paper adopts the unsupervised clustering method to construct the MSR model. In addition, as discussed in Section 4.2, marketing spammers can be recognized by five variables: the number of forums in which a forum user posts original posts within a year (NF), the number of original posts over 12 months (NOP), the standard deviation of the number of posts over 12 months (SDNP), the average number of words for all original posts posted by a forum user within a year (ANW), the average content richness level for all original posts posted by a forum user within a year (CRL). Hence, the five corresponding clustering attributes, that is, #NF, #NOP, #SDNP, #ANW, and #CRL, will be employed in the clustering model. The marketing spammers will be finally separated from the normal users by the MSR model. The MSR model is based on the K-means clustering method. Additionally, we normalize the value of these measures to [0, 1]. Additionally, the K in the K-means clustering is taken as 2.

5. Experiments

This section performs the forum spammer recognition of Chinese automobile reviews. Section 5.1 introduces the experimental dataset used in this paper. Section 5.2 discusses the main experimental results.

5.1. Data Collection and Annotation

5.1.1. Data Collection. China is one of the biggest markets in the world in terms of automobile sales growth [29]. Automobile forums have become the most important place for Chinese automobile buyers to refer to automobile information. Therefore, in this paper, user reviews in automobile forums (Autohome and Bitauto) are used as our experimental datasets. First, Autohome and Bitauto are the top two comprehensive automobile portals, which share 30.9% and 18.3% of automobile media in China, respectively [30]. Second, these two portals have developed independent subforums for each car model. That is to say, as long as a user registers an account, he/she can post or comment under all subforums. Therefore, we do not need additional tools to judge whether the users posting on different forums are the same person, which is very helpful to calculate the variables we define in Section 3.

We utilize the data of the Tiggo7 and Baojun610 forums, which are found on these two websites to fully verify the recognition models we proposed. The Tiggo7 dataset from October 2016 to January 2017 includes 81,753 forum users. The Baojun610 dataset from 2015 includes 4,755 forum user records and information from 370,204 user profiles for all the Bitauto.com forums. For each forum user record, we record the following relevant information: post title, post, post time, reply time, nickname, user comment, and floor. For each user profile information, the following relevant information is recorded: nickname, forum name, number of followers, number of followers, and identity.

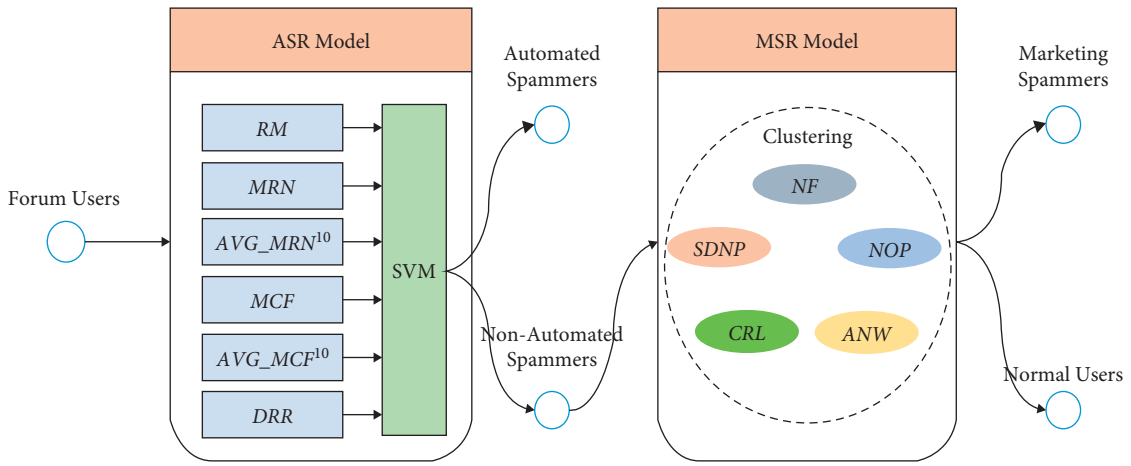

Figure 2: Framework of the two-level recognition model for forum spammers.

5.1.2. Annotation. Finding the "gold-standard" ground truth of labelling spammers is an open problem, and there is no solution to it [6]. In this paper, we manually label some forum users through the observation of abnormal behavioral patterns and users' post content in forums. Additionally, we refer to some existing manual labelling methods, which are listed in the following section:

(1) Users who post multiple duplicate or near duplicate replies [6]: Some examples include replies such as "I am going to buy this car" and "I like this car's appearance." These kinds of replies can be used to reply to any post in automobile forums and match the subject of a post perfectly. In addition, these duplicate replies usually show extreme emotions without any supporting evidence.

(2) Users who post meaningless or contradicting replies [6]: An example includes replies such as "Please contact me using QQ number, as I have coupons." In addition, some users may post many replies showing completely different opinions.

(3) Users who post many reviews that are full of empty adjectives and purely glowing praises with no shortcomings [31]. Unlike the abovementioned abnormal behavioral patterns, this labelling criterion needs to be used with other criteria, because a few normal forum users also occasionally have this behavior.

Cross-checking among multiple volunteers must also be used to ensure the authenticity of labelled data based on the above labelling criteria. We recruit eight volunteers and 509 automated spammers and 3,865 normal users are labelled out of 12,549 forum users in the Tiggo7 forum.

5.2. Comparison Analysis. In this section, we demonstrate the performance of the ASR and MSR models in recognizing forum spammers on the Tiggo7 and Baojun610 datasets.

5.2.1. Experiment 1: Recognize Automated Spammers. We test the performance of the ASR model using the Tiggo7 dataset. The dataset is divided into the training set and test set according to the ratio of 7 : 3. To verify the importance of each feature to the ASR model, in addition to using all the features to build the ASR model, we also conducted six comparative experiments. Each experiment removes one feature to test how much the feature improves the model performance. Table 8 shows the experimental results of the ASR model on the Tiggo7 dataset. We can see that the ASR model achieves satisfactory results in recognition automated spammers, and the experimental results also prove that each feature is indispensable to the ASR model.

5.2.2. Experiment 2: Recognize Marketing Spammers. The ASR model first recognizes 36 automated spammers on the Baojun610 dataset, and one of them is a normal forum user as manually verified. Moreover, we test the performance of the MSR model using the Baojun610 dataset. As seen from Figure 3, our recognition model recognized 6 marketing spammers in the Baojun610 forum who have also been verified manually.

In addition, we notice that a few forum users are automobile evaluators who posted many original posts and replies in many forums. Their behavior patterns are similar to those of marketing spammers, so they may be considered marketing spammers by the MSR model. As a special user group in the automobile forum, these automobile evaluators are not considered in our experiments because there are no such users in other types of forums. Eventually, the ASR and MSR models recognized 41 forum spammers in all the Baojun610 forums. The experimental results show that our behavior-driven recognition models are effective and accurate.

More interestingly, we noticed that a forum user named "Baidu Knows" (in Chinese), indicated by the green circle in Figure 4, and the forum user named "Secret Passage" (in Chinese), indicated by the yellow circle in Figure 4,

Table 8: Experimental results of ASR model with different features.

Feature	Precision	Recall	$F1$-score
All	0.964	0.937	0.950
All-RM	0.757	0.825	0.789
All-MRN	0.843	0.845	0.844
All-AVG_MRN[10]	0.817	0.835	0.826
All-MCF	0.924	0.908	0.916
All-AVG_MCF[10]	0.901	0.894	0.897
All-DRR	0.889	0.853	0.871

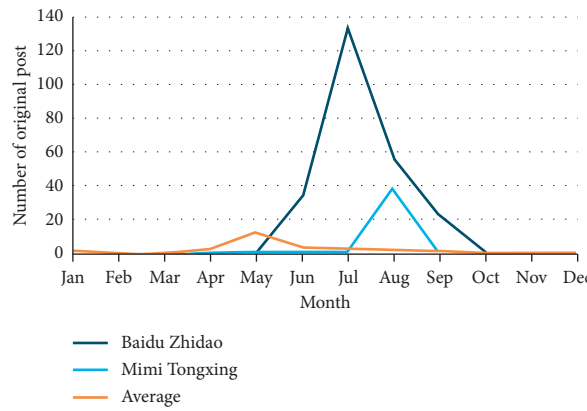

Figure 3: The illustration of the number of the original post.

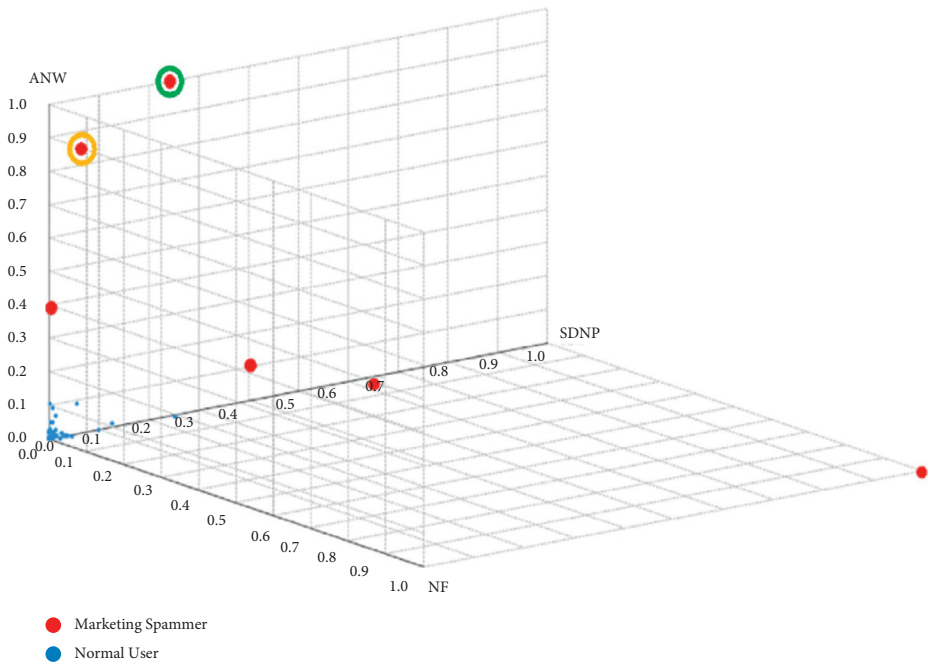

Figure 4: The recognition result of the MSR model for the marketing spammers.

surprisingly posted original posts in 140 and 118 forums, respectively. As we can see in Figure 3, they completely stopped posting after many original posts. The number of original posts that they posted is significantly higher than the average number of original posts of other forum users. We then accessed their user profiles on the Bitauto website, as seen in Figures 5 and 6.

As shown in Figure 5, the forum user named "Baidu Knows" (in Chinese) posted many original posts in forums on March 25, 2015. In the morning, he complained that his

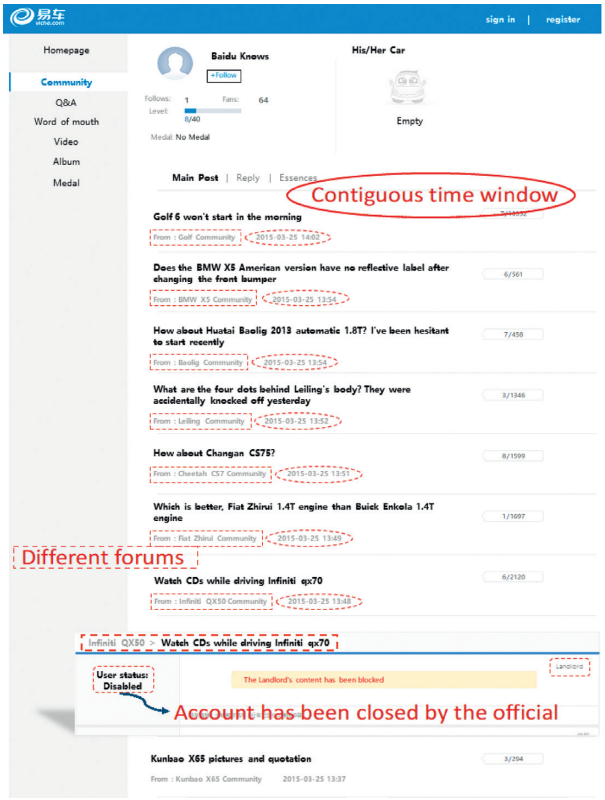

Figure 5: The profile of "Baidu Knows."

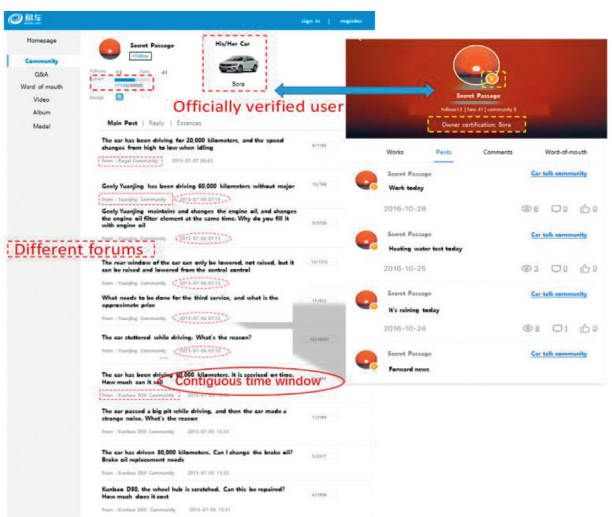

Figure 6: The Bitauto-verified profile of "Secret Passage."

automobile, a VW Golf, could not be started. Then, in the afternoon, he watched a DCD in his automobile, an Infiniti QX70. His last original post was posted on August 04, 2017. Currently, his original posts and replies have been deleted by the officials, and the account has been closed. This also proves that our MSR model is effective and that the recognition result is precise.

As seen from Figure 6, the forum user named "Secret Passage" (in Chinese) is an officially verified forum user who has a high level of influence. He posted original posts in many forums in a single day, and this behavior is similar to that of the forum user named "Baidu Knows" (in Chinese). He not only praised his automobile, a Geely Vision that has been driven 60,000 km with few serious problems so far, but also complained about the idling problem of his Buick Regal automobile, which has been driven 20,000 km. In addition, he also wishes to sell his Senova D50 automobile. From his contradictory words, we can infer that he is a forum spammer.

Table 9: Comparison experiment with other models.

Model	Precision	Recall	$F1$-score
Hu's model [4]	0.886	0.918	0.902
Chen's model [5]	0.878	0.922	0.897
Yu's model [18]	0.924	**0.943**	0.933
The proposed architecture	**0.964**	0.938	**0.951**

Table 10: Running time of the proposed model.

Total time (min)	Feature extraction (min)	Two-level model	
		ASR (min)	MSR (min)
16.16	12.85	1.59	1.72

5.2.3. Experiment 3: Comparison with Other Methods. In this section, the proposed architecture is compared with three representative models [4, 5, 18]. Table 9 shows the comparisons of the precision, recall, $F1$-score of each model on the Tiggo7 dataset. It is obvious that the proposed model outperforms other models. We believe that this is because we take more account of the user's behavior features. This also shows that the behavior feature-based method is better than the previous methods.

5.2.4. Experiment 4: Analysis of Running Time. Finally, we count the running time of the proposed model, as shown in Table 10, including feature extraction and two-level model. We can easily find that feature extraction takes up most of the time. This is because we need to calculate not only the personal behavior features of users but also the interactive behavior features between different users, which increases the burden of calculation. In addition, according to the feature extraction method described in Section 3, we can infer that the complexity of feature extraction depends on the following points: the total number of forum users, the number of forum posts, and the length of forum posts.

6. Conclusion

Fake reviews in forums are always an obstacle for enterprises to make effective use of the information in forums. And forum spammers are constantly updating their technology or changing their posting methods to prevent them from being detected by the fake reviews recognition system. Although the forum spammers try to disguise themselves as ordinary users, this purposeful posting will eventually show

different behaviors from ordinary users. Therefore, this paper changes the research target from understanding abnormal reviews and the suspicious relationship among forum spammers to discovering how they must behave (follow or be followed) to achieve their monetary goals. Based on different behavior features, forum spammers can be classified into automated forum spammers and marketing forum spammers. The support vector machine-based ASR model and the k-means clustering-based MSR model are developed, and their applications are demonstrated by using car forum reviews written in Chinese. The final experimental results illustrate the effectiveness of our behavior-driven recognition models.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This research was supported by the National Natural Science Foundation of China (no. 72101075 and 72101078), the Fundamental Research Funds for the Central Universities (nos. JZ2020HGQA0168 and JZ2021HGQA0204), and the Foundation for Innovative Research Groups of the National Natural Science Foundation of China (no. 71521001).

References

[1] X. T. Vu and P. Morizet-Mahoudeaux, *A User-Centered Approach for Integrating Social Data into Groups of Interest*, Elsevier Science Publishers B. V., Amsterdam, The Netherlands, 2015.

[2] B. Zhao, Z. Zhang, W. Qian, and A. Zhou, "Identification of collective viewpoints on microblogs," *Data & Knowledge Engineering*, vol. 87, no. 9, pp. 374–393, 2013.

[3] L. Spinney, "How Facebook, fake news and friends are warping your memory," *Nature*, vol. 543, pp. 168–170, 2017.

[4] X. Hu, T. Jiliang, G. Huiji, and L. Huan, "Social spammer detection with sentiment information," in *Proceedings of the IEEE International Conference on Data Mining IEEE*, pp. 180–189, Shenzhen, China, December 2014.

[5] Y. R. Chen and H. H. Chen, "Opinion spam detection in web forum: a real case study," in *In Proceedings of the, International Conference*, pp. 173–183, Florence, Italy, May 2015.

[6] C. Chen, K. Wu, V. Srinivasan, and X. Zhang, "Battling the internet water army: detection of hidden paid posters," 2011, http://arxiv.org/abs/1111.4297.

[7] P. Hayati, K. Chai, V. Potdar, and A. Talevski, "Behaviour-based web spambot detection by utilising action time and action frequency," in *Proceedings of the Computational Science and ITS Applications-ICCSA 2010, International Conference*, pp. 351–360, DBLP, Fukuoka, Japan, March 2010.

[8] J. P. Singh, S. Irani, N. P. Rana, Y. K. Dwivedi, S. Saumya, and P. Kumar Roy, "Predicting the "helpfulness" of online consumer reviews," *Journal of Business Research*, vol. 70, no. 70, pp. 346–355, 2017.

[9] Y.-M. Li, H.-M. Chen, J.-H. Liou, and L.-F. Lin, "Creating social intelligence for product portfolio design," *Decision Support Systems*, vol. 66, pp. 123–134, 2014.

[10] S. M. Mudambi and D. Schuff, "What makes a helpful online review? a study of customer reviews on amazon.com," *Social Science Electronic Publishing*, vol. 34, no. 1, pp. 185–200, 2012.

[11] Y. Chen and J. Xie, "Online consumer review: word-of-mouth as a new element of marketing communication mix," *Management Science*, vol. 54, no. 3, pp. 477–491, 2008.

[12] M. Ghannoum, "Prevalence and mitigation of forum spamming," in *Proceedings of the 2011 IEEE Infocom*, vol. 34, no. 17, pp. 2309–2317, Shanghai, China, April 2011.

[13] Y. Shin, S. Myers, M. Gupta, and P. Radivojac, "A link graph-based approach to identify forum spam," *Security and Communication Networks*, vol. 8, no. 2, pp. 176–188, 2015.

[14] Y. J. Lee, J.-M. Shim, H.-G. Cho, and G. Woo, "Detecting and visualizing the dispute structure of the replying comments in the internet forum sites," in *Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, pp. 456–463, IEEE Computer Society, Huangshan, China, October 2010.

[15] Y. Shin, M. Gupta, and S. Myers, "The nuts and bolts of a forum spam automator," in *Proceedings of the Usenix Conference on Large-Scale Exploits and Emergent Threats*, p. 3, USENIX Association, Boston, MA, USA, March 2011.

[16] Y. Niu, W. Yi-Min, C. Hao, M. Ming, and H. Francis, "A quantitative study of forum spamming using context-based analysis," in *Proceedings of the Network and Distributed System Security Symposium*, NDSS 2007, San Diego, CA, USA, February 2007.

[17] H. Liu, Z. Yuchao, L. Hao, Wu Junjie, W. Zhiang, and Z. Xu, "How many zombies around you," in *Proceedings of the 2013 International Conference on Data Mining*, pp. 1133–1138, Dallas, TX, USA, December 2013.

[18] D. Yu, N. Chen, F. Jiang, B. Fu, and A. Qin, "Constrained NMF-based semi-supervised learning for social media spammer detection," *Knowledge-Based Systems*, Knowledge-Based Systems125.C, vol. 125, , pp. 64–73, 2017.

[19] P. Hayati, V. Potdar, K. Chai, and A. Talevski, "Characterization of web spambots using self organizing maps," *Computer Systems Science and Engineering*, vol. 26, no. 2, 2011.

[20] A. Radford, R. Jozefowicz, and I. Sutskever, "Learning to generate reviews and discovering sentiment," 2017, http://arxiv.org/abs/1704.01444.

[21] L. Akoglu, M. Mcglohon, and C. Faloutsos, "Oddball: spotting anomalies in weighted graphs," in *Proceedings of the Pacific-Asia Conference on Advances in Knowledge Discovery and Data Mining*, pp. 410–421, Springer-Verlag, Hyderabad, India, June 2010.

[22] R. K. Dewang and A. K. Singh, "State-of-art approaches for review spammer detection: a survey," *Journal of Intelligent Information Systems*, vol. 50, no. 2, pp. 231–264, 2018.

[23] M. Jiang, C. Peng, B. Alex, F. Christos, and Y. Shiqiang, "Inferring strange behavior from connectivity pattern in social networks," in *Proceedings of the 2014 Pacific-Asia Conference on Knowledge Discovery and Data Mining*, Tainan, Taiwan, May 2014.

[24] J. Ratkiewicz, M. Conover, B. G. Alves, A. Flammini, and F. Menczer, "Detecting and tracking political abuse in social media," in *Proceedings of the International Conference on Weblogs and Social Media*, DBLP, Barcelona, Catalonia, Spain, July 2011.

[25] Y. Sun and K. Loparo, "Opinion spam detection based on heterogeneous information network," in *Proceedings of the*

2019 IEEE 31st International Conference on Tools with Artificial Intelligence (ICTAI), November 2019.

[26] S. Ghosh, V. Bimal, K. Farshad et al., "Understanding and combating link farming in the twitter social network," in *Proceedings of the 21st International Conference on World Wide WebACM*, pp. 61–70, Lyon France, April 2012.

[27] M. Z. Asghar, A. Ullah, S. Ahmad, and A. Khan, "Opinion spam detection framework using hybrid classification scheme," *Soft computing*, vol. 24, no. 5, pp. 3475–3498, 2020.

[28] E. P. Lim, V.-A. Nguyen, N. Jindal, B. Liu, and H. Wirawan Lauw, "Detecting product review spammers using rating behaviors," in *Proceedings of the ACM International Conference on Information and Knowledge Management ACM*, pp. 939–948, Toronto Ontario Canada, October 2010.

[29] JATO. http://www.jato.com/global-car-sales-5-6-2016-due-soaring/.

[30] iResearch, "The monthly report about internet advertising of chinese automotive industry," in Chinese, 2016.

[31] A. Mukherjee, B. Liu, and N. Glance, "Spotting fake reviewer groups in consumer reviews," in *Proceedings of the International Conference on World Wide Web ACM*, pp. 191–200, Lyon France, April 2012.