WILEY | Hindawi

Research Article

Research on Fake News Detection Based on Diffusion Growth Rate

Jinyin Chen,[1,2] **Chengyu Jia,**[2] **Qinfeng Li,**[2] **Haibin Zheng,**[1,2] **Wenhong Zhao,**[3] **Mingyuan Yan,**[4] **and Changting Lin** [5,6]

[1]*Institute of Cyberspace Security, Zhejiang University of Technology, 310023, China*
[2]*College of Information Engineering, Zhejiang University of Technology, 310023, China*
[3]*College of Information Engineering, Jiaxing Nanhu University, 314001, China*
[4]*Mike Cottrell College of Business, University of North Georgia, GA 30597, USA*
[5]*Zhejiang University, 310014, China*
[6]*Binjiang Institute of Zhejiang University, 310014, China*

Correspondence should be addressed to Changting Lin; linchangting@gmail.com

With the rapid development of the Internet, social media has become a convenient online platform for users to obtain information, express opinions, and communicate with each other. Users are keen to participate in discussions on hot topics and exchange opinions on social media. A lot of fake news has also arisen at this moment. However, existing fake news detection methods have the problem of relying too much on textual features. Textual features are easy to be tampered with and deceive the detector; thus, it is difficult to distinguish fake news only by relying on textual features. To address the challenge, we propose a fake news detection method based on the diffusion growth rate (Delta-G). To identify the real and fake news, Delta-G uses graph convolutional networks to extract the diffusion structure features and then adopts the long-short-term memory networks to extract the growth rate features on time series. In the experiments, Delta-G is verified on two news datasets, Twitter and Weibo. Compared with the three detection methods of decision tree classifier, support vector machines with a propagation tree kernel, and RvNN, the accuracy of the Delta-G on the two datasets is improved by an average of 5% or more, which is better than all the baselines.

1. Introduction

Recently, followed by the rapid growth of the Internet, social media is widely used as a platform on which people can capture information, express opinions, and communicate with one another. However, fake news also arises as more and more people devote themselves to the discussion of popular topics and share their views on social media. To draw people's attention, fake news tends to provide the public with more novel views and special information [1], to trigger people's curiosity and motivate them to spread fake news further. Thus, they realize the specific wicked purpose of the malicious publisher greatly harms society and causes tremendous financial loss. The Pew Research Center of America has researched the origin from which the Americans get the news in 2018, and the result shows that about 66% of Americans capture information via social media, while 57% of them regard that information as inaccurate [2]. This means that the online fake information has been widely infiltrated into the lives of netizens and has also been widely recognized by them. Just like an opinion rose by Lewandowsky et al. [3], "Democracy relies on the well-trained public," which indicates even though a little proportion of people have received fake news, sociopolitical decisions that violate the public's interest could be made. For instance, a piece of fake news about swine flu posted on Twitter in 2009 has put people in Texas and Kansas into panic [4], while another post on Weibo claims that iodized salt could protect people

from nuclear radiation caused millions in China to rush to supermarkets for salt and soy sauce [5]. With the rapid development of social media, such phenomena are no longer rare incidents on social media; the news could be spread before getting through the examination of disciplined journalists [6]. Therefore, a method that could detect the spreading of fake news with efficiency is critical in protecting people from the potential threat caused by fake news.

The existing fake news detection method works based mainly on key features such as training the binary classifier with the user's characteristics [7–9], message contents, and the spread patterns. Commonly used classifiers include support vector machine (SVM) [10], random forest (RF) [11], and decision tree [12]. Besides, more features like user's comments, time series structures, and emotional attitudes are included in detection. Nevertheless, these methods rely mainly on feature engineering, which is extremely laborious. Moreover, these manually crafted features often rely excessively on specific data, which is short of higher-order features; thus, the applicability of them is quite limited.

Recently, a series of fake news detection methods based on deep learning has risen. These methods mine higher-order features through textual content and the propagation path, respectively, and thereby distinguish fake news. Nevertheless, the difference in textual features between real news and fake news is usually quite small. Figure 1 represents the contrast of a piece of real and fake news on the same topic. They both describe the content related to Nepal's earthquake and have a vivid image. However, the first post is a piece of fake news while the second one is real news. The first image is from other events, but it is difficult for ordinary users to distinguish the authenticity of the source of the image. These kinds of knowledge would seldom be acquired by ordinary people, which explains why innocent people might forward fake news and spread them out unconsciously. For computers, since both posts have fairly similar keywords, such as "Nepal" and "earthquake," it makes the detection of fake news via textual features even harder. It is normal for existing natural language processing technology to mix these two posts given their similarity. Therefore, more and more studies have tried to verify the authenticity of news by features beyond its contents. Research shows that the diffusion structure between real and fake news is different in nature; thus, many studies have been conducted to identify fake news by mining the structural features of information in the process of diffusion [13–15]. A natural thought would be utilizing graph convolutional networks (GCN) to extract the topological features in the diffusion process [16–18]. In the process of feature extraction, GCN would collect the features of every adjacent node and aggregate the local information for each node. However, the feature information used in the aggregation of adjacent nodes is some overall statistical features based on information within the social context, such as the total number of retweets and the number of followers, while ignoring the changes in these features over time.

According to a study published in *Science*, fake news tends to spread faster than real news. This research demonstrates that the conclusion above applies to all kinds of news. It is about six times faster for a tweet with fake content to be spread to 1,500 people than that without. This experiment further confirms the thesis of this paper, i.e., the features of time series are critical in discriminating authentic news from fakes.

Since the fake news detection model relies excessively on textual features while the characteristic of time series is likely to be ignored, we propose a fake news detection method based on the growth rate of news diffusion, Delta-G. To be specific, the first step is to utilize GCN to extract the topological features between different time intervals in the process of diffusion. Then, the diffusion features would be input into the long-short-term memory networks (LSTM) for further extraction of growth rate features in time series and detect the fake news. Compared with fake news detection methods based on diffusion structures, Delta-G further includes the time series structures of the news spreading, which could identify fake news more efficiently.

The contributions of this paper are summarized as follows:

(i) Since the fake news detection model relies excessively on textual features and the characteristic of time series is likely to be ignored, a fake news detection method delta-G based on the growth rate of diffusion is proposed

(ii) Compared with fake news detection methods based on diffusion structure, Delta-G utilizes GCN for feature extraction while aggregating the time series structures of the diffusion, which could effectively identify fake news

(iii) Extensive experiments demonstrate that Delta-G shows 86.4% and 90.8% accuracy on Twitter and Weibo datasets, respectively, outperforming existing baselines

2. Related Works

In the study of fake news detection, some researchers adopt the idea of feature extraction. They extract expression and diffusion features of fake news concluded by experts or their experiences, followed by the real/fake classification via machine learning technics such as SVM and RF [19–21]. Their shortage is the manual information extraction, i.e., it cannot automatically extract features from a large amount of online data. Nowadays, benefiting from the development of deep learning, artificial intelligence has increased its popularity globally, which makes it possible for detecting fake news automatically. One of the core concepts of deep learning is adopting distributed representation scheme and automatically learning and extracting semantic features from a wide range of texts. Distributed representation learning can solve the problem of semantic computation between objects in the area of social computing, mapping text, user, and objects to a unique lower degree vector semantic space. This process enables AI to automatically mine features from tremendous data on the Internet and measure whether the

(a) Fake news about Nepal's earthquake

(b) Real news about Nepal's earthquake

Figure 1: Comparison between fake news and real news about Nepal's earthquake.

news is real, without the requirement for experts to manually conclude the features [22–24].

At present, many engineers abroad are working on the autodetection of fake news. According to the method used for feature extracting, the fake news detection methods could be divided into two classes: methods based on feature engineering or deep learning. Meanwhile, they could also be classified according to the input features of different sources, i.e., methods based on the context of news or social circumstances [25]. Among these, the method based on the context of news could be divided into knowledge-based or style-based, while the context of social circumstance could be divided into standpoint-based or diffusion-based.

2.1. Detection Based on the News' Content. Since fake news has the intention to hide faulty information in news, therefore, the most direct detection method to verify the authenticity of news is to examine the authenticity of all important information in news. Knowledge-based methods are essentially made use of external sources and check whether the opinion proposed is true. The goal of fact-checking is to distribute true value to opinions in a specific context [26]. People have paid increasing attention to fact-checking, and many effects have been devoted to the development of a feasible system of automatic fact-checking. The existing fact-checking method could be categorized into expert-oriented, crowd-oriented, and computation-oriented. Expert-oriented fact-checking methods rely heavily on certain data and documents investigated by experts in the area of mankind; such websites include PolitiFact and Snopes. Nevertheless, expert-oriented fact-checking requires a high level of intelli-

gence and is fairly time-consuming, which indicates it would be low in efficiency and limited in adaptability. Crowd-oriented fact-checking, on the other hand, arises from the idea of "swarm intelligence," which enables ordinary people to comment on news, after which those notes would be analyzed collectively and provide the overall judgment on the authenticity of the news. For instance, Fiskkit enables users to discuss and denote the accuracy of certain parts of the news, while an antifake news robot called "For Real," which turns out to be a public account of an instant communication app, LINE, enables users to report suspicious news, which would be further investigated by editors. Lastly, a computation-oriented method provides a self-extending system to detect fake news, which is mainly based on the knowledge of open networks and structured knowledge maps, and tests whether the claim of news could be derived from existing facts [27–29].

Most publishers of fake news would write in a specific manner and spread misleading information to attract and persuade a wide range of consumers, which would not likely be the case in real news. Therefore, manner-based detection method attempts to capture the specific manipulator of the writing manner. Recently, an advanced natural language processing model is applied to recognizing fake news from its deep parsing and rhetorical structure. The deep paring model is realized through the probabilistic context-free grammars (PCFG), which could transform sentences into the description of syntactic stylometry. Based on PCFG, several rules for detecting fake news could be developed, such as the rule of production of lexicalize/unlexicalized and the rule of grandparents [30]. The theorem of rhetorical structure

can distinguish the validity of news [31]. A deep network model, such as convolutional neural network (CNN), has also been applied in the field of fake news classification [32]. Kaliyar et al. [33] propose a BERT-based (Bidirectional Encoder Representations from Transformers) deep learning approach by combining different parallel blocks of the single-layer deep CNN having different kernel sizes and filters with the BERT. Nasir et al. [34] propose a novel hybrid deep learning model that combines convolutional and recurrent neural networks for fake news classification. Objective-oriented methods are aimed at capturing features that could represent the objectivity of the news. News that violates this principle could be in the manner of extremist parties or so-called clickbait news. The style of extreme partisan style represents extreme behaviour in favouring of a particular party, which turns out to be one of the most common intentions of making up fake news. These articles could be detected by their linguistic features [35]. Clickbait news refers to the news with exaggerated and sensational eye-catching topics instead of adequate research, while real news topic is merely the refining of the author's main arguments. As a result, exaggerated and sensational eye-catching topics appear to be an important feature in detecting fake news [36].

2.2. Detection Based on Social Background. The method based on social background intends to infer the authenticity of original news articles via users' viewpoints on relevant posts. The standpoint of the posts could either be explicit or implicit. An explicit standpoint is the direct expression of emotion or viewpoint, while an implicit standpoint could automatically be extracted from posts on social media. The definition of standpoint detecting is the task of automatically determining whether the user is approved, neutral, or against some target entity, incident, or opinion [37]. Previous standpoint classification methods depend mainly on hand-made embedding features to detect standpoint [38]. The approach of the theme model, such as Latent Dirichlet Allocation (LDA) [39], could learn the potential standpoint from the theme. Altogether, these approaches could infer the accuracy of the news from the standpoint of news of relevant topics. Tacchini et al. [40] have proposed a binary network between user and posts on Facebook that rely on the standpoint of "like" or "dislike." Based on this network, a semisupervised probability model is developed to predict the likelihood for a post to be spite. Jin et al. [39] investigated the topic model to understand potential information in viewpoint and further utilize these viewpoints to test the authenticity of relevant posts and news.

Fake news detection methods based on diffusion determine the reliability of news via its interrelation with relevant posts on social media. These methods take the hypothesis that the reliability of news is highly correlated with relevant posts on social media. Isomorphic and heterogeneous trusted networks can be constructed to monitor the process of diffusion. The isomorphic trusted network consists of entities of a single type, like posts or events. While heterogeneous trusted network involves entities of different types, like posts, events, and subevents [41]. A PageRank-liked credibility propagation algorithm proposed by Gupta et al.

[42] realized the encoding of the trustworthiness of the user and the implication of the posts based on a three-tier heterogeneous information network of users, tweets, and events. Meanwhile, Jin et al. [39] have proposed to include potential subevent in the construction of the hierarchical network and also use the graph optimization framework to infer the reliability of the event.

3. Fake News Detection Based on Diffusion Growth Rate

3.1. Framework. In this section, we first introduce the model framework, then define fake news and diffusion growth rate.

We propose a fake news detection method Delta-G based on diffusion growth rate. Firstly, GCN is utilized to extract the topological features from different time intervals in the diffusion process. Then, the diffusion features would be input into LSTM for further extraction of growth rate features in time series and realize the fake news detection. Compared with existing fake news detection methods based on diffusion structures, Delta-G further include features in time series structures, which could identify fake news more efficiently.

The framework of Delta-G contains three major parts, i.e., feature enhancer, feature extractor, and classifier, as shown in Figure 2. Among these, the feature enhancer is responsible for splicing the features of the root node of fake news with the newly activated feature nodes at each time interval to enhance the overall influence of the root node. Feature extractor could be divided into propagation structure feature extractor, i.e., the GCN, and propagation growth rate feature extractor, i.e., LSTM. Delta-G would first utilize GCN to extract the topological features from different time intervals in the diffusion process. After which the diffusion features would be encoded as series and input into LSTM for further extraction of growth rate features in time series and realize the classification of real and fake news. Compared with fake news detection methods based on diffusion structures, Delta-G further include features in time series structures and enhance the overall performance of the model.

Next, we will introduce the definition of fake news in this article. Fake news refers to news that is made up, which form is similar to real news, but varies in the process of formatting and intention. What fake news lacks is the proper process of editing to ensure the accuracy and reliability of the content. Fake news could be roughly divided into two types, one is that contains incorrect or misleading information, and the other is the deliberate dissemination of false information. The detection of fake news refers to the exact classification of fake news via efficient feature extraction methods.

Finally, we will introduce the definition of diffusion growth rate in this paper. Diffusion growth rate refers to the higher-order representation on time series of the difference between the activated users in the network at two contiguous moments in a fixed time interval. And the time series feature of the diffusion structure is extracted through the sequence model.

3.2. Feature Enhancement. The root node of fake news usually contains adequate information to have a wider impact. Therefore, identifying the origin from which the fake news
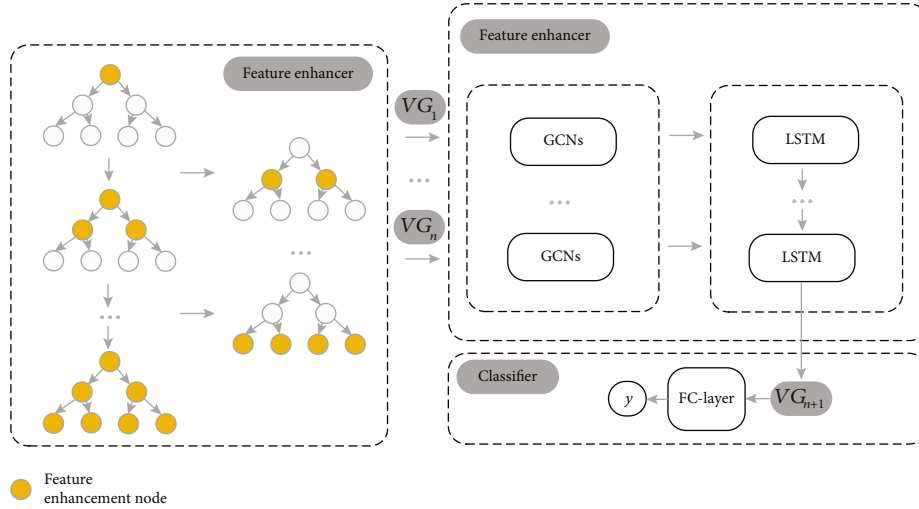
FIGURE 2: The framework of Delta-G.

has spread out from a complex network is critical in the sense of preventing and controlling fake news from spreading. This paper has fully utilized the feature of the root node in the feature extractor to enhance the feature of the newly activated nodes at each time interval. For the GCN of the layer, the newly activated characteristics of the hidden layer and the characteristics of the root node of the hidden layer in the layer would be jointly constructed into a new feature matrix:

$$\tilde{H}_k = \text{concat}\left(H_k, (H_{k-1})^{\text{root}}\right), \qquad (1)$$

where H_k is the newly activated features of the hidden layer and $(H_{k-1})^{\text{root}}$ is the hidden layer features of the root node of the $k-1$ layer. $\tilde{H}_k$ is the concatenated feature matrix.

As shown in Figure 3, to simulate the important influence the root node has in the actual diffusion process, we enhance the feature of each newly activated node on every single GCN and combined the hidden feature of this newly activated node with the feature of the previous root node. While combining other nodes with their hidden feature, in this manner, the feature would be within the same dimension.

3.3. Feature Extraction

3.3.1. Diffusion Structure Feature Extraction. The fake news detecting algorithm based on diffusion growth rate utilizes GCN to extract the features of the diffusion structure between different time intervals, thereby obtaining the expression of high dimension features in the process of diffusion. GCN is a neural network layer, in which the layer-to-layer propagation formula is expressed as follows:

$$H_k = \sigma\left(A H_{k-1} W + b\right), \qquad (2)$$

where $W \in R^{F \times F'}$ is the weight matrix of the model, $b \in R^{F'}$ is the biases, σ is a nonlinear function for activation. $A =$ $\tilde{D}^{-1/2} \tilde{A} \tilde{D}^{-1/2}$, $\tilde{A} = A + I_N$, and A is the adjacent matrix of Graph G, I_N is the identity matrix, and $\tilde{D}$ is stiffness matrix.

After the extraction of multiple GCN, the feature of diffusion structure of different time intervals would be obtained. Ultimately, these diffusion features would be input into LSTM for further extraction of diffusion features in time series, i.e., the feature of the diffusion growth rate.

GCN could extract useful features properly when the train set and test set are based on the same graph structure. However, GCN has two major limitations. Firstly, it is unable to accomplish the task of conclude learning, i.e., dealing with the problem with dynamic graphs. Task of conclude learning refers to the case when the graph structure is different between the train set and test set. Normally, the process of training would only be conducted on a subgraph, while the testing process is expected to handle unknown nodes. Secondly, limitations in dealing with digraphs, given the difficulty of assigning different weights of learning to different adjacent nodes. Therefore, we introduce graph attention networks (GAT) to promote the quality of structural features extraction in the diffusion process. Essentially, GAT has two paths of computing, i.e., the graph attention on global and mask. To better extract the graph structure features, we use the mask graph attention method to perform the attention mechanism operation on each node's neighbours.

GAT would first calculate the coefficient of attention. For node i, its similarity coefficient with all its adjacent nodes for $j \in N_i$ could be calculated by:

$$e_{ij} = a\left(\left[W h_i \| W h_j\right]\right), \qquad (3)$$

where the linear mapping of the shared parameter W increases the dimension of node features, which is a common method of feature extractor. $[\cdot \| \cdot]$ on the other hand joint the feature of node i and node j after their conversion. Finally, $a(\cdot)$ maps the jointed high-dimensional feature on a real number. Therefore, the learning of correlation between node i and node j is completed through the development
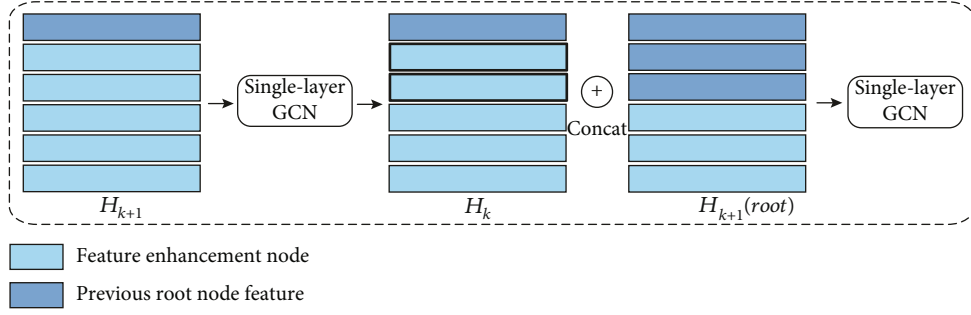
FIGURE 3: Feature enhancer.

parameter W amendment to the mapping of $a(\cdot)$. The function of Softmax would be responsible for the calculation of correlation coefficients between nodes and normalization.

$$a_{ij} = \frac{\exp\left(\text{LeakyReLU}\left(e_{ij}\right)\right)}{\sum_{k \in N_i} \exp(\text{LeakyReLU}(e_{ik}))}. \tag{4}$$

After deriving the coefficient of attention, the adjacent nodes' features would be aggregated through a weighted summation, which offers a new feature h_i' for each node, which contains information about its neighbours.

$$h_i' = \sigma\left(\sum_{j \in N_i} a_{ij} W h_i\right). \tag{5}$$

It could be found from the equation above that the correlation between the feature of nodes is better concluded in the model; thus, theoretically, this model could outperform the model of GCN.

3.3.2. Diffusion Growth Rate Feature Extraction. Since the features extracted by GCN at different time intervals are presented in the form of sequence, the experiment introduces the LSTM, which has an outstanding performance in sequence processing to handle the sequence features in the process of information diffusion as well as efficiently extracts the features of the growth rate of the diffusion structure in the time series. LSTM is a special form of recurrent neural network that is mainly constructed to solve the problem of vanishing gradient and gradient explosion arising in the training process of a long sequence. Compared with normal RNN, LSTM has better performance in the longer sequences. The equation of LSTM is as follows:

$$\begin{cases} i_t = \text{sigmoid}\left(W_i[h_{t-1}, x_t] + b_i\right), \\ f_t = \text{sigmoid}\left(W_f[h_{t-1}, x_t] + b_f\right), \\ \tilde{C}_t = \tan h(W_C[h_{t-1}, x_t] + b_C), \\ o_t = \sigma(W_o[h_{t-1}, x_t] + b_o), \\ C_t = f_t \odot C_{t-1} + i_t \odot \tilde{C}_t, \\ h_t = o_t \odot \tilde{C}_t, \end{cases} \tag{6}$$

where the input gate is denoted by i_t, the forgotten gate is denoted by f_t, and o_t is the output gate. W is the parameter of weight that needs to be learned, and b is the biases. h_{t-1} is the feature of the hidden layer at time $t - 1$, while x_t is the input at time t. $\odot$ represents Hadamard production, i.e., corresponded in two matrixes.

Besides LSTM, a contrast experiment is conducted on tanh-RNN and GRU. Tanh-RNN is a traditional recurrent neural network; the neural input it receives at time t includes the hidden state h_t and the output y_t at present. Therefore, the inputted x_t of tanh-RNN contains only information at time t, rather than information about the sequence. Thus, extra steps are needed to derive h_t, i.e., also input h_{t-1}, which is the historical information. h_t and y_t could be derived as follows:

$$h_t = \sigma_1(U x_t + W h_{t-1} + b), \tag{7}$$

$$y_t = \sigma_2(V h_t + c), \tag{8}$$

where U, W, V are matrices after linear transformation concerning x, h, y. b and c are the biases. σ_1 is the activation function for deriving h_t, which refers to the tanh function in the tanh-RNN model, while σ_2 usually implies the Softmax function.

Furthermore, LSTM overcomes the problem of vanishing gradient and gradient explosion in the traditional form of the RNN model with the gating mechanism. GRU could be seen as a simplified version of LSTM. LSTM contains three gates, forgotten gate, input gate, and output gate, while GRU has only two gates, update gate and reset gate. Besides, compared with LSTM, GRU does not have the cell state c. The formula of GRU is as follows:

$$\begin{cases} z_t = \text{sigmoid}(W_z[h_{t-1}, x_t]), \\ r_t = \text{sigmoid}(W_r[h_{t-1}, x_t]), \\ z_t = \tan h([r_t \odot h_{t-1}, x_t]), \\ h_t = (1 - z_t) \odot h_{t-1} + z_t \odot \tilde{h}_t, \end{cases} \tag{9}$$

where the update gate and reset gate is expressed by z_t and r_t, respectively. The reset gate r_t takes control of the proportion of information input from the previous stage h_{t-1} to the candidate status, as the smaller the r_t is, the

smaller its production with h_{t-1}, and the less the information h_{t-1} that would be included in the candidate status. The update gate is responsible for controlling the proportion of information that is used to command the previous stage h_{t-1} would be reserved to the new stage h_t, the larger the value of $(1 - z_t)$, the more the information is reserved.

3.4. Classifier. After deriving the feature of growth rate from LSTM, the FC layer would be applied to decrease the feature dimension back to 2, and the features learned would be normalized by the Softmax layer, such that the fake news is eventually being detected. The formula of Softmax is as follows:

$$\text{softmax}(y_i) = \frac{\exp(y_i)}{\sum_{k=1}^{K}\exp(y_k)}, \quad (10)$$

where $\exp(\cdot)$ is the exponential function with the natural constant as the base. y_i is the confidence of class i. K is the total number of categories.

Finally, the cross-entropy cost function is used to measure the degree of the wrong prediction. Among which y represents the real label, and p is the estimated value of the model, the loss function is:

$$L = -[y \log(p) + (1 - y) \log(1 - p)]. \quad (11)$$

4. Experiment and Analytics

4.1. Experimental Setup. Experiment platform. We use i7-7700K 4.20 GHzx8 (CPU), TITAN 12GiBx2 (GPU), 16 GBx4 (RAM), Ubuntu 16.04 (OS), Python 3.6, and Tensorflow-gpu-1.3.

Dataset. Two public fake news datasets, Twitter, and Weibo.

Twitter. The dataset is consisted of short messages posted on Twitter, with each tweet associated with textual content (both source tweet and retweet content) and images/videos and include the context of social information (uid, tweet ID, post time delay, and retweet relationship). This dataset has approximately 17,000 individual posts and involves different kinds of incidents. The dataset has been divided into two parts: the train set (which consists of 9,000 fake posts and 6,000 real posts) and the test set (which consists of 2,000 posts). Moreover, they are divided in a specific way such that the incidents in posts will not overlap each other.

Weibo. The fake news collected from Weibo is within the time interval between May 2012 to January 2016 and has all come through the verification of the official rumor refuting system of Weibo. This system encourages normal users to report suspicious posts on Weibo, which would be investigated and finally be demonstrated as fake news or real news. The definition of real news is those proved by the Xinhua News Agency. Data preprocessing step includes deleting repetitive and low-quality images to ensure the homogeneity of the entire dataset. This dataset contains the complete tweet content (tweet ID, title, image link, tweet blogger, issue time, and retweet relationship).

Comparing algorithm. Decision tree classifier (DTC), SVM with a propagation tree kernel (SVM-TK), and RvNN [43]. DTC is a fake news detection method based on multiple artificial features that classify using decision tree, while SVM-TK is a classifier that employs the spreading tree kernel and is based on diffusion structure. RvNN detects rumors using RNN that employs tree structures with GRU units and learns the expression of fake news through diffusion structures.

4.1.1. Evaluation Metrics. Accuracy: the definition of accuracy is the percentage of correct estimates relative to the whole sample, which is:

$$\text{accuracy} = \frac{(TP + TN)}{(TP + FP + TN + FN)}, \quad (12)$$

where TP represents the true positive, TN represents the true negative, FP represents the false positive, and FN represents the false negative.

Precision: precision calculates the number of true samples which gets an estimation of positive in a proportion of all samples that are estimated as positive, the formula is as follows:

$$\text{precision} = \frac{TP}{(TP + FP)}. \quad (13)$$

Recall: the recall rate is the proportion of true samples which get an estimation of positive in all true samples, the formula is:

$$\text{recall} = \frac{TP}{(TP + FN)}. \quad (14)$$

F1 -score: $F1$-score is the harmonic mean of precision and recall, which is:

$$F1 = 2 \times \text{precision} \times \frac{\text{recall}}{(\text{precision} + \text{recall})}. \quad (15)$$

To summarize, accuracy reflects the model's capacity in distinguishing negative samples, with higher accuracy, the model would be more confident in verifying negative samples, while recall rate reflects the model's capacity in distinguishing positive samples, with a higher recall rate; the model would be more confident in verifying positive samples. $F1$-score is an integration of them; the higher the $F1$-score, the more robust the model is.

4.2. Structural Analysis of Optimal Model. The optimal structure of the model is determined by experiments. First of all, for the feature extractor of diffusion structure, this paper tests the performance of Delta-G under GCN of different layers. The experiment has tested two datasets on GCN of 2, 3, 4, and 5 layers, respectively; the result of the experiment is shown in Figure 4.

It is shown by the result that Delta-G has the best performance on both datasets when the layer of GCN is 3.
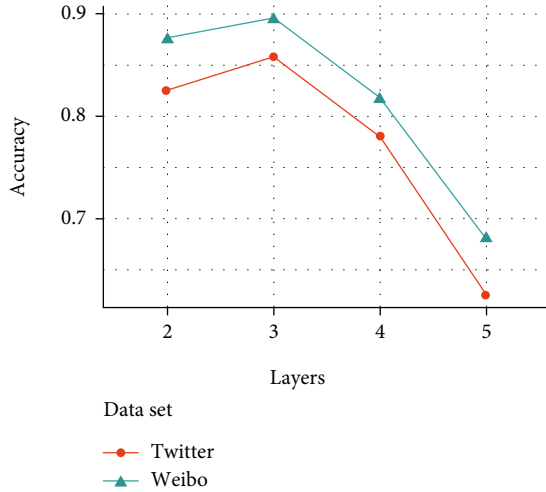
Figure 4: Performance of the Delta-G under different GCN layers.

Figure 5: Performance of the Delta-G under different RNNs.

When the number of layers exceeds 3, the performance of the model would experience a significant decline. Therefore, to ensure the model performance, the default setting of the layer of GCN would be fixed at 3 for subsequent experiments.

In addition, for feature extractor of growth rate, three RNN models are considered to extract the feature on time series, which are tanh-RNN, LSTM, and GRU. Among these, tanh-RNN is just the traditional RNN model and does not contain gate units. Different RNN models would be used to extract features of growth rate, and the optimal model would be determined according to the performance of Delta-G under each RNN model.

As shown in Figure 5, first of all, GRU and LSTM outperform tanh-RNN on both datasets, which means RNN models with gates would generally outperform the traditional RNN model. Secondly, the performance of LSTM is slightly better than GRU on both datasets. Nevertheless, GRU has the advantage of requiring fewer parameters and costs less time to converge and therefore can save a lot of time, which significantly accelerates the process of iteration. As a result, in practice, models should be chosen according to the specific situation to detect fake news with the most efficiency and effectiveness.

4.3. Efficiency Analysis of Delta-G. To prove the efficiency of the proposed methods, this paper compares the performance of Delta-G with three baselines under experiments. The result has shown that in most instances, Delta-G can classify the authenticity of news with more accuracy than baselines. Table 1 has listed the performance of a couple of fake news detection methods in the two datasets.

It could be found in Table 1 that methods based on deep learning would generally outperform other methods that use artificial features. This indicates deep learning methods could capture more effective features and learn about higher-order representations of fake news. Besides, in most cases, Delta-G has a better performance in detecting compared to baselines, especially those based on diffusion struc-
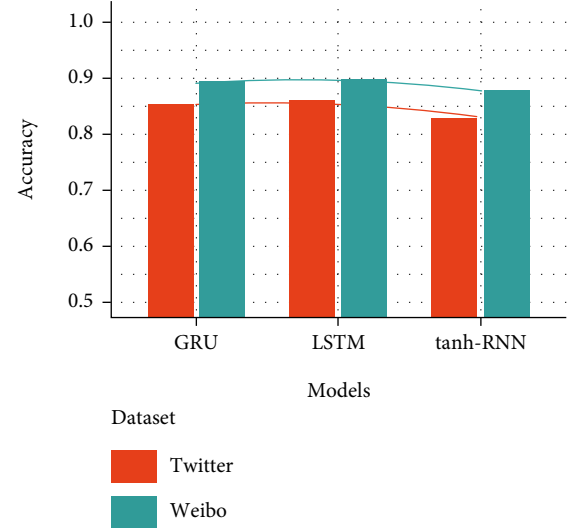
tures, which indicates the effectiveness of combining features of diffusion and time series in the detection of fake news. The accuracy of Delta-G would only underperform RvNN in the false set of the two datasets. Moreover, the introduction of the graph attention mechanism has further improved the performance of Delta-G, which indicates the effectiveness of the introduced attention mechanism in extracting the diffusion structure.

In fact, in the experiments above, what GCN considers when dealing with the adjacent matrix is undirected graph. According to Bian et al. [13], the direction in which the message is transmitted in the social networks also stands as one the important information in detecting fake news. Inspired by this conclusion, this paper adopts directional GCN, which includes two structures, from top to bottom and from bottom to top. From top to bottom means information spread out from the parent node, which is the same as the diffusion process of fake news, while for the from bottom to top structure, information aggregated from subnode to parent node, as shown in Figure 6.

As it is shown in Figure 7, the introduction of the digraph does improve the performance of the model to some extent, which indicates that the causal characteristics of the spread of fake news from top to bottom along the relationship chain and the structural characteristics of the spread in the community from bottom to top are conducive to the detection of fake news. Nevertheless, the improvements brought by the digraph are not as significant as the attention mechanism, which indicates aggregating the feature of adjacent nodes according to their attention weight could provide more effective features, which is critical to the detection of fake news.

4.4. Ablation Experiments. To further explore the importance of diffusion structure on features of time series, we conduct ablation experiments on the Delta-G method, i.e., the Delta-G method is tailored to a range of extent to verify the influence that different parts have on the overall

TABLE 1: Prediction performance comparison.

| Datasets | Methods | Accuracy | True | | | Fake | | |
			Precision	Recall	F1-score	Precision	Recall	F1-score
Twitter	DTC	0.731	0.724	0.757	0.740	0.739	0.704	0.721
	SVM-TK	0.808	0.735	0.902	0.834	0.721	0.652	0.772
	RvNN	0.827	0.847	0.833	0.840	**0.904**	0.820	0.812
	Delta-G	0.855	0.855	0.883	0.869	0.854	0.820	0.837
	Delta-G-GAT	**0.864**	**0.857**	**0.908**	**0.878**	0.872	**0.820**	**0.845**
Weibo	DTC	0.831	0.847	0.815	0.831	0.815	0.847	0.830
	SVM-TK	0.857	0.839	0.885	0.861	0.878	0.830	0.857
	RvNN	0.873	0.816	0.964	0.884	**0.956**	0.782	0.861
	Delta-G	0.896	0.846	**0.968**	0.913	0.953	0.858	0.903
	Delta-G-GAT	**0.908**	**0.871**	0.958	**0.913**	0.953	0.858	**0.903**

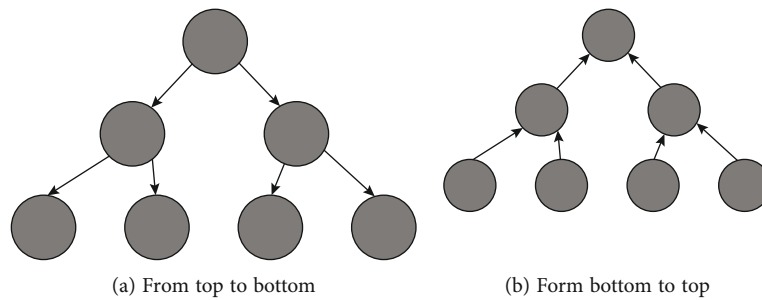(a) From top to bottom   (b) Form bottom to top

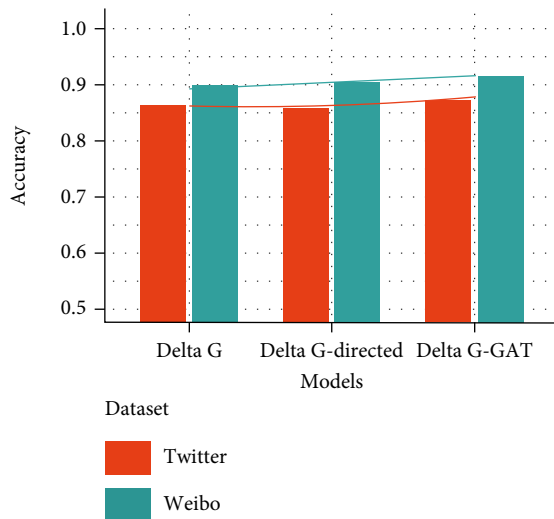FIGURE 6: Two structures in directed GCN.

FIGURE 7: Comparison of fake news detection performance of three variants of the Delta-G.
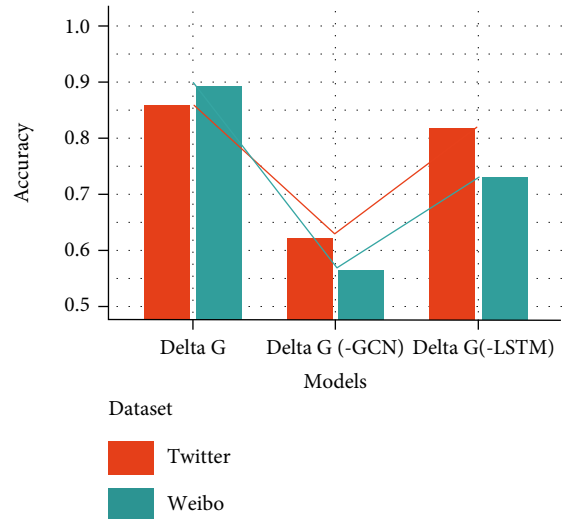

FIGURE 8: The fake news detection performance of the Delta-G when ablating different structures.

performance of the model. While holding all other parameters of the model constant, the above experiment is conducted, and the result is shown in Figure 8.

In the experiments, Delta-G (-GCN) represents the Delta-G model without the GCN module. To ensure the effectiveness of the feature inputted into LSTM, GCN is replaced by SVM to conduct the feature extraction. Delta-G (-LSTM) represents the Delta-G model without the LSTM

module which directly conducts the classification upon the output of GCN. The result of this experiment has shown that when Delta-G model losses its feature on diffusion structure, its capacity for classification would experience a major decline, which indicates the importance of the feature of diffusion structure is in the detection of fake news. Meanwhile, the sequence model is also vital to the classification of news and could significantly enhance the performance of the

model, which proves that the feature of diffusion structure on time series is critical to the detection of fake news.

In summary, features of diffusion structure and time series are both critical to the detection of fake news. Therefore, the Delta-G model which factors in both features shows an outstanding performance in tasks of fake news detection.

5. Conclusion

In conclusion, we propose a fake news detection method Delta-G, which is based on the diffusion growth rate, in allusion to the problem that the textual features are easy to be manipulated; thus, the traditional detector could not provide satisfying results in the detection of fake news. There are mainly three parts of Delta-G, feature enhancer, feature extractor, and classifier. The feature enhancer is responsible for splicing the features of the root node of fake news with the newly activated feature nodes at each time interval to enhance the overall influence of the root node. Feature extractor could be divided into propagation structure feature extractor, i.e., the GCN, and propagation growth rate feature extractor, i.e., LSTM. Delta-G, would first utilize GCN to extract the topological features from different time intervals in the diffusion process. Then, the diffusion features would be encoded as series and input into LSTM for further extraction of growth rate features in time series and realize the classification of real and fake news. Compared with fake news detection methods based on diffusion structures, Delta-G further includes features in time series structures and enhances the overall performance of the model. The experiments conducted on two different datasets using three different baselines have demonstrated that Delta-G can realize the classification of fake news efficiently. Meanwhile, it has been proved by experiment that the introduction of the graph attention mechanism has improved the performance of Delta-G to some extent.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

References

[1] S. Vosoughi, D. Roy, and S. Aral, "The spread of true and false news online," *Science*, vol. 359, no. 6380, pp. 1146–1151, 2018.

[2] K. E. Matsa and E. Shearer, "News use across social media platforms," *Pew Research Center*, vol. 10, 2018.

[3] S. Lewandowsky, U. K. H. Ecker, C. M. Seifert, N. Schwarz, and J. Cook, "Misinformation and its correction," *Psychological Science in the Public Interest*, vol. 13, no. 3, pp. 106–131, 2012.

[4] E. Morozov, "Swine flu: Twitter's power to misinform," *Foreign Policy*, 2009.

[5] K. Wu, S. Yang, and K. Q. Zhu, "False rumors detection on Sina weibo by propagation structures," in *2015 IEEE 31st International Conference on Data Engineering*, pp. 651–662, Seoul, Korea (South), 2015.

[6] G. Tong, W. Wu, and D. Z. Du, "Distributed rumor blocking with multiple positive cascades," *IEEE Transactions on Computational Social Systems*, vol. 5, no. 2, pp. 468–480, 2018.

[7] B. Prabhu Kavin, S. Karki, S. Hemalatha et al., "Machine learning-based secure data acquisition for fake accounts detection in future mobile communication networks," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 6356152, 10 pages, 2022.

[8] M. Shubha, S. Piyush, and A. Ratish, "Analyzing machine learning enabled fake news detection techniques for diversified datasets," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 1575365, 18 pages, 2022.

[9] J. Xing, S. Wang, X. Zhang, and Y. Ding, "HMBI: a new hybrid deep model based on behavior information for fake news detection," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 9076211, 7 pages, 2021.

[10] C. Cortes and V. Vapnik, "Support-vector networks," *Machine Learning*, vol. 20, no. 3, pp. 273–297, 1995.

[11] X. Li, "Using random forest for classification and regression," *Chinese Journal of Applied Entomology*, vol. 50, no. 4, pp. 1190–1197, 2013.

[12] X. Yang and J. Zhang, "Decision tree and its key techniques," *Computer Technology and Development*, vol. 17, no. 1, pp. 43–45, 2007.

[13] T. Bian, X. Xiao, T. Xu et al., "Rumor detection on social media with bi-directional graph convolutional networks," *AAAI Conference on Artificial Intelligence*, vol. 34, no. 1, pp. 549–556, 2020.

[14] Y. J. Lu and C. T. Li, "GCAN: graph-aware co-attention networks for explainable fake news detection on social media," *Annual Meeting of the Association-for-Computational-Linguistics*, vol. 1, pp. 505–514, 2020.

[15] Y. Wu, Z. Xie, S. Ji et al., "Fraud-agents detection in online microfinance: a large-scale empirical study," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 1, p. 1, 2022.

[16] T. N. Kipf and M. Welling, "Semi-supervised classification with graph convolutional networks," 2017, https://arxiv.org/abs/1609.02907.

[17] M. Han, M. Yan, Z. Cai, Y. Li, X. Cai, and J. Yu, "Influence maximization by probing partial communities in dynamic online social networks," *Transactions on Emerging Telecommunications Technologies*, vol. 28, no. 4, 2017.

[18] M. Han, J. Li, Z. Cai, and Q. Han, "Privacy reserved influence maximization in gps-enabled cyber-physical and online social networks," in *2016 IEEE International Conferences on Big Data*

and Cloud Computing (BDCloud), Social Computing and Networking (SocialCom), Sustainable Computing and Communications (SustainCom)(BDCloud-SocialCom-SustainCom), pp. 284–292, Atlanta, GA, USA, 2016.

[19] S. Kumar, R. West, and J. Leskovec, "Disinformation on the web: impact, characteristics, and detection of wikipedia hoaxes," in Proceedings of the 25th International Conference on World Wide Web, pp. 591–602, Canada, 2016.

[20] N. Jindal and B. Liu, "Opinion spam and analysis," in Proceedings of the 2008 International Conference on Web Search and Data Mining, pp. 219–230, Palo Alto, California, USA, 2008.

[21] S. Kumar, B. Hooi, D. Makhija, M. Kumar, C. Faloutsos, and V. S. Subrahamanian, "FairJudge: trustworthy user prediction in rating platforms," 2017, https://arxiv.org/abs/1703.10545.

[22] H. Karimi and J. Tang, "Learning hierarchical discourse-level structure for fake news detection," Annual Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, 2019, https://arxiv.org/abs/1903.07389.

[23] C. Song, C. Yang, H. Chen, C. Tu, Z. Liu, and M. Sun, "CED: credible early detection of social media rumors," IEEE Transactions on Knowledge and Data Engineering, vol. 33, no. 8, pp. 3035–3047, 2021.

[24] K. Shu, S. Wang, and H. Liu, "Beyond news contents: the role of social context for fake news detection," in Proceedings of the twelfth ACM International Conference on Web Search and Data Mining, pp. 312–320, Melbourne VIC, Australia, 2019.

[25] K. Shu, A. Sliva, S. Wang, J. Tang, and H. Liu, "Fake news detection on social media," ACM SIGKDD Explorations Newsletter, vol. 19, no. 1, pp. 22–36, 2017.

[26] A. Vlachos and S. Riedel, "Fact checking: task definition and dataset construction," in Annual Meeting of the Association-for-Computational-Linguistics, pp. 18–22, Association for Computational Linguistics, Baltimore, Maryland, USA, 2014.

[27] Y. Wu, P. K. Agarwal, C. Li, J. Yang, and C. Yu, "Toward computational fact-checking," Proceedings of the VLDB Endowment, vol. 7, no. 7, pp. 589–600, 2014.

[28] B. Shi and T. Weninger, "Fact checking in heterogeneous information networks," in Proceedings of the 25th International Conference Companion on World Wide Web, pp. 101-102, Canada, 2016.

[29] G. L. Ciampaglia, P. Shiralkar, L. M. Rocha, J. Bollen, F. Menczer, and A. Flammini, "Computational fact checking from knowledge networks," PLoS One, vol. 10, no. 6, p. 1, 2015.

[30] S. Feng, R. Banerjee, and Y. Choi, "Syntactic stylometry for deception detection," in Proceedings of the 50th Annual Meeting of the Association for Computational Linguistics, pp. 171–175, Jeju, Republic of Korea, 2012.

[31] V. L. Rubin and T. Lukoianova, "Truth and deception at the rhetorical structure level," Journal of the Association for Information Science and Technology, vol. 66, no. 5, pp. 905–917, 2015.

[32] W. Y. Wang, "'Liar, liar pants on fire': a new benchmark dataset for fake news detection," Annual Meeting of the Association-for-Computational-Linguistics, vol. 2, pp. 422–426, 2017.

[33] R. K. Kaliyar, A. Goswami, and P. Narang, "FakeBERT: fake news detection in social media with a BERT-based deep learning approach," Multimedia Tools and Applications, vol. 80, no. 8, pp. 11765–11788, 2021.

[34] J. A. Nasir, O. S. Khan, and I. Varlamis, "Fake news detection: a hybrid CNN-RNN based deep learning approach," International Journal of Information Management Data Insights, vol. 1, no. 1, article 100007, 2021.

[35] M. Potthast, J. Kiesel, K. Reinartz, J. Bevendorff, and B. Stein, "A stylometric inquiry into hyperpartisan and fake news," Annual Meeting of the Association-for-Computational-Linguistics, vol. 1, pp. 231–240, 2018.

[36] Y. Chen, N. J. Conroy, and V. L. Rubin, "Misleading online content: recognizing clickbait as 'false news'," in Proceedings of the 2015 ACM on Workshop on Multimodal Deception Detection, pp. 15–19, Seattle, Washington, USA, 2015.

[37] S. M. Mohammad, P. Sobhani, and S. Kiritchenko, "Stance and sentiment in tweets," ACM Transactions on Internet Technology, vol. 17, no. 3, pp. 1–23, 2017.

[38] V. Qazvinian, E. Rosengren, D. Radev, and Q. Mei, "Rumor has it: identifying misinformation in microblogs," in Proceedings of the 2011 Conference on Empirical Methods in Natural Language Processing, pp. 1589–1599, Edinburgh, Scotland, UK, 2011.

[39] Z. Jin, J. Cao, Y. Zhang, and J. Luo, "News verification by exploiting conflicting social viewpoints in microblogs," AAAI Conference on Artificial Intelligence, vol. 30, no. 1, pp. 2972–2978, 2016.

[40] E. Tacchini, G. Ballarin, M. L. Della Vedova, S. Moret, and L. De Alfaro, "Some like it hoax: automated fake news detection in social networks," 2017, https://arxiv.org/abs/1704.07506.

[41] Z. Jin, J. Cao, Y. G. Jiang, and Y. Zhang, "News credibility evaluation on microblog with a hierarchical propagation model," in 2014 IEEE International Conference on Data Mining, pp. 230–239, Shenzhen, China, 2014.

[42] M. Gupta, P. Zhao, and J. Han, "Evaluating event credibility on twitter," in Proceedings of the 2012 SIAM International Conference on Data Mining, pp. 153–164, Anaheim, California, USA, 2012.

[43] J. Ma, W. Gao, and K. F. Wong, "Rumor detection on twitter with tree-structured recursive neural networks," in Proceedings of the 56th Annual Meeting of the Association for Computational Linguistics (ACL 2018), pp. 1980–1989, Melbourne, Australia, 2018.