An attention-based unsupervised adversarial model for movie review spam detection

Yuan Gao, Maoguo Gong, Senior Member, IEEE, Yu Xie, and A. K. Qin, Senior Member, IEEE

Abstract—With the prevalence of the Internet, online reviews have become a valuable information resource for people. However, the authenticity of online reviews remains a concern, and deceptive reviews have become one of the most urgent network security problems to be solved. Review spams will mislead users into making suboptimal choices and inflict their trust in online reviews. Most existing research manually extracted features and labeled training samples, which are usually complicated and time-consuming. This paper focuses primarily on a neglected emerging domain—movie review, and develops a novel unsupervised spam detection model with an attention mechanism. By extracting the statistical features of reviews, it is revealed that users will express their sentiments on different aspects of movies in reviews. An attention mechanism is introduced in the review embedding, and the conditional generative adversarial network is exploited to learn users’ review style for different genres of movies. The proposed model is evaluated on movie reviews crawled from Douban, a Chinese online community where people could express their feelings about movies. The experimental results demonstrate the superior performance of the proposed approach.

Index Terms—Movie reviews, Spam detection, Attention mechanism, Generative adversarial networks (GANs).

I. INTRODUCTION

WITH the emerging and developing of Web 2.0 that emphasizes the participation of users, consumers increasingly depend on user-generated online reviews to make purchase or investment decisions [1] [2] [3]. Online reviews enable consumers to post reviews describing their experiences with products and improve the ability of users to evaluate unobservable product quality. However, these growing text information is also full of various uncontrollable risk factors that needs to be seriously treated and managed by websites and platforms. A significant impediment to the usefulness of reviews is the existence of review spam, which is designed to give an unfair view of products and influence users’ perception of them by inflating or damaging their reputation [4] [5]. Both over-rating and under-rating affect the sales performance of products, and it is thus an important task to detect review spam to protect the genuine interests of consumers and product vendors.

In the past few years, there has been a growing interest in review spam detection from both academia and industry [6] [7]. A preliminary investigation is given in [8], where three types of review spam are identified, including untruthful reviews (reviews that maliciously promote or defame products), reviews on brands but not products, and non-reviews (e.g. advertisements). Since they have no manually labeled training instances, untruthful review detection is performed by using duplicate reviews as labeled deceptive data, and a regression model is built on these samples. Most subsequent methods utilize supervised or semi-supervised models under its influence by manually identifying review spam and extracting features [9] [10] [11]. However, it is incredibly time-consuming and impractical for service providers to label previous spammers, because a spammer will carefully craft a review that is just like other innocent reviews [12], and even a small number of incorrect annotations may bring poor results of the model. Moreover, feature identification and construction is also tricky and complicated. Therefore, it is necessary to propose an unsupervised way for review spam detection.

Most existing works on review spam detection focus on product reviews. Compared with online product review platforms, online movie review platforms appear later and thus receive little attention. This paper focuses primarily on movie review spam detection. Top reviews and online word-of-mouth have a significant impact on the box office performance of movies [13] [14], while the censorship is not strict and anyone can post reviews and express their sentiments online. Under the substantial commercial interest, more and more review spammers make deceptive critics to increase the evaluation of the target movie deliberately and discredit the competition movies arbitrarily, which will mislead users who plan to watch movies and attract publishers to put funds into review manipulation rather than filmmaking. For these reasons, detecting movie review spams is essential and urgent for the movie industry. Different from product reviews, movie reviews have the following characteristic. Due to the subjectivity of movie reviews, it is a challenging task to label them manually and therefore supervised methods are no longer applicable. Furthermore, carefully crafted deceptive reviews usually look perfectly normal, thus the artificially extracted features, such as text similarity or length of review, are ineffective. Besides, movie reviews usually entail unique movie plots or actors, which increase the burden of spam detection. As a result, spam detection of movie reviews is more challenging than that of product reviews.

To address the aforementioned challenges, the paper proposes a novel movie review spam detection method using an attention-based unsupervised model with conditional generative adversarial networks. Unlike the previous approaches for review spam detection, the presented user-centric model
can achieve outstanding performance under the circumstance of movie reviews. The characteristics of movie reviews are discussed in depth, which naturally raise several assumptions about deceptive reviews. Meanwhile, it is verified that the user’s attention (e.g. plot, actors, visual effects) are always distinct for different genres of movies. During the process of mapping reviews into low-dimensional dense vectors, the weights of feature words change adaptively according to users’ behavior in spammer detection. Generally, the selected features of models gradually changed from shallow (the length of reviews) to deep (users’ interests) with the development of deep learning techniques.

Word embedding, which is a distributed representation method, is widely used in various natural language processing (NLP) tasks, such as opinion analysis [21] [22] and sentiment classification [23] [24]. Word embedding methods represent words as continuous dense vectors in a low-dimensional space, which capture lexical and semantic properties of words. Mikolov et al. [25] proposed SkipGram, in which vectors are obtained from the internal representations from neural network models of text. It optimizes a neighborhood preserving likelihood objective using stochastic gradient descent with negative sampling. To be specific, given a sequence of training words \( s = (w_1, w_2, ..., w_{|s|}) \), the SkipGram model seeks to maximize the average log-probability of observing the context of a word \( w_i \) conditioned on its representation \( \Phi(w) \). The \( \Phi(w) \) is a mapping function that maps a word to low-dimensional dense vector, and its value is the weight from the input layer to the hidden layer of the neural network. The number of neurons in the input layer corresponds to the size of the vocabulary, and that in the hidden layer is the embedding dimension.

\[
\max_{\Phi} \quad \frac{1}{|s|} \sum_{i=1}^{|s|} \sum_{c \leq j \leq i \land j \neq 0} \log Pr(w_{i+j} \mid \Phi(w_i)),
\]

where the context is composed of words on both sides of the given word within a window size \( c \). A larger \( c \) could result in more training samples and thus lead to higher accuracy, at the expense of the training time. Introducing the randomness, dynamic window size is better than fixed one, as a central word

The remainder of this paper is organized as follows. Section II briefly presents the related backgrounds and algorithms about review spam detection, word embedding and generative adversarial networks. In Section III, clear and objective definitions of the review spam and the problem of review spam detection are given, then the details of the approach are described. Section IV shows several ways to artificially detect deceptive reviews, as well as extensive experiments to validate the effectiveness. Finally, we conclude with a discussion of the proposed framework and summarize the future work in Section V.
Spam Detection

P (Review | Movie)

User Concerns

Modified SIF Method

Movie Features Vector

Linguistic Features Vector

Word Embeddings In Reviews

Users

Reviews

Movies

Fig. 1: A graphical illustration of the review spam detection model. User concerns are embedded into the sentence embeddings leveraging modified SIF method, thus more meaningful linguistic features with attention are extracted. Several critical features of movies, such as user rating, movie genres and region, are encoded and concatenated them as the movie features vector. Afterwards, the matching relation between movies and reviews are learned to discriminate whether a particular movie-review pair is deceptive.

may be related to many or only a few words in a sentence. Since movie reviews are usually not too long in length, the window size is set to a uniform distribution of 1 to 5 in the experiment. Considering the symmetric effect over the current word and context words in the low-dimensional representation space, the conditional probability \( P_r(w_o | Φ(w_i)) \) is modeled as a softmax unit:

\[
P_r(w_o | Φ(w_i)) = \frac{\exp(Φ(w_o) · Φ(w_i))}{\sum_{w \in W} \exp(Φ(w) · Φ(w_i))},
\]

where \( w_i \) and \( w_o \) are the input and output words, and \( W \) are words in the vocabulary. The appealing, intuitive interpretation of word vectors enables them to be used in many machine learning algorithms and strategies.

Inspired by the success of generative adversarial networks [26] in the computer vision, recently, the idea of adversarial training has been extensively explored [27] [28]. The adversarially trained model is based on two different networks trained with unsupervised data. One network is the generator (\( G \)), which aims at learning the distribution over training data via a mapping of noise samples. The other one is the discriminator (\( D \)), which aims at discriminating real data from fake ones generated from \( G \). GANs are capable of learning the distribution of normal data, and then compare the abnormal data with the corresponding generated normal data for anomaly detection. They alleviate the severe problem in anomaly detection of obtaining the ground truth, and enable to detect abnormal samples by computing the difference [29] [30]. In this paper, GANs are innovatively applied to review spam detection drawing on the idea of generating reviews and discriminating spams. Specifically, \( G \) is trained to generate embedding vectors of reviews under certain conditions, while \( D \) to learn the distribution of vectors as well as the correlations between movie elements and reviews.

III. METHODOLOGY

In this section, details of the proposed model are presented. The overall architecture of the proposed model is presented in Fig. 1. At first, the SkipGram model is leveraged to learn low-dimensional dense word embeddings from all reviews, and the SIF method calculates the weighted average of word vectors in the sentence and removing the common parts of the corpus to generate sentence embeddings. In the process, user concerns are introduced and the weights of words are further adjusted according to their degree of affiliation with the concerns. The encoded movie features and sentence vectors form the review pairs together, and the conditional generative adversarial network could learn the matching relation and identify the deceptive reviews.

It begins by giving a formal definition of the review spam and the problem of review spam detection, and the inherent correlations between the user’s attention and features of movies are demonstrated. After that, it introduces the sentence vector with an attention mechanism, which has a superior performance on similarity measurement. Finally, an attention-driven conditional generative adversarial network framework is proposed, which simultaneously learns to perform review generation and attention matching.
A. Problem Statement

Review spam detection aims to train an unsupervised model which is able to detect deceptive reviews on a dataset that is highly biased towards a particular class, i.e., comprising a majority of normal non-spam reviews and only a few abnormal reviews. Let $D$ be the set of unlabeled reviews of a given user comprising $M$ reviews, $D = \{r_1, r_2, ..., r_M\}$, and additional movie information $C = \{c_1, c_2, ..., c_M\}$. Each review $r = \{w_1, w_2, ..., w_{|r|}\}$ consists of a sequence of word tokens, where $w_r \in R$ represents the $r^{th}$ token in the sentence and $R$ is a corpus of tokens. Review spam detection attempts to identify whether a review about a movie in $D$ is a spam or non-spam, given the auxiliary information (score, genres, region) of this movie.

Recent researches conclude that online reviews are valuable marketing resources for users and vendors with critical implications for a product’s success [31] [32]. In order to better distinguish between truthful and deceptive reviews, several implicit but essential assumptions are proposed in this paper, which are:

Assumption 1. Users’ historical reviews are normal and truthful, while their reviews of movies released in recent years are likely to be deceptive reviews [33] [34].

Spammers will post deceptive reviews to increase the evaluation of the target movie deliberately, and they may discredit the competition movies arbitrarily. Considering the goal of spammers is to inflate or damage the target movie’s reputation so as to affect its box office, there is no need for them to post deceptive reviews to a movie which has been taken out of theaters or released decades ago. Moreover, spammed movies only make up a small percentage of the total number of user reviews, and a few misjudgement will not have much effect on the model since the approach is attention-driven and the credibility is given by conditional probability. Different from the linear model, generative adversarial networks are not sensitive to outliers, and a small number of deceptive reviews does not change the confidence boundary [35]. The historical deceptive review will not introduce any error into the results, unless it happens to have the same condition as that of reviews in the test set. Therefore, historical reviews of a user can be utilized as truthful samples to learn the confidence boundary, and those posted in recent years serve as test samples to be detected.

Assumption 2. A normal user usually has a relatively consistent attitude toward specific actors and directors, which means a user could be a spammer if he or she gives completely opposite reviews to the same actor or director [36] [37].

Whether users like or hate an actor, their attitudes are often hard to change. Admittedly, an actor’s acting skill may improve or decrease, but it is a gradual process and is therefore acceptable to our model. However, a sudden opposite attitude towards a certain actor or director could be considered deceptive. For example, a user claims that “He is my favorite actor and I would love to see the premiere for him”, but while checking the user’s historical reviews over, it is found out that he only gives moderate reviews to the actor, and there is no doubt that this user is a spammer. On the contrary, fans of an actor may always give praise for his or her movies, regardless of the actual quality. Note that it does not mean that each opposite rating is necessarily a deceptive review. The conditional GAN is able to learn the matching relation to reviews from the input movie features, and automatically judge the potential importance of each feature. Hence, the extracted rating features may not be the deciding factors.

Assumption 3. Users will post review spam driven by benefits instead of real feelings, thus it is difficult for them to evaluate the movie from the perspective of normal reviews, and their language style or attention could be distinct from those of previous reviews of similar movies [38] [39].

The common underlying assumption for semantic-based review spam detection methods is that the language style of
deceptive reviews is different from normal ones. For movie reviews, the attention is further incorporated into the linguistic features. Because reviews always embody users’ personal tendency of the given movie [40], user’s sentimental polarities are able to be found by methods of sentiment analysis. Inspired by previous researches [41], user’s attention to a movie is further elaborated into the following four aspects: plot, visual effects, sound effects and acting skill. It is valuable for exploring attractive (and undesirable) aspects, which could help to extract additional information from reviews. In order to validate the effectiveness of the attention mechanism, the method without it, i.e. adCGAN_w/o_attention, has been proposed and compared with our model in Section IV. The method does not embed user’s attention into sentence vectors, and the conditional GAN can only utilize the matching relation between movies and reviews for spam detection.

Fig. 2 reveals that users’ attention to the four aspects varies according to the genres of movies, and different users tend to have distinct attention to these elements. For instance, user 2 is usually interested in the plot of a movie. However, he might be suspected of being a spammer if he suddenly focuses on praising or criticizing the sound effects of a Sci-Fi movie. Besides, the user profile will be clearer and more authentic by combining other features.

Similar to the users’ attention to genres of movies, their rating distributions, which indicate users’ expectations of movies in different regions, are also diverse and meaningful, as is shown in Fig. 3. Through combining movie elements and movie-related information to fuse the respective attributes into a joint model, a fine-grained user profile will be formed, and it could therefore facilitate user behavior modeling and review spam detection.

B. Sentence Embedding with Attention Mechanism

Previous work generated sentence embeddings by composing word embeddings using operations on vectors and matrices. However, the simple average of the initial word embeddings does not work very well, since common words (e.g. ‘the’, ‘and’) have the same weight as key words in the sentence. The directed inspiration for our work is the smooth inverse frequency (SIF) method [42], which computes the weighted average of the word vectors in the sentence and then removes the projections of the average vectors on their first singular vector. Especially, the word vectors are obtained from SkipGram, which is trained on the whole dataset D.

1) Feature Words of Movie Elements: After the formal definition of a user’s attention to a movie, the feature word list needs to be built. It is proved in [43] that words in reviews always converge when users comment on product features. The same conclusion could be drawn for movie reviews according to the statistical results on labeled data [36], and a few words are able to capture most features, which are saved as the main part of the feature word list.

Table I shows the basic feature words of movie elements. For a better generalization ability, five representative words for each aspect are selected in advance. Afterward, words with highest vector similarity to that in Table I are picked out, and those with high frequency in movie review corpus are added into feature word list as well. If the above feature words appear in a user’s reviews, they are perceived as his or her attention to the corresponding movie elements.

2) Modified SIF Method: The SIF method is based on the latent variable generative model [44] for text. The model regards corpus generation as a dynamic process, where the t-th word is produced at step t. The process is driven by the random sampling of a discourse vector \( v_t \in \mathbb{R}^d \), which changes over time and represents the state of the sentence. The inner product between the discourse vector \( v_t \) and the vector \( v_w \) of word \( w \) indicates the correlations between the word and the discourse. The probability of observing a word \( w \) at time \( t \) is calculated by a log-linear word production model:

\[
Pr[w \text{ emitted at time } t \mid v_t] \propto \exp(\langle v_t, v_w \rangle).
\]

### Table I: Basic feature word list of movie elements.

| Element class | Feature words                  |
|---------------|--------------------------------|
| Plot          | story, plot, script, logic, scenario |
| Visual Effect | scene, picture, scenery, shot, editing |
| Sound Effect  | music, song, sound, soundtrack, theme |
| Acting Skill  | character, role, acting, actor, cast |
All the $v_i$’s in the sentence $s$ are replaced for simplicity by a fixed discourse vector $v_s$, since the discourse vector $v_i$ does not change much \(42\).

However, some words occur out of context, and some common words often appear regardless of the discourse. Two types of smoothing terms are therefore introduced in the log-linear model. The additional term $\exp(w)$ allows words to occur even if their vectors have low inner products with $v_s$, where $p(w)$ is the unigram probability of a word in the corpus. The common discourse vector $v_0 \in \mathbb{R}^d$ serves as a correction term for the most frequent discourse that is often related to the syntax, which increases the co-occurrence probability of words that have a high component along $v_0$. Noted that though feature words $w_f$ are frequent in the entire corpus, which lead to a very large $p(w)$, there is a strong correlation between $w_f$ and $v_s$. In order to improve the connection between sentence vectors and feature words, the value of scalar $\alpha$ is constrained so that users’ attention could be better captured. Concretely, the probability of a word $w$ in the sentence $s$ is modeled by:

$$P[w \text{ emitted in sentence } s \mid v_s] = \alpha p(w) + (1 - \alpha) \frac{\exp(\langle v_s, w \rangle)}{Z_{v_s}},$$

s.t. $\alpha = 0$ if $w$ in feature word list,

(4)

where $v_s = \beta v_0 + (1 - \beta) v_s$ and $v_0 \perp v_s$. $\alpha$ and $\beta$ are hyperparameters, and $Z_{v_s} = \sum_{w \in V} \exp(\langle v_s, w \rangle)$ is the normalizing constant. The equation allows a word $w$ that unrelated to the discourse $v_s$ to be emitted according the two terms: the unigram probability in the entire corpus of the word $w$, and the correlation with the common discourse vector $v_0$. The two terms are controlled by the scalar $\alpha$, which is set to 0.95 since $p(w)$ is several orders of magnitude smaller than the latter term. A wide range of the parameter $\beta$ can achieve close-to-best results, and the value is 0.1 in the experiment, which indicates that $v_0$ is more important in corpus generation. A larger $\beta$ will magnify the role of the syntax and cause the corpus to be homogeneous.

Feature words appear frequently in the corpus thus their $p(w)$ are large, which means they could be related to the syntax and unimportant. Therefore, the value of $\alpha$ is constrained to 0 for feature words, thus they could fit closely into the main idea of the sentence $v_s$. The final sentence embedding is defined as the maximum likelihood estimation for the vector $v_s$, which is the weighted average of the word embeddings in the sentence. By referring the derivation and solving process in \(42\), the estimation for $v_s$ is approximately:

$$\arg\max \sum_{w \in s} f_w(v_s) \propto \sum_{w \in s} \frac{1 - \alpha}{1 + \alpha (1 - \beta)} v_s w,$$

s.t. $\alpha = 0$ if $w$ in feature word list,

(5)

where the partition function $Z$ is roughly the same for all $v_s$ since $v_w$ are roughly uniformly dispersed on their assumption. Since $Z$ is fixed in all directions, the weight of word in the sentence depends only on the probability $p(w)$, and word that appears more frequently has smaller weight. It leads to a down sampling of the frequent words, whereas feature words are embedded in the sentence vectors without being down sampled, so that they are able to express the theme of reviews and catch users’ attention. By calculating the first principal component of the vector $v_s$, the direction $v_0$ could be estimated. The final sentence vector $v_s$ is obtained by subtracting the projection of $v_s$ to their first singular vector $u$.

$$v_s = v_s - uu^T v_s.$$  

(6)

The latter term $uu^T v_s$ serves as the common discourse vector in the whole corpus. The coupling degree of each sentence vector is reduced by removing the common component, which further enhance the robustness and make the theme of sentences clearer.

C. Attention-driven Conditional GANs

Since there are a large number of normal reviews but few deceptive reviews, the model is supposed to learn the distribution of normal data from these samples. Based on the differences between the input test sample and normal reviews, the model could make a judgement about whether the sample is a spam or not. This approach is naturally corresponding to the idea of GANs.

Nevertheless, there are still two problems to be solved before GANs are utilized to review spam detection. Unlike traditional anomaly detection, each review corresponds to a particular movie, which means that deceptive reviews have no specific features or distribution. A review posted by this user is normal, while the identical one posted by another user could be a spam, and the same goes for different movies. On the other hand, if $D$ converges well, it will fail to discriminate between real reviews and generated ones, which is contrary to our purpose. Therefore, the theoretical model is modified motivated by the above empirical observation. Although a single review cannot be judged to be truthful or deceptive, whether it follows the writing style that the user developed on similar movies before is a key entry point. The model draws on the idea of conditional GANs \(27\) and set the movie’s additional information as conditions, and each user’s data is trained into a separate model. Moreover, the architectural details of $G$ and $D$ are referred to \(28\), considering the superiority of the Wasserstein GAN. Towards more efficient modeling, the conditional GAN changes as follows, whose architecture is shown in Fig. 4.

**Generator.** Given the joint distribution $P(v, c_g)$ of sentence vectors $v$ and conditions $c_g \in C$ from real samples, $G$ aims to learn a parameterized conditional distribution $P(v, z, c_g, \theta_g)$ that best approximates the true distribution. The prior input noise vectors $z$ and additional information $c_g$ are combined in joint hidden representation, and the adversarial training framework allows for considerable flexibility in how the hidden representation is composed. The generated sentence vector is conditioned on the network parameters $\theta_g$, noise vectors $z$ and generator conditions $c_g$. The loss for $G$ is defined as:

$$L_G = -E_{z \sim P_z(z)} [D(G(z \mid c_g) \mid c_g)],$$

(7)

where the noise vector $z$ is drawn from a noise distribution $P_z(z)$, and $G(z \mid c_g)$ are sentence vectors generated by noise $z$ under generator conditions $c_g$. The goal of the generator $G$ is to generate as realistic reviews as possible. Therefore, it achieves the optimal performance if the discriminator $D$
cannot distinguish real reviews from the generated ones, i.e. the output of discriminator $D(G(z|c_g)|c_g)$ is close to 1. In the process, $G$ and $D$ work under the same conditions $c_g$, which means that they only focus on the linguistic features of reviews.

**Discriminator.** The sentence vector $v$ and the condition $c_d$ are concatenated as the input of $D$, where $v$ is identified whether it is real or fake by computing the probability $Pr(v|c_d, \theta_d)$. Since the ultimate goal is to detect whether a review is deceptive through $D$, it is therefore necessary to avoid the problem of being unable to distinguish real reviews from generated ones after sufficient training. Different conditions for $G$ and $D$ are creatively deployed during their training, so that the model is able to learn the distribution of review vectors as well as the correlations between conditions and reviews concurrently, which is assumed to be critical in Section III. The loss for $D$ is defined as:

$$\mathcal{L}_D = \mathbb{E}_{z \sim P_z(\varepsilon)} [D(G(z|c_g)|c_d)] - \mathbb{E}_{x \sim P_{data}(x)} [D(x|c_d)].$$

(8)

On the condition of $c_d$, $D$ is supposed to identify the matching reviews $x$ as real, and the generated reviews $G(z|c_g)$ that match $c_g$ as fake. In other word, for the discriminator $D$, the best outcome is to predict $D(x|c_d)$ to be 1 and $D(G(z|c_g)|c_d)$ to be 0. Fake reviews vectors are produced under generator conditions $c_g$, while they are concatenated to discriminator conditions $c_d$ and labeled fake. Noted that real review vectors $x$ are matched to $c_d$, which is resampled from the dataset and completely different from $c_g$. As mentioned above, generated reviews are real under the condition of $c_g$ while they are fake under the condition of $c_d$, as users’ attention varies with different genres of movies, corresponding to the fact that a spammer usually cannot evaluate the movie from the perspective of normal reviews. In this way, $D$ could identify a review to be fake or deceptive if it does not match the context or the style of historical reviews.

**IV. EXPERIMENTS**

In this section, the proposed model is compared with six state-of-the-art anomaly detection methods in terms of precision, recall and F1-measure. Before evaluating the performance of the proposed approach, where and how to collect the dataset are discussed.

**A. Dataset**

In this paper, all reviews are collected from Douban, a huge Chinese online community where uses share their reviews to express their feelings about movies and score the movies with one star to five stars. Although the approach and the comparison algorithms are unsupervised, reviews need to be manually labeled in order to verify the effectiveness of the models. Therefore, several ways to identify spammed movies and reviews are explored as follows.

Due to the fact that spammers tend to give extreme ratings when they praise or criticize a movie driven by benifits, it is assumed that the distribution of ratings of normal movies is different from that of spammed movies, whose tendency toward polarization is more noticeable. Hence the Wasserstein metric is leveraged to find outliers in the distribution of ratings, which are suspected of being deceptive. Wasserstein metric is a distance function defined between probability distributions, and the distance between similar distributions is smaller. The Wasserstein distance between each movie and the datum reference is calculated, and the datum reference is the mean of ratings of all movies with same Douban score as the current one. The results are reported in Fig. 5.

It is evident that *The Wandering Earth* is much larger than 2012 on the proportion of one-star ratings and five-stars ratings, though their Douban score and genres of movies are similar. The word-of-mouth of *The Wandering Earth* is polarised, which leads to a larger Wasserstein distance, hence it is more suspected of being deceptive. Moreover, the proportions of reviews with different ratings over time are investigated, as shown in Fig. 6.

Fig. 4: Architecture of the modified conditional GAN. A batch of movie features are sampled and fed into the generator as conditions, in order to generate the reviews. Then another batch of movie features and the corresponding reviews are resampled from the training set and denoted as real. On the contrary, the resampled movie feature and generated review pairs are labeled fake. The discriminator is able to learn both linguistic features from reviews and the matching relation from these pairs, and therefore to identify deceptive reviews that does not match the linguistic style or the context.
Fig. 5: The distribution of the Wasserstein distance between ratings of movies and the mean value, where the black dot 2012 and the red dot *The Wandering Earth* are highlighted.

Fig. 6: The proportion of positive reviews, moderate reviews and negative reviews of *The Wandering Earth* over time.

It can be seen that the distributions of positive reviews and moderate reviews are roughly in line with that of all reviews, but most negative reviews are concentrated on February 5th, when *The Wandering Earth* was released. It is also consistent with the analysis of the features of spammers that they will influence users' perception of movies by posting biased reviews when the movie is released. Combining the Wasserstein distance, the proportion of ratings and users’ view, six spammed movies are identified, including *The Wandering Earth*.

Douban displays 500 positive reviews, 500 moderate reviews and 500 negative reviews for each movie as top reviews. In determining specifically whether a review is deceptive, we solicit the help of five volunteer graduate students to make independent judgements on the dataset. The criteria for review spam come from *30 Ways You Can Spot Fake Online Reviews* [2] which provides some techniques to spot deceptive online reviews. Besides, the features of review spam presented in Section III are also utilized as a reference. In addition, The user review weighting system of Douban platform offers great help. In order to avoid the spammers’ manipulation in the word-of-mouth of movies, Douban platform developed a weighting system for users’ reviews and ratings according to the daily behaviors of users. Therefore, the help votes (how many people think that review is helpful) and the ranking in the review list are also considered as the judgement bases of review spam. The ranking of reviews by the help votes and the ranking of Douban are compared, and the differences in position in sorting are viewed as the suspicion level. More specifically, a review is more likely to be deceptive if it has numerous help votes but ranks low on Douban. The paper collects 13,056 reviews from 3,261 users on nine movies as the test set, in which 10,268 are truthful reviews and 2,788 are deceptive, then the rest of historical reviews of these users are used for training.

Fig. 7 shows that most users in the dataset posted more than 500 movie reviews, which facilitate us to mine their viewing preferences and review styles. Besides, through the meticulous investigation and analysis of users’ interest in watching movies, six critical features are defined as conditions for generating user reviews, as illustrated in Table II. These features are encoded in different ways and concatenated to embedding vectors of review, and the dimension of that is set 100. The average director score means the average of user’s ratings for previous movies of this director that user has rated.

2[https://consumerist.com/2010/04/14/how-you-spot-fake-online-reviews](https://consumerist.com/2010/04/14/how-you-spot-fake-online-reviews)
Fig. 7: The visualization of the number of reviewed movies and the log of rated movies for users.

| Conditions        | Encoding mode         | Dimension |
|-------------------|-----------------------|-----------|
| Movie score       | Real-Number Encoding  | 1         |
| User rating       | Real-Number Encoding  | 1         |
| Region            | One-Hot Encoding      | 4         |
| Movie genres      | One-Hot Encoding      | 20        |
| Average director score | Real-Number Encoding | 1         |
| Average actor score    | Real-Number Encoding | 1         |

or commented, and the average actor score is also calculated in this way.

B. Baselines and Parameter Settings

Since the paper is the first to do research on the movie review spam detection and innovatively propose the attention mechanism of reviewers, it is impractical and unfair to directly compare with other review spam detection algorithms that focus on the product. Moreover, all of these review spam detection algorithms are supervised or semi-supervised, to the best of our knowledge. Therefore, the condition vectors mentioned in Section IV-A are concatenated with the review vectors together and six state-of-the-art unsupervised outlier detection algorithms are evaluated on the dataset.

| Conditions   | Encoding mode         | Dimension |
|--------------|-----------------------|-----------|
| Movie score  | Real-Number Encoding  | 1         |
| User rating  | Real-Number Encoding  | 1         |
| Region       | One-Hot Encoding      | 4         |
| Movie genres | One-Hot Encoding      | 20        |
| Average director score | Real-Number Encoding | 1         |
| Average actor score    | Real-Number Encoding | 1         |

or commented, and the average actor score is also calculated in this way.

Multi-class SVM (MCSVM) \cite{47} \cite{48} is a non-probabilistic binary linear classifier. It follows a similar setting with OCSVM. As multi-class SVM cannot handle the case that the labels of all training samples are consistent, unmatched movie-review pairs, which are introduced in the training of the discriminator $D$, serve as the fake samples.

Minimum Covariance Determinant (MCD) \cite{49} is a distributional fit to Mahalanobis distances which uses a robust shape and location estimate. The MCD of data points is the mean and covariance matrix based on the sample of a size that minimizes the determinant of the matrix. The contamination, which controls the proportion of abnormal samples, is 0 in the dataset.

Isolated Forest (iForest) \cite{50} builds an ensemble of isolated trees for a given dataset, then anomalies are those instances which have short average path lengths on the isolated trees. It detects anomalies based on the concept of isolation without employing any distance or density measure. There are two variables in this method: the number of trees to build and the sub-sampling size, and they are set to 100 and 256 respectively depending on the size of the dataset.

Variational Autoencoder (VAE) \cite{51} uses reconstruction probability in anomaly detection. It utilizes the generative characteristics of the variational autoencoder to derive the reconstruction of the data, thus it could analyze the underlying cause of the anomaly. The network structure of the encoder and decoder is set similarly to that of the generator and discriminator.

C. Complexity Analysis and Efficiency Evaluation

In the proposed algorithm, the preprocessing of reviews, i.e., the sentence embedding, for both training and testing phase consist of two part, respectively corresponding to the SkipGram model and the SIF method. Specifically, the computational complexity of SkipGram is $O(c\gamma l \log n)$, where $c$ is the window size, $n$ is the total number of words, $\gamma$ is the number of sampling and $l$ is the length of the sampling sequence. For the SIF method, its complexity is $O(msd)$, in which $s$ is the
number of sentences, \( m \) is the average number of words in each sentence, and \( d \) is the embedding dimension. The total number of words \( n \) is larger than the product of \( m \) and \( s \), since there will be repeated words in sentences.

For the conditional GAN, the computational complexity can be represented as \( O(DET/B) \), in which \( D \) is the number of training samples, \( E \) represents epochs, \( B \) is the batch size, and \( T \) is the computational complexity in each iteration. The generator and discriminator are composed of fully connected layers, dropout, batch normalization and the activation functions, with fully connected layers taking up most of the operation time. Therefore, \( T \) can be further expressed as \( O(T) \approx O(\sum_{i=2}^{L} N_i N^{i-1}) \), in which \( N^i \) is the number of neurons in the \( i \)-th layer, and \( L \) is the number of layers in the network.

The computational complexity of neural network is hard to accurately describe due to many free variables, so the number of floating-point operations (FLOPs) is introduced to show the complexity of the model intuitively. The FLOPs of fully connected layers can be computed as:

\[
FLOPs = (2I - 1)O,
\]

where \( I \) is the input dimensionality and \( O \) is the output dimensionality. Similar to the computational complexity, the time consumption of batch normalization and activation functions are not taken into account, since they are negligible compared with fully connected layers. The number of parameters and FLOPs are reported in Table III.

| Module   | Layer | Parameters | FLOPs  |
|----------|-------|------------|--------|
| Generator | fc-1  | 33,024     | 65,536 |
|          | fc-2  | 131,584    | 262,144|
|          | fc-3  | 131,328    | 262,144|
|          | output| 25,700     | 51,200 |
|          | total | 321,636    | 641,024|
| Discriminator | fc-1  | 33,024     | 65,536 |
|           | fc-2  | 32,896     | 65,536 |
|           | fc-3  | 8,256      | 16,384 |
|           | output| 65         | 147,584|
|           | total | 74,241     | 147,584|

There are 395,877 trainable parameters for the conditional GAN, and the total number of FLOPs of the model is 788,608. The computational efficiency is evaluated on a NVIDIA Tesla V100 GPU. In the training phase, the mini-batch SGD [52] is employed as the optimizer, and the batch size is set to 128. It takes less than 15ms for the training of a mini batch of samples in each iteration, including the forward and backward propagation. In the testing phase, the inference process for each review can be completed in 0.1ms, as it only requires one forward propagation of the discriminator, which ensures a real-time online review spam detection.

The computational efficiency is evaluated on a NVIDIA Tesla V100 GPU. In the training phase, the mini-batch SGD [52] is employed as the optimizer, and the batch size is set to 128. It takes less than 15ms for the training of a mini batch of samples in each iteration, including the forward and backward propagation. In the testing phase, the inference process for each review can be completed in 0.1ms, as it only requires one forward propagation of the discriminator, which ensures a real-time online review spam detection.

**D. Results**

Before comparing with other algorithms, the effectiveness of the proposed method is verified. Vectors mapped by reviews utilizing the modified SIF method are aggregated, and the nearest neighbor approach is used to find out whether a review has the same rating as its neighbors. For reviews with the same rating, multiple tests are conducted to ensure the accuracy of the experiment, and the results are represented by the proportions of neighbors with different ratings.

The secondary diagonal of the similarity matrix in Fig. 8 represents an accurate clustering in the five-star rating system, and it indicates that the embedding method is able to maintain the original attributes and meaning of the positive review and negative review. Because of the strong subjectivity of users’ ratings and reviews, it does not perform well on clustering moderate reviews, but it can still roughly assess a reviewer’s attitude toward the movie. On this basis, the additional information and review vectors are fed into the conditional GAN for training and learning. Noted that the loss functions of \( \mathcal{G} \) and \( \mathcal{D} \) are not following those of the original conditional GAN. They work together to identify fake reviews instead of competing with each other, and the loss curve is shown in Fig. 9.

\( \mathcal{G} \) aims to fool \( \mathcal{D} \) and let it judge the generated vectors to be true, and the loss of \( \mathcal{G} \) reaches the minimum value at around 10,000 epochs, which means generated vectors can completely deceive \( \mathcal{D} \). The goal of \( \mathcal{D} \) is to distinguish between real reviews that match conditions and generated reviews that do not. For example, a one-star review which is full of praise is undoubtedly a fake review. Since conditions are randomly assigned to generated vectors, it is inevitable that random condition is similar to the real condition, especially for users who have single viewing preference and rating habit. Therefore, \( \mathcal{D} \) is better at identifying real samples than fake ones, as illustrated in Fig. 9(b).

Afterward, the performance of the algorithm is evaluated on the dataset crawled from Douban. Several standard evaluation metrics are adopted: accuracy, precision, recall and F1-score, which are computed using a micro-average, i.e., from the aggregate true positive, false positive and false negative rates,
as suggested in [53]. The above evaluation metrics of truthful samples and deceptive samples are computed respectively, and the comparison results between our model and state-of-the-art methods are shown in Table IV.

It is clear that the proposed adCGAN achieves the best performance in terms of accuracy, precision and F1-score on both truthful and deceptive reviews. Since the training samples may contain some deceptive reviews, linear models, which map the data and learn their boundaries (e.g. OCSVM, MCSVM and MCD), have poor performance on review spam detection. Note that OCSVM achieves the highest recall rate for truthful reviews but the lowest recall rate for deceptive ones, which means that support vector machines indiscriminately identify a majority of the testing samples as truthful due to the wrong boundaries. Leveraging unmatched movie-review pairs, MCSVM performs a little better than OCSVM, but it still faces the problem of identifying most of the deceptive reviews as truthful ones. For iForest, a random dimension is selected to build a tree, but a large amount of dimension information is not utilized, which are not mutually independent in review vectors, resulting in reduced reliability of the algorithm. To our surprise, another simple density-based model, LOF, is able to detect a majority of deceptive reviews, though it comes at the cost of minimal accuracy. The VAE architecture detects outliers by calculating reconstruction probability. The difference between VAE and adCGAN is that many generated samples with fake conditions are leveraged in the presented approach in the process of judgement (reconstruction), which is equivalent to demarcate the data in the original space and conducive to learning their distribution. Moreover, the result of the model without attention mechanism (adCGAN_w/o_attention) demonstrates the assumptions in Section III that a normal user usually has relatively consistent attention towards specific movies. The presented adCGAN can not only generate highly effective vectors whose distribution is close to that of real review vectors, but also determine if a movie review is derived from the corresponding additional information, and hence it achieves significantly better performance than baseline algorithms.

### V. Discuss, Implication, and Conclusion

In this paper, a novel adCGAN model is developed for movie review spam detection. To address the problem of lacking labeled training samples, a new implementation of GAN is introduced by resampling conditions from the dataset. It also leverages the attention mechanism to facilitate GAN to capture the correlations of movie-review pairs, which improves the accuracy of the model. The experimental results on Douban dataset demonstrate the superior performance on movie review spam detection.

![Fig. 9: The loss and discriminant probability of the conditional GAN.](image-url)
The idea of unmatched training pairs and the attention mechanism can be migrated to various review spam detection, such as literature reviews and other types of reviews that reflect users’ consistent interests. However, it may not be well suited to product reviews, since they are more related to the quality of product, while the adCGAN model is user-centric and focuses on user preference. Furthermore, it is necessary for the proposed method to set the feature words manually, thus element class and feature words need to be reinvestigated for other types of reviews, which limits the generality of the model.

The following directions can be explored in the future:
(1) The paper has investigated the effectiveness of adCGAN on movie review spam detection. The generalization ability of the model can be further improved by mining the inherent attributes of reviews, in order to make it scalable for other types of review spam detection.
(2) The adCGAN model could simultaneously capture review styles and viewing preferences, which are embedded in the weight of GAN. It is attractive to extract the rich information in the follow-up work and leverage it in recommendation systems.

REFERENCES
[1] A. Y. Chua and S. Banerjee, “Helpfulness of user-generated reviews as a function of review sentiment, product type and information quality,” Comput. Human Behav., vol. 54, pp. 547–554, 2016.
[2] G. Zhao, X. Lei, X. Qian, and T. Mei, “Exploring users’ internal influence from reviews for social recommendation,” IEEE Trans. Multimedia, vol. 21, no. 3, pp. 771–781, 2018.
[3] X. Li, C. Wu, and F. Mai, “The effect of online reviews on product sales: A joint sentiment-topic analysis,” Inf. Manag., vol. 56, no. 2, pp. 172–184, 2019.
[4] N. Hu, I. Bose, Y. Gao, and L. Liu, “Manipulation in digital word-of-mouth: A reality check for book reviews,” Decis. Support Syst., vol. 50, no. 3, pp. 627–635, 2011.
[5] N. Hu, L. Liu, and V. Sambamurthy, “Fraud detection in online consumer reviews,” Decis. Support Syst., vol. 50, no. 3, pp. 614–626, 2011.
[6] R. K. Dewang and A. K. Singh, “State-of-art approaches for review spammer detection: a survey,” J. Intell. Inf., vol. 50, no. 2, pp. 231–264, 2018.
[7] H. Xue, Q. Wang, B. Luo, H. Seo, and F. Li, “Content-aware trust propagation toward online review spam detection,” ACM J. Data Inf. Qual., vol. 11, no. 3, pp. 1, 2019.
[8] N. Jindal and B. Liu, “Opinion spam and analysis,” in Proc. 1st Int. Conf. Web Search Data Min., 2008, pp. 219–230.
[9] D. Mayzlin, Y. Dozer, and J. Chevalier, “Promotional reviews: An empirical investigation of online review manipulation,” Am. Econ. Rev., vol. 104, no. 8, pp. 2421–55, 2014.
[10] N. Saitani, K. Adi, and M. S. Allili, “A supervised approach for spam detection using text-based semantic representation,” in Proc. 3rd Int. Conf. E-Technol., 2017, pp. 136–148.
[11] F. Khursheed, Y. Zhu, C. W. Yohannese, and M. Iqbal, “Rectical of supervised learning on review spam detection: An empirical analysis,” in Proc. 12th Int. Conf. Intell. Syst. Knowl. Eng., 2017, pp. 1–6.
[12] M. Ott, Y. Choi, C. Cardie, and J. T. Hancock, “Finding deceptive opinion spam by any stretch of the imagination,” in Proc. 49th Assoc. Comput. Linguist. Human Lang. Technol., vol. 1, 2011, pp. 309–319.
[13] H. Ma, J. M. Kim, and E. Lee, “Analyzing dynamic review manipulation and its impact on movie box office revenue,” Electron. Commer. Res. Appl., vol. 35, p. 100840, 2019.
[14] R. Legoux, D. Larocque, S. Laporte, S. Belmahi, and T. Bouquet, “The effect of critical reviews on exhibitors’ decisions: Do reviews affect the survival of a movie on screen?” Int. J. Res. Mark., vol. 33, no. 2, pp. 157–374, 2016.
[15] M. Crawford, T. M. Khoshgoftaar, J. D. Prusa, A. N. Richter, and H. Al Najada, “Survey of review spam detection using machine learning techniques,” J. Big Data, vol. 2, no. 1, p. 23, 2015.
[40] Q. Sun, J. Niu, Z. Yao, and D. Qiu, “Research on semantic orientation classification of Chinese online product reviews based on multi-aspect sentiment analysis,” in Proc. 3rd IEEE/ACM Int. Conf. Big Data Comput. Appl. Technol., 2016, pp. 262–267.

[41] T. T. Thet, J. Na, and C. S. Khoo, “Aspect-based sentiment analysis of movie reviews on discussion boards,” J. Inf. Sci., vol. 36, no. 6, pp. 823–848, 2010.

[42] S. Arora, Y. Liang, and T. Ma, “A simple but tough-to-beat baseline for sentence embeddings,” in Proc. 5th Int. Conf. Learn. Represent., 2017.

[43] M. Hu and B. Liu, “Mining and summarizing customer reviews,” in Proc. 10th ACM SIGKDD Int. Conf. Knowl. Discov. Data Min., 2004, pp. 168–177.

[44] S. Arora, Y. Li, Y. Liang, T. Ma, and A. Risteski, “A latent variable model approach to pmi-based word embeddings,” Trans. Assoc. Comput. Linguist., vol. 4, pp. 385–399, 2016.

[45] M. M. Breunig, H. P. Kriegel, R. T. Ng, and J. Sander, “LOF: identifying density-based local outliers,” in Proc. 6th ACM SIGMOD Int. Conf. Manag. Data, vol. 29, no. 2, 2000, pp. 93–104.

[46] B. Schölkopf, J. C. Platt, J. Shawe Taylor, A. J. Smola, and R. C. Williamson, “Estimating the support of a high-dimensional distribution,” Neural comput., vol. 13, no. 7, pp. 1443–1471, 2001.

[47] Y. Liu and Y. F. Zheng, “One-against-all multi-class SVM classification using reliability measures,” in Proc. 2005 IEEE Int. Joint Conf. Neural Netw., vol. 2, 2005, pp. 849–854.

[48] M. Quinn and J. I. Olszewski, “British sign language recognition in the wild based on multi-class SVM,” in Proc. 2019 Fed. Conf. Comput. Sci., Inf. Syst., 2019, pp. 81–86.

[49] J. Hardin and D. M. Rocke, “Outlier detection in the multiple cluster setting using the minimum covariance determinant estimator,” Comput. Stat. Data Anal., vol. 44, no. 4, pp. 625–638, 2004.

[50] F. T. Liu, K. M. Ting, and Z. Zhou, “Isolation forest,” in Proc. 8th IEEE Int. Conf. Data Min., 2008, pp. 413–422.

[51] J. An and S. Cho, “Variational autoencoder based anomaly detection using reconstruction probability,” Spec. Lect. IE, vol. 2, pp. 1–18, 2015.

[52] M. Li, T. Zhang, Y. Chen, and A. J. Smola, “Efficient mini-batch training for stochastic optimization,” in Proc. 20th ACM SIGKDD Int. Conf. Knowl. Discov. Data Min., 2014, pp. 661–670.

[53] G. Forman and M. Scholz, “Apples-to-apples in cross-validation studies: pitfalls in classifier performance measurement,” ACM SIGKDD Explor., vol. 12, no. 1, pp. 49–57, 2010.