Disinformation Propagation Trend Analysis and Identification Based on Social Situation Analytics and Multilevel Attention Network

Junchang Jing, Fei Li, Bin Song, Zhiyong Zhang, *IEEE Senior Member*, Kim-Kwang Raymond Choo, *IEEE Senior Member*

***Abstract*—Digital disinformation, such as those occurring on online social networks (OSNs), can influence public opinion, create mistrust and division, and impact decision- and policy-making. In this study, we propose a disinformation diffusion trend analysis and identification method, which utilizes social situation analytics and a multilevel attention network. First, we present a division and feature representation approach of social user circle based on the content sequence (internal driving factor) and social contextual information (external driving factor) of users associated with disinformation. Second, disinformation content feature, crowd response feature and time-series feature are represented by utilizing embedding layer and bidirectional long short-term memory neural networks (Bi-LSTM). We also present an attention mechanism model based on multi-feature fusion, which can dynamically adjust the weight of each feature. On this foundation, the fused features are fed into the multi-layer perceptron to identify the propagation quantity trend. According to the experimental results of real-world OSNs and social situation metadata, we conclude that while disinformation occurs across OSN platforms, the disinformation is more likely to spread widely in the original OSN platform. We also identify four typical disinformation propagation trends based on propagation patterns and propagation peak times. Findings from our experiments demonstrate that our proposed approach accurately identifies and predicts the diffusion trend of disinformation, which can then be utilized to inform mitigation strategy.**

***Index Terms*—Disinformation, social situation, user behavior, propagation trend analysis, attention network.**

I. INTRODUCTION

ONLINE social networks (OSNs) have become an important tool for information exchange and sentiment communication in our digitalized society [1][2][3]. On the flip side, OSNs can be abused to generate and spread false information and rumors, such disinformation can take place in real-time and far-reaching (e.g., received by users from different countries). More concerning, researchers have found that fake news spreads faster and has broader coverage in comparison to actual (fact-checked) news on OSNs [4]. In the context of the recent COVID-19 pandemic, the spread of false information relating to the virus and vaccines has been known to mislead large populations in different countries and create division within the society [5][6]. This reinforces the importance of designing effective and advanced approaches, such as deep learning [7] and broad learning [8], to accurately identify the spread of false information in real-time, as well as predicting the disinformation spread based on recent trends.

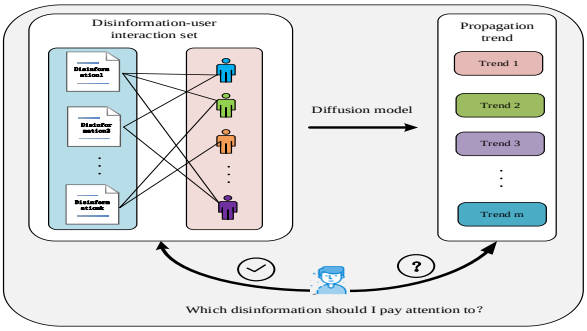


Fig. 1. A simplified example of disinformation flow.

The spreading of false information can be broadly categorized into disinformation and misinformation [9][10]. Disinformation (see also Fig. 1) refers to the malicious spreading of false information, whilst misinformation is the spread of false information spread unknowingly (i.e., without malicious or bad intention). In other words, the goal of disinformers is to support their opinions by changing the views of other disseminators using false information, and disinformers are unlikely to change their opinions and beliefs about the topic. On the contrary, misinformers who propagate misinformation are likely to change their stand after obtaining reliable evidence of the information's authenticity [11]. Given the malicious nature of disinformation, we will focus on the

The work was supported by National Natural Science Foundation of China Grant No.61972133, Project of Leading Talents in Science and Technology Innovation for Thousands of People Plan in Henan Province Grant No.204200510021, and Program for Henan Province Key Science and Technology No.222102210177, No.222102210072 and No.212102210383, China Postdoctoral Science Foundation Grant No.2021M700885. The work of K.-K. R. Choo was supported only by the Cloud Technology Endowed Professorship. (Corresponding author: Zhiyong Zhang, Email: xidianzzy@126.com).

Junchang Jing, Bin Song and Zhiyong Zhang are with Information Engineering College, Henan International Joint Laboratory of Cyberspace Security Applications, Henan University of Science and Technology, Luoyang 471023, China. E-mail: {junchangjing, xidianzzy}@126.com, songbin@haust.edu.cn. Fei Li is with Computer Research Institute of the University of Chinese Academy of Sciences, Beijing 100080, and Pengcheng Laboratory, Shenzhen 518055, China. E-mail: lifei@sequoiadb.com. Kim-Kwang Raymond Choo is with the Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, 78249, USA. E-mail: raymond.choo@fulbrightmail.org.

dissemination trend of disinformation in this article.

Disinformation dissemination approaches can be divided into three categories, and of which infectious disease dynamics based-approaches appear to be the most popular [12][13]. However, these approaches have two major limitations. First, the propagation dynamics models are only theoretical modeling of false information dissemination in nature, and second, they only focus on the propagation of one type of false information. To overcome the limitations of existing infectious disease dynamics-based approaches, scholars have also adapted deep learning-based approaches to study false information dissemination [14][15]. For example, one can utilize word embedding to represent the content of false information, and then further analyze and mine the behavior patterns of users spreading false information. Approaches in the third category analyze the statistical properties of the false information propagation (e.g., using Lorentz curve, Gini coefficient and Parma ratio) [16]. For example, some researchers study the differences in their propagation modes by combining real information with false information at the early stages of dissemination [17].

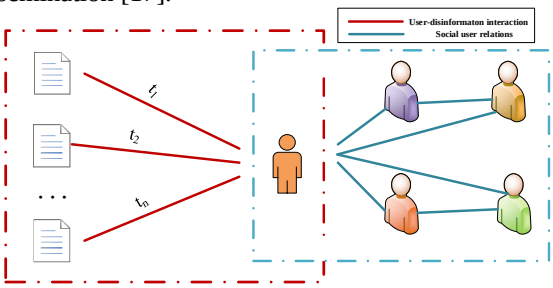


Fig. 2 The division structure graph of social user circle. It consists of two subgraphs, namely the user-disinformation interaction subgraph (left part) and the social user relation subgraph (right part). Note that t_1, t_2 and t_n represent the time when the user propagates disinformation.

The spread of false information in OSNs shows the characteristics of a circle (group) clustering structure, which is similar to the traditional social interpersonal relationship network. A social user circle (group) usually refers to a collection of users with the same or similar interests and social relationships. The latest research results on groups and social circles have been reported by Moon and Liu in the field of network science and engineering [18][19]. Here, Moon et al. [18] proposed a group-based continuous-time Markov epidemic dynamics model, Liu et al. [19] introduced the representation of social user circle into a personalized recommendation algorithm to improve the recommendation effect of the model. Inspired by [18][19], we realize the division of the social user circle from two aspects: the content of users spreading false information and users' social contextual information. Fig. 2 shows the division structure of the social user circle.

A summary of existing challenges is as follows.

1. Complexity and interactivity of the circles' structure of false information dissemination: Existing false information dissemination approaches do not generally consider the impact of social user circles on disinformation propagation. Therefore, the formal representation and division of social user circles remain one of the challenges yet to be addressed.

2. Dynamics of weight distribution of multiple propagation features: Different propagation characteristics may have different impacts on false information propagation at different periods. This reinforces the importance of accurately quantifying the weight distribution mechanism of various propagation characteristics.

3. Effectiveness of cross-platform propagation trend analysis and early warning: If we are able to more effectively utilize limited observation data to analyze the correlation of cross-platform false information dissemination trend, we will be able to facilitate the early detection of disinformation dissemination.

Situation analytics has been widely studied by software engineering researchers [20][21][22]. With the diversification of social network services, significant human-centered data has been generated in human-human and human-machine interactions. In our prior work [23], we demonstrated how one can use the social situational analysis theory to analyze social user behavior patterns. However, we observe that communication trend identification has not been discussed in the disinformation propagation literature. Therefore, we seek to study false information dissemination in OSNs using an integrated social situational analysis theory and deep learning-based approach. Specifically, in our approach we propose a division and representation of the social user circle from two aspects, namely: content of users spreading disinformation and social contextual information of users. Considering the various propagation characteristics of disinformation, an attention mechanism is introduced to solve the weight distribution problem of propagation characteristics. Furthermore, we select statistical indicators, such as the Lorentz curve and Gini coefficient, to analyze and discuss the correlation between the dissemination trend of disinformation and the type of audience entity and dissemination time, and identify the dissemination trend of disinformation. The main contributions of this article can be described as follows.

1. We propose a social user circle division and representation method based on users' dissemination of disinformation content (internal driving factor) and social contextual information (external driving factor). Specially, according to the content sequence of users spreading disinformation over a period of time, this study proposes a user content preference feature representation model based on Bi-LSTM and auto-encoder to realize the hidden representation of user content preference features. Moreover, according to the strength of the social relationship between users and their directly connected friends set, a user relationship representation model based on the attention mechanism is proposed to realize the hidden representation of users' corresponding social relationship characteristics. The above two types of features are concatenated, and the division and representation of the social user circle are realized through an unsupervised clustering algorithm, which is applied to the identification of the disinformation dissemination trend.

2. We propose an attention mechanism model based on multi-feature fusion, which can dynamically adjust the weight of each feature. Moreover, the content feature, crowd response feature and time-series feature are represented by the embedding layer and Bi-LSTM. Thus, the fused features including content feature, crowd response feature, time-series

feature and social user circle feature are fed into the multi-layer perceptron to identify the propagation quantity trend.

3. We collect 1,858,575 Socialsitu metadata based on social situation analysis technology, and assess the performance of the approach presented in this article through a range of experiments. The experimental results show that the communication trend identification method proposed in this study can not only accurately identify the communication quantity trend of disinformation in the future, but also provide support for the government and management departments to take effective intervention measures in advance. To our knowledge, we are the first to investigate a trend identification method of user spreading disinformation based on social situation analytics in a realistic online social network scenario.

4. In the process of identifying the spread trend of disinformation, we draw two interesting and vital conclusions: i) while disinformation occurs across OSN platforms, the disinformation is more likely to spread widely in the original OSN platform. ii) we identify four typical disinformation propagation trends based on propagation patterns and propagation peak times.

This article is organized into six sections. In Section II, we review other related approaches for false information dissemination. Section III describes the problem, and Section IV presents our proposed approach. In Section V, we present and discuss our evaluation findings, prior to concluding our research in section VI.

II. Related Works

Understanding the dissemination of false information in OSNs from different perspectives have been extensively studied in recent years. Here, we will focus on approaches based on infectious disease dynamics, statistical properties of social networks, and deep learning – see Sections II.A to II.C.

A. Infectious disease dynamics-based approach

Using infectious disease dynamics-based false information dissemination approaches to mine propagation patterns of false information has been widely studied and discussed [12][13] [24][25][26][27]. For example, Shrivastava et al. [12] proposed a false information defensive dynamics model by utilizing a susceptible-verified-infected-recovered model, and analyzed and discussed the stability, equilibrium and basic reproduction number of the model. Dong et al. [13] presented an SIS rumor propagation dynamics model, in which they combined the propagation dynamics and population dynamics model. They also discussed the effects of different infection rate and cure rate parameters on the emerging rumor propagation behavior. Rumors and authoritative information propagation model was proposed by Zhang et al. [24]. They established a super propagation mechanism and estimated the basic reproduction number and final propagation scale of the model. In [25], a rumor propagation model based on multi-feature fusion was designed. On the basis of it, they further proposed a multi-feature rumor blocking strategy with a multi-layer network structure. For multi-layer social networks, the two-layer rumor propagation dynamic model has been analyzed and discussed by Cui et al. [26] who considered the internal characteristics and propagation structure characteristics of rumor. Wang et al. [27] constructed an improved energy model and analyzed the propagation mode and control strategy of rumors in multi-layer social networks.

B. Statistical properties of the social networks-based approach

Statistical properties based on false information dissemination approaches mainly rely on some classical statistical indicators to quantify and compare propagation patterns of false information [4][16][17][28][29]. For example, Vosoughi et al. [4] selected the number of nodes and cascades as indicators to quantify and compare the differences between the two types of information in depth, size, maximum breadth and structural virality. This research work provides important ideas for correctly distinguishing true news from false news. Glenski et al.[16] used three classical statistical indicators including Lorenz curve, Gini coefficient and Parma ratio, to quantify and analyze the propagation behavior of different users. The authors found there were significant differences in the propagation behavior of users from various news sources. Zhao et al. [17] analyzed and compared the propagation patterns of real and fake information in the early spreading stage. They found that the propagation patterns of fake information are significantly different from that of real information in OSNs. In addition, research on the propagation patterns of false information by social bots has also been reported [10][28][29]. For instance, Shao et al. [28] studied the propagation pattern of social bots spreading low-credibility content information. The authors found social bots not only spread such information after it is published but also focus on a large number of influential users through the reply and mention functions of social platforms. In [29], the relationship between social bots and false news propagation time was explored. They found evidence that social bots are usually active in the early spreading moments. At the same time, the communication target of social bots was more inclined to social user groups with certain influences.

C. Deep learning-based approach

Due to renewed interest in deep learning, it is not surprising that there have been attempts to utilize deep neural networks to study the false information dissemination model in OSNs. For instance, Xiao et al. [14] provided a rumor propagation approach in OSNs based on representation learning and game theory. The authors first expressed the feature space of rumor and anti-rumor by utilizing the representation learning method. Next, the relationship between rumor and anti-rumor was quantified and analyzed based on game theory. Finally, they presented a group behavior model of dynamic rumor and anti-rumor propagation. In [30], the authors analyzed the differences between false information disseminators and non-disseminators in user characteristics. Based on the analytical observations, they further exploited the multilayer perceptron model to predict the trend of users' spreading false information.

Attention mechanism was first widely used in visual attention systems and showed unique advantages [31]. In recent research, researchers have applied attention mechanisms to solve the modeling problem of social network scenarios. For example, Yu et al. [32] extracted the importance weights of the content and time of false information based on the attention mechanism. They established a content and temporal co-attention mechanism which was capable of reducing the effect of noise data. Ni et al. [33] constructed a multi-perspective attention network by considering text semantic attention and

propagation structure attention. In [34], Chen et al. developed a deep attention network for learning the time-series representation of false information posts. This approach was automatically capable of capturing hidden representations of posting series.

Note that OSN platforms such as Weibo, WeChat, QQ, etc., possess the information sharing function including sharing to the local social platform or third-party social platforms, as well as individuals or groups. Therefore, based on the typical OSN platforms architecture, this paper carries out a series of research on the analysis and identification of the disinformation dissemination trend.

III. Problem Definitions

A. Problem Statement

The main research goal of this article is to analyze and identify the spread trend of disinformation in OSNs. The specific definitions utilized herein are given as follows.

Definition 1: The user historical propagation disinformation collection is defined as $G_F^{u_i} = \{(F, u_i) \mid F = \{f_1, f_2, \cdots, f_n\}, u_i \in U\}$.

By definition, $G_F^{u_i}$ is the user u_i historical propagation disinformation collection, which is composed of disinformation sequence F propagated by the user u_i. f_i=$\{w_1, w_2, \ldots, w_m\}$, where f_i denotes the i-th disinformation spread by the user u_i and w_j denotes the j-th words belonging to f_i .

Definition 2: A social situation at time t, *Socialsitu*(t), is defined as *Socialsitu*(t)=$\{obj, ID, d, A, E, T\}_t$.

Based on the social situation analysis theory presented by us [23][35], we introduce the social object (*obj*) tuple and social target (*T*) tuple by considering the social scene of disinformation propagation. Specially, *obj* represents the social object accessed by social users, such as disinformation and true information. *ID* denotes the social user's identity information (user's group and role). *d* denotes the user's atom-desire at time *t*. *A* represents the user's behavior corresponding to *d* at time *t*. *E* represents environmental information, which includes the terminal information that the user used. *T* denotes the target of audience entities, including the local platforms, individuals, groups and circles of friends of the third-party platforms.

Definition 3: The social relationship between social users is expressed as $SR = \{(e_{ij})_{|U| \times |U|}, 1 \le i, j \le |U|\}$.

Here, e_{ij} represents the total number of responses from u_j to u_i. Specifically, it refers to the number of likes, shares and comments of u_j on the disinformation published by u_i. Note that e_{ij} and e_{ji} represent different meanings between u_i and u_j. We can quantitatively find the strength of the relationship between users through a directed link e_{ij} and e_{ji} .

Definition 4: The propagation sequence of disinformation f_i, *prop*(f_i), is denoted as $prop(f_i) = \{(u_0, socialsitu(t_0)), (u_1, socialsitu(t_1)), \cdots, (u_k, socialsitu(t_k))\}$.

Here, the spread of disinformation can be regarded as the propagation time-series concerning socialsitu. *socialsitu* (t_k) represents the corresponding *socialsitu* of the user u_k at time t_k. Therefore, the set of disinformation propagation sequences can be defined as S=$\{prop(f_1), prop(f_2), \ldots\ldots, prop(f_N)\}$.

Definition 5: Identification of disinformation dissemination trend.

For a given disinformation f_i, according to the propagation sequence *prop*(f_i) of the disinformation from the release time t_0 to the current time t_c, the content characteristics c_i' , crowd response characteristics r_i' , time-series characteristics p_i' and social user circle characteristics sc' of the disinformation are constructed and represented, and on this basis, the propagation trend $\hat{y}_i = f(c_i', r_i', p_i', sc')$ of the disinformation f_i at time $t_c + \Delta t$ is further identified. This study aims to explore the optimal mapping function f, so that it can accurately identify the propagation trend $\hat{y}_i$ of disinformation f_i.

In order to more clearly describe the above definitions given in this part, we summarize the key symbols and their corresponding meanings in Table I.

TABLE I
THE KEY NOTATIONS IN PROBLEM DEFINITION

Notation	Description
u_i	A user u_i
U	The social user collection
f_i	The i-th disinformation
F	The disinformation collection
$G_F^{u_i}$	The user historical propagation disinformation collection
SocialSitu(t)	A social situation at time t
SR	The social relationship between social users
$prop(f_i)$	The propagation sequence of disinformation f_i
S	The disinformation propagation sequences collection
t_0	The release time
t_c	The current time
c_i'	The content characteristics
r_i'	The crowd response characteristics
p_i'	The time-series characteristics
sc'	The social user circle characteristics
$\hat{y}_i$	The identified propagation trend of disinformation f_i

B. Problem Formulation

This part formally describes our research problem in this article. First, we construct the user historical propagation disinformation collection $G_F^{u_i} = \{(F, u_i) \mid F = \{f_1, f_2, \cdots, f_n\}, u_i \in U\}$, social situation six-tuple sequence *Socialsitu*(t)=$\{obj, ID, d, A, E, T\}_t$, and social relationship between social users $SR = \{(e_{ij})_{|U| \times |U|}, 1 \le i, j \le |U|\}$. Second, the division of the social user circle is realized from the disinformation content transmitted by users (internal driving factor) and users' social relationship network (external driving factor). Then, according

to the disinformation propagation sequence $prop(f_i)=\{(u_0,socialsitu(t_0)),(u_1,socialsitu(t_1)),\cdots,(u_k,socialsitu(t_k))\}$,

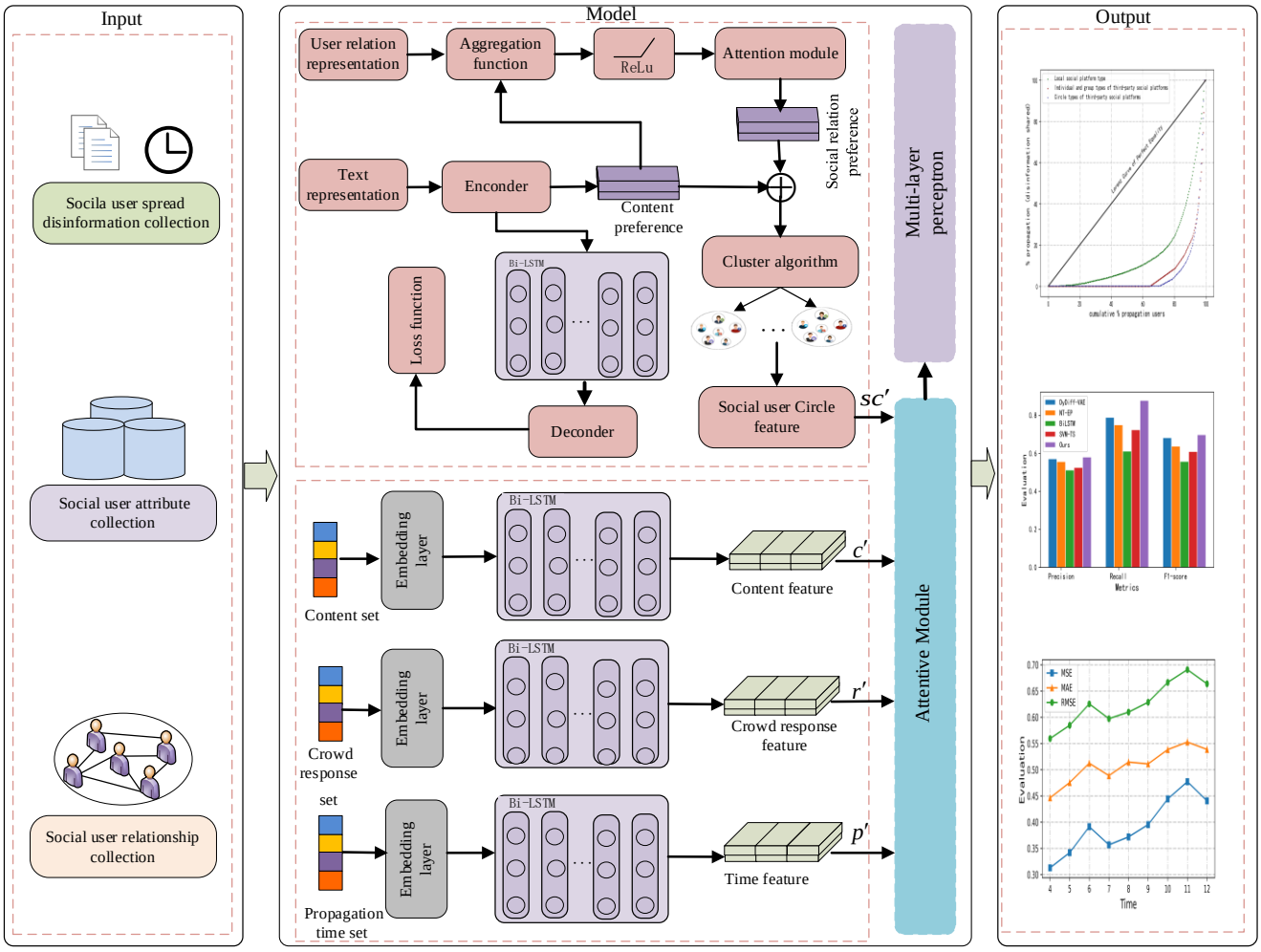


Fig. 3. The proposed framework for disinformation diffusion trend analysis and identification. It includes three major components: input part, model construction and output part. The input part contains social user spread disinformation collection such as COVID-19 topic, social user attribute collection such as account age, gender and friends count, etc., and social user relationship collection including the interactions (i.e. the number of likes, shares and comments) between users. The model construction part is mainly composed of social user circle division and representation by utilizing Bert, Bi-LSTM, auto-encoder network, and cluster algorithm, and multi-feature (content feature, crowd response feature, time-series feature and social user circle feature) fusion and representation by utilizing embedding layer, Bi-LSTM and attention mechanism. The output part includes the results of propagation trend analysis and identification, such as correlation analysis between the dissemination trend of disinformation and the types of audience entities, propagation trend performance analysis.

the content characteristics, crowd response characteristics and time-series characteristics are represented, and the feature weight is dynamically adjusted through the attention mechanism. Finally, the fused features are fed into the multi-layer perceptron to identify the propagation quantity trend Y^* of the disinformation after the time Δt. More specifically, the problem is described as follows.

$$\left.\begin{array}{c} U=\{u_1,u_2,\cdots,u_{|U|}\} \\ G_F^{u_i}=\{(F,u_i)\,|\,F=\{f_1,f_2,\cdots,f_n\},u_i\in U\} \\ f_i=\{w_1,w_2,\cdots,w_m\} \\ \text{Socialsitu(t)}=\{\text{obj, ID, d, A, E, T}\} \\ SR=\{(e_{ij})_{|U|\times|U|},1\le i,j\le|U|\} \\ prop(f_i)=\{(u_0,socialsitu(t_0)),(u_1,socialsitu(t_1)),\cdots,(u_k,socialsitu(t_k))\} \\ \text{S}=\{prop(f_1),prop(f_2),\cdots,prop(f_N)\} \end{array}\right\}\Rightarrow Y^*=\arg\max_i P_i(Y_i\,|\,G,F,SR,S)$$

1) *Input:* According to the relevant definitions and descriptions given in part III-A, the input part corresponding to the model can be represented as follows.

1. The social user set $U=\{u_1,\cdots,u_{|U|}\}$.
2. The social user historical propagation disinformation collection $G_F^{u_i}=\{(F,u_i)\,|\,F=\{f_1,f_2,\cdots,f_n\},u_i\in U\}$.
3. The i-th disinformation $f_i=\{w_1, w_2,\ldots,w_m\}$.
4. The social user relationship network $SR=\{(e_{ij})_{|U|\times|U|},1\le i,j\le|U|\}$.
5. The disinformation propagation sequence $prop(f_i)=\{(u_0,socialsitu(t_0)),(u_1,socialsitu(t_1)),\cdots,(u_k,socialsitu(t_k))\}$.
6. The disinformation propagation sequences collection

$S=\{prop(f_1),prop(f_2),\ldots\ldots,prop(f_N)\}$.

2) *Output:* Based on the above description, the outputs of the model can be expressed as follows.

1. The characteristics of the social user circle $SC=\{sc_1,sc_2,\cdots,sc_p\}$. We establish a social user circle division model by considering the content sequence and social user relationship of users spreading disinformation. First, based on the disinformation collection $G_F^{u_i}$ propagated by user u_i, the preference characteristic $x_{u_i}^{(I)}$ of user u_i propagated content can be obtained. Second, according to the user's social relationship set *SR*, the user's social relationship characteristic $x_{u_i}^{(S)}$ can be represented. Finally, the social user circle is divided by a clustering algorithm, and its corresponding features *SC* are also represented.

2. The quantity trend of disinformation dissemination $Y^*=\arg\max_i P_i(Y_i\mid G,F,SR,S)$. To accurately identify the propagation trend of disinformation after the period Δt, based on the division of social user circle, this article establishes a multi-feature fusion attention model by combing the characteristics of social user circle, the content characteristics of disinformation, the crowd response characteristics of disinformation and time-series characteristics. This model is capable of dynamically adjusting the weight of each feature. In addition, the fused features are fed into the multi-layer perceptron model to identify the propagation quantity trend.

IV. Proposed Method

To discuss and analyze the problems proposed in the previous sections, first, a social user circle division and representation method based on users' dissemination of disinformation content and social contextual information is presented. Specially, during the process of social user circle division, according to the strength of the social relationship between users and their directly connected friends set, a user relationship representation approach based on attention mechanism is presented to realize the hidden representation of users' corresponding social relationship characteristics. Next, we propose an attention mechanism model based on multi-feature (content feature, crowd response feature, time-series feature and social user circle feature) fusion to dynamically adjust the weight of each feature. Finally, the fused features are fed into the multi-layer perceptron to identify the propagation quantity trend. In addition, we develop an approach based on statistical indicators, such as Lorentz curve and Gini coefficient to quantify and analyze the correlation between the dissemination trend of disinformation and the types of audience entities. The model framework of the disinformation propagation trend is shown in Fig. 3.

A. Social User Circle Division and Representation Method for Disinformation Dissemination

In this section, we extract the content preference characteristics and social relationship characteristics of users' dissemination of disinformation from two perspectives: i) the dissemination sequence generated in the interaction between users and disinformation, and ii) the strength of the social relationship between users. Then, an improved affinity propagation (AP) clustering algorithm is utilized to realize the social user circle division and feature representation of disinformation dissemination.

The content of social users' historical dissemination of disinformation can objectively reflect users' internal interests and preferences. To accurately capture the semantic and contextual information of disinformation, we utilize the pre-trained Bert (bidirectional encoder representations from transformers, Bert) model [36] to encode each disinformation according to the text sequence of disinformation transmitted by each user. The *k*-th disinformation f_k spread by the user u_i is represented as follows.

$$x_k^{(u_i)}=\{x_{k1},\cdots,x_{kn_k}\}=Bert(f_k) \tag{1}$$

where $x_{ki}\in R^{d_w}$, d_w refers to the dimension of word embedding.

Compared with the classical *LSTM* model, *Bi-LSTM* can consider the forward and backward information flow in the network at the same time. Considering that there may be a certain correlation between users propagating disinformation in different periods, we establish a user content preference feature representation model based on Bi-LSTM and auto-encoder. Moreover, to reduce the cost of manually extracting complex features, this auto-encoder model can effectively encode the features corresponding to the user propagated disinformation through unsupervised learning. According to the user u_i historical propagation disinformation sequence matrix $X_{u_i}=\{x_1^{u_i},\cdots,x_n^{u_i}\}$, the encoder can be constructed as $\phi_1: X_{u_i}\rightarrow x_{u_i}^{(I)}$. Moreover, the input vector x_t of the *t*-th position, the hidden state $h_{t-1}^{(1)}$ of the previous position and the hidden state $h_{t+1}^{(2)}$ of the next position, are transformed into the hidden state h_t of the current time step through *Bi-LSTM*, which is specifically expressed as follows.

$$h_t^{(1)}=\overrightarrow{LSTM}(h_{t-1}^{(1)},x_t) \tag{2}$$

$$h_t^{(2)}=\overleftarrow{LSTM}(h_{t+1}^{(2)},x_t) \tag{3}$$

$$h_t=h_t^{(1)}\oplus h_t^{(2)} \tag{4}$$

where $h_t^{(1)}$ and $h_t^{(2)}$ represent the output of the *t*-th position of the forward and backward LSTM layer, respectively, $\oplus$ refers to the concatenation operation between $h_t^{(1)}$ and $h_t^{(2)}$, h_t denotes the output of the *t*-th position of the *Bi-LSTM* network. By updating and iterating the hidden state, the hidden vector $x_{u_i}^{(I)}$ of user propagation disinformation can be obtained. For the decoder $\phi_2: x_{u_i}^{(I)}\rightarrow X_{u_i}$, the decoding process is opposite to the encoding process, and the original user propagation disinformation sequence matrix X_{u_i} can be reconstructed. Therefore, the auto-encoder network can be represented as

$$Z_1=Bi\text{-}LSTM(X_{u_i}) \tag{5}$$

$$x_{u_i}^{(I)}=\phi_1(Z_1) \tag{6}$$

$$Z_2=Bi\text{-}LSTM(x_{u_i}^{(I)}) \tag{7}$$

$$\hat{X}_{u_i}=\phi_2(Z_2) \tag{8}$$

where ϕ_1 and ϕ_2 refer to the corresponding activation functions of the model in the process of encoding and decoding,

respectively. The loss function of the auto-encoder model can be defined as

$$Loss_{u_i} = \sum_{n=1}^{N} \left\| X_{u_i} - \hat{X}_{u_i} \right\|_2^2 \quad (9)$$

In the training process, we continuously adjust the model training parameters according to the loss function value of the auto-encoder to obtain the hidden representation of the user propagation disinformation sequence. After the model training, we remove the decoder and only retain the encoder corresponding to the model. The output vector $x_{u_i}^{(I)}$ of the encoder is used as the interest and preference feature vector of the user spreading the disinformation content.

According to the relevant theory of user relations in OSNs [37], the preferences of communicators are usually easily affected by their directly connected friends. Therefore, communicators may have similar interests and preferences with their friends. Inspired by reference [38], on the basis of extracting the interests and preferences characteristics of the neighbors set $N(i)$ of the user u_i, the social relation characteristic of the disseminator u_i is represented as follows:

$$x_{u_i}^{(S)} = \varphi(W \cdot Aggre_{neigb(u_i)}\left(\{X_s, \forall s \in N(i)\}\right) + b) \quad (10)$$

where φ refers to the nonlinear activation function, that is *Relu*, $Aggre_{neigb(u_i)}$ represents the aggregation function for neighbors of user u_i. In fact, the strength of the relationship between communicators and their directly connected friends may be different, and they are more inclined to spread disinformation to friends with strong relationships. Therefore, to more fully represent the characteristics of users' social relations, we further capture the neighbors who have an important impact on the communicator u_i by using an attention mechanism. The specific formulas are shown as follows.

$$x_{u_i}^{(S)} = \varphi\left(W \cdot \left\{\sum_{s \in N(i)} \alpha_{is} X_s\right\} + b\right) \quad (11)$$

$$\alpha'_{is} = w_2 \cdot \varphi(w_1 \cdot X_s + b_1) + b_2 \quad (12)$$

$$\alpha_{io} = \frac{\exp(\alpha'_{is})}{\sum_{s \in N(i)} \exp(\alpha'_{is})} \quad (13)$$

where α_{is} refers to the strength of the relationship between the disseminator u_i and its neighbor. The communication content features $x_{u_i}^{(I)}$ and social relationship features $x_{u_i}^{(S)}$ are concatenated, and the communication preference features of the user u_i are expressed as follows.

$$c_{u_i} = concat(x_{u_i}^{(I)}, x_{u_i}^{(S)}) \quad (14)$$

AP is an unsupervised machine learning algorithm, which is suitable for coping with large-scale high-dimensional data [39]. Compared with the traditional unsupervised algorithms such as *K*-means, the advantage of AP clustering algorithm is that it does not need to manually set the number of clusters in advance. In addition, this algorithm avoids the local optimization problem caused by selecting an inappropriate cluster center for initiation. We calculate the similarity matrix *S* between users according to the propagation preference feature vector c_{u_i} of each user u_i,

$$S = \begin{bmatrix} s_{(u_1,u_1)} & s_{(u_1,u_2)} & \cdots & s_{(u_1,u_n)} \\ s_{(u_2,u_1)} & s_{(u_2,u_2)} & & s_{(u_2,u_n)} \\ \vdots & & \ddots & \vdots \\ s_{(u_n,u_1)} & s_{(u_n,u_2)} & \cdots & s_{(u_n,u_n)} \end{bmatrix} \quad (15)$$

where $s_{(u_i,u_k)} = -\left\| c_{u_i} - c_{u_k} \right\|^2$. The cluster center $SC = \{sc_1, sc_2, \cdots, sc_p\}$ is obtained by using an improved AP algorithm [40], in which sc_i denotes the feature corresponding to the *i*-th cluster center.

Algorithm 1 The social user circle partition algorithm for disinformation dissemination

Input: Social user set U, User historical propagation disinformation set $G_F^{u_i}$, Social relationship set *SR*, Disinformation propagation sequence $prop(f_i) = \{(u_0, socialsitu(t_0)), (u_1, socialsitu(t_1)), \cdots, (u_k, socialsitu(t_k))\}$

Output: Social user circle feature set $SC = \{sc_1, sc_2, \cdots, sc_p\}$

1. Initialize *K*, *l*, $Loss_{min}$,t_0, β
2. **for** $u_i \in U$ and i $\leftarrow$ 1to $|U|$ **do**
3. **for** $f_k \in G_F^{u_i}$ and k $\leftarrow$ 1to *K* **do**
4. Encode disinformation f_k into $x_k \in R^l$ by Bert algorithm from Eq(1);
5. Generate text sequence matrix $X_{u_i} \in R^{K \times l}$;
6. **end for**
7. **end for**
8. Calculate the parameters of the Bi-LSTM and auto-encoder model from Eq(2) - Eq(8);
9. Calculate the loss function value *Loss* of the Bi-LSTM and auto-encoder model from Eq(9);
10. **if** $Loss \leq Loss_{\min}$
11. **break**
12. **end if**
13. Generate propagation content feature vector $x_{u_i}^{(I)}$;
14. Calculate social relationship feature vector $x_{u_i}^{(S)}$ from Eq(10)- Eq(13);
15. Generate propagation preference feature vector c_{u_i} from Eq(14);
16. Generate the cluster center set $SC = \{sc_1, sc_2, \cdots, sc_p\}$ by improved AP algorithm;
17. **Return** social user circle feature set *SC*

B. Representation of the Disinformation Propagation Characteristics

1) Content feature representation: First, each word w_i of disinformation f_i ($f_i = \{w_1, w_2, \cdots, w_m\}$) is embedded into the vector $x_i \in R^{K_D}$ through the embedding layer. Then, *Bi-LSTM* is utilized to obtain the hidden feature representation $e_{C'}$ of disinformation. Finally, the embedding matrix of

disinformation content feature can be expressed as $e_{C'} = \{h_1, h_2, \cdots, h_m\}$, where $e_{C'} \in R^{m \times K_D}$.

2) Crowd response feature representation: Due to the novelty and temptation of disinformation in social platform, it usually causes the response of social user crowds during the spread of disinformation. The crowd response of disinformation f_i can be described as a response sequence composed of a group of users, that is $R(f_i) = \{(u_1, r_1, t_1), (u_2, r_2, t_2), \cdots, (u_n, r_n, t_n)\}$. The tuple $(u_i, r_i, t_i) \in R(f_i)$ indicates that the user u_i responds to the disinformation f_i with the response r_i at time t_i. For each tuple, we utilize the Bi-LSTM *module* to extract the hidden feature vector $c_i \in R^{d_1}$ of the content r_i of user comments. In addition, the basic attribute characteristics of the user u_i contain *account age*, *gender* (0/1), *friends count*, *publishing information count*, *followers count*, *followers to friends ratio*, *follower rate*, and *friend rate*. The basic attribute feature vector $b_i \in R^{d_2}$ corresponding to the user is obtained through the embedding layer. Therefore, the *i*-th response characteristic of disinformation f_i can be expressed as

$$r_i = c_i \oplus b_i, \ r_i \in R^d \tag{16}$$

where $d=d_1+d_2$, d_1 and d_2 represent the dimensions of the user comment feature and the basic attribute feature vector, respectively. The crowd response characteristic matrix of disinformation f_i can be expressed as

$$e_{R'} = r_1 \oplus r_2 \oplus \cdots \oplus r_n \tag{17}$$

where $e_{R'} \in R^{n \times d}$.

3) Time-series feature representation: First, time slice and discretize the complete lifecycle of disinformation is utilized to obtain the time-series of disinformation propagation. For a given disinformation f_i, the propagation time length T is divided into multiple time intervals, say, $T = \{\Delta t_1, \Delta t_2, \cdots, \Delta t_n\}$. At the same time, the propagation quantity in each time interval is calculated. Thus, the time-series of propagation quantity can be represented as $P = \{p_{\Delta t_1}, p_{\Delta t_2}, \cdots, p_{\Delta t_n}\}$. Then, the embedding matrix $e_P \in R^{n \times K_T}$ of time-series P is obtained through the embedding layer. Bi-LSTM can not only capture the hidden features of propagation time-series from both backward and forward hidden states but also mine the long-term dependencies in time -series. Therefore, the embedding matrix e_p is fed into the *Bi-LSTM* network to further extract the disinformation propagation time-series characteristics $e_{P'} = \{e_{t_1}, e_{t_2}, \cdots, e_{t_n}\}$ ($e_{P'} \in R^{n \times K_T}$) .

C. Trend Identification Model of Disinformation dissemination

1) Construction of attention mechanism model based on multi-feature fusion: Different social user circles may have different impacts on the dissemination process of disinformation. Some social user circles may better promote the dissemination of disinformation of some specific contents, thus affecting the dissemination trend of this kind of disinformation. Therefore, the interaction and influence of social user circles and disinformation propagation should be considered. We utilize an attention mechanism to obtain the impact of different social circles on disinformation content and realize the feature representation of social user circles combined with the characteristics of social content. The specific formulas are shown as follows.

$$B_i = W'_{sc} \tanh(W_{sc} sc_i) \odot \tanh(W_c c') \tag{18}$$

$$\alpha_{SC} = soft\max(B) \tag{19}$$

$$sc' = \sum_{i=1}^{p} \alpha_{SC_i} \cdot sc_i \tag{20}$$

where B_i indicates the influence of the *i*-th social user circle during the spread of disinformation, sc_i denotes the *i*-th social circle characteristic, and c' refers to disinformation content characteristic.

Due to the novelty and temptation of disinformation, the interaction process between social users and disinformation may generate more crowd responses at the early stages of dissemination. However, it is difficult to obtain the key and effective time characteristics at the early stages of propagation due to the short observable time length. The time characteristics of this stage have no obvious impact on the identification of the dissemination trend of disinformation. At stable stage, time characteristics can better affect the communication trend of disinformation. Therefore, different characteristics may have different impacts on the dissemination trend at different time stages. By utilizing the attention mechanism [41], we pay more attention to the time steps that have a great impact on the dissemination trend of disinformation and pay less attention to other steps. The input vector corresponding to the attention mechanism can be expressed as

$$m_{t_i} = Concat(sc'_{t_i}, c'_{t_i}, r'_{t_i}, p'_{t_i}) \tag{21}$$

where sc'_{t_i}, c'_{t_i}, r'_{t_i} and p'_{t_i} represent the hidden states of social user circle characteristic, content characteristic, crowd response characteristic and time-series characteristic at step t_i respectively. We decompose matrix M into query matrix Q, key matrix K and value matrix V, which are expressed as follows:

$$Q = MW^{(Q)} \tag{22}$$

$$K = MW^{(K)} \tag{23}$$

$$V = MW^{(V)} \tag{24}$$

where M refers to the combination of vectors m_{t_i} of each time step, $M \in R^{T \times d}$, T represents the total number of time steps, and $W^{(Q)}$, $W^{(K)}$ and $W^{(V)}$ represent the mapping of matrix M to the corresponding weight matrix in different linear spaces respectively. In addition, we set the above three weight matrices by random initialization, and further optimize the weights by using the gradient corresponding to the training data. The attention module can be expressed as

$$Atten(Q, K, V) = Soft\max(\frac{QK^T}{\sqrt{d}})V \tag{25}$$

where d refers to the dimension of matrices Q, K and V. In addition, the multi-head attention model can simultaneously consider the subspace representation information corresponding to different positions. Therefore, we further boost the performance of the model through the multi-head attention mechanism. Some heads may pay attention to the impact of crowd response characteristics at the early stages of dissemination, while others may pay attention to the impact of time-series characteristics on disinformation dissemination at

other stages. The simplified form of attention module is shown as follows:

$$H = \text{Attentive}(M) \quad (26)$$

where H represents the output of the attention mechanism model of multi-feature fusion.

2) Disinformation dissemination trend identification: To identify the propagation trend of disinformation, we design a multi-layer perceptron with multiple full connection layers based on multi-feature fusion. The specific calculation formula is shown as follows:

$$\hat{y} = W_{h_2}\,\mathrm{Re}lu(W_{h_1} \cdot H + b_{h_1}) + b_{h_2} \quad (27)$$

where W_{h_1}, W_{h_2}, b_{h_1} and b_{h_2} represent the weights and biases to be learned in the full connection layer, respectively. $\hat{y}$ indicates the identification result of the propagation trend of disinformation.

Algorithm 2 Disinformation propagation trend identification algorithm

Input: Social user spread disinformation collection $G_F^{u_i} = \{(F, u_i) \mid F = \{f_1, f_2, \cdots, f_n\}, u_i \in U\}$; Social user circle feature collection $SC = \{sc_1, sc_2, \cdots, sc_p\}$; Social user crowd response collection $R = \{(R_i, f_i) \mid R_i = \{(u_1, r_1, t_1), (u_2, r_2, t_2), \cdots, (u_n, r_n, t_n)\}, f_i \in F\}$

Output: Propagation trend matrix $Y^* = \arg\max_i P_i(Y_i \mid G, F, SC, R)$

Initialize parameter θ, epoch_max, epoch, batch_size
for all $(x_k, y_k) \in$ TrainingDataset **do**
  while epoch $\leq$ epoch_max **do**
    for each batch $\subseteq$ TrainingDataset **do**
      Calculate the embedding vector of content features c' by utilizing embedding layer and Bi-LSTM module;
      Calculate the embedding vector of crowd response features r' from Eq(16)-Eq(17);
      Calculate the embedding vector of time-series features p' by utilizing embedding layer and Bi-LSTM module;
      Calculate the social user circle features sc' from Eq(18)-Eq(20);
      Calculate multi-feature fusion vector H from Eq(21)-Eq(26);
      Calculate propagation trend identification results $\hat{y}$ from Eq(27);
      Update the model parameter set θ by Adam algorithm;
      epoch = epoch+1
    endfor
  endwhile
endfor
for all $x_k \in$ TestingDataset **do**
  Predict $Y^* = \arg\max_i P_i(Y_i \mid G, F, SC, R)$
endfor
Return Y^*

V. Experimental Setup and Results

A. Experimental Setup

We first describe the experimental dataset including Socialsitu metadata and then introduce the evaluation indicators used in the experiment. Finally, several representative methods are provided and discussed.

1) Experimental Data: We choose a real online social network platform Shareteches (formerly CyVOD) [42] (http://www.shareteches.com) to carry out the experimental study. The platform includes mobile applications (Android and iOS) and website platform, and the platform dynamically obtains the Socialsitu metadata sequence generated by social users in real-time. The Socialsitu metadata has been widely used in social user behavior pattern analysis [23], malicious social bot detection [43] and social network platform security evaluation [44]. We collect 1,858,575 Socialsitu metadata including comprehensive information from the beginning of social users' first appearance on this platform until October 2021. By preprocessing those Socialsitu metadata, we further obtain Socialsitu metadata with regard to disinformation in all sessions and reconstruct an entire disinformation dataset for exploring the disinformation propagation law. The disinformation dataset contains rich attributes, such as text and picture content, publisher profiles, forwarder profiles and user comment information. Due to the poor standardization of disinformation content in social platform, we utilize regular expressions including punctuation and emoticons, to filter special text symbols.

2) Evaluation Metrics: In this article, two sets of evaluation indexes are utilized for our proposed methods, including the regression task which is to identify the disinformation propagation trend and the classification task which is to identify the disinformation propagation scope.

For the regression task of propagation trend identification, we evaluate the performance of the presented methods utilizing the following three indexes:

- *MSE* refers to the Mean Squared Error, which embodies the change of the error between the real value y_i and the predicted value $\hat{y}_i$ in the test set. The calculation formula of *MSE* is represented as $E_{MSE} = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2$.
- *RMSE* represents the Root Mean Squared Error, which is the arithmetic square root of *MSE*. Moreover, *RMSE* is usually used to calculate the deviation between the predicted value $\hat{y}_i$ and the real value y_i in the test set. The calculation formula of *MSE* is denoted as $E_{RMSE} = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2}$.
- *MAE* is the Mean Absolute Error, which is calculated by the sum of the absolute error value of the real value y_i and the predicted value $\hat{y}_i$ in the test set. Moreover, it can intuitively embody the gap between the predicted

value $\hat{y}_i$ and the real value y_i. The specific calculation formula of *MAE* is $E_{MAE} = \frac{1}{n}\sum_{i=1}^{n}|y_i - \hat{y}_i|$.

Here, to improve the fitting effect in the model training process, we select the same transformation method as deepcas [45]. The calculation formula is given as follows:

$$y_i = \ln(n_i + 1) \quad (28)$$

where n_i denotes the actual propagation quantity of disinformation f_i.

For the classification task, it is important to select a suitable threshold τ of propagation scope. First, according to the propagation quantity y_i of disinformation, the disinformation samples are sorted from high to low. Similar to prior research [50], the proportion of the division standard corresponding to the disinformation with large propagation scope and the disinformation with small propagation scope is set to 1:4. Thus, the size of the threshold is determined. After calculating the threshold τ of propagation scope, then disinformation with $y_i(T) \geq \tau$ is labeled large scale propagation tendency. Otherwise, it is labeled small scale propagation tendency. Here, *T* refers to the selected determined time parameter. To evaluate the performance of the model for the classification task, we select the following indexes:

- *Precision* is represented as $P = \frac{TP}{TP + FP}$.
- *Recall* is represented as $R = \frac{TP}{TP + FN}$.
- *F*1-*score* refers to the harmonic mean of *Precision* and *Recall*, which is defined as $F1 - score = \frac{2 \times TP}{2 \times TP + FP + FN}$.

Here, *TP* indicates the propagation scope of disinformation identified by the model is greater than the threshold τ, and the actual propagation scope is greater than the threshold τ. *FN* represents the propagation scope of disinformation identified by the model is greater than the threshold τ and the actual propagation scope is less than the threshold τ. *FP* indicates the propagation scope of disinformation identified by the model is less than the threshold τ and the actual propagation scope is greater than the threshold τ. *TN* refers to the propagation scope of disinformation identified by the model is less than the threshold τ, and the actual propagation scope is less than the threshold τ. The classification results are represented as a confusion matrix (see Table II).

TABLE II
CONFUSION MATRIX FOR CLASSIFICATION MODEL

Actual class	Predicted class	
	Large scale propagation ("1")	Small scale propagation ("0")
Large scale propagation ("1")	True positive, TP	False negative, FN
Small scale propagation ("0")	False positive, FP	True negative, TN

3)Baseline Approaches: To comprehensively evaluate the effect of the disinformation dissemination trend method presented in this study, we analyzed and discussed several representative approaches:

DyDiff-VAE[46]: DyDiff-VAE is a diffusion model, which can predict the final propagation scope of information according to the propagation probability.

RNe2Vec[47]: The RNe2Vec model presented by researchers is a method for predicting the popularity of information dissemination. We employ this method to predict the propagation trend of disinformation.

NT-EP[48]: NT-EP is a non-topology approach by constructing a weighted propagation graph for each information. Moreover, this model is capable of predicting the propagation scope of information.

Inf-VAE[49]: Inf-VAE is a propagation prediction model based on variational auto-encoder integrated homophily and influence.

EPAB[50]: This model represents the user characteristics, time-series characteristics and network structure characteristics, and uses a Bayesian network to predict the information trend.

Other methods: We select some traditional machine learning and deep learning algorithms, such as support vector machine [51] and bidirectional long short-term memory network [52], to solve the problem of dissemination trend identification.

B. Results and analysis

We report and discuss the experimental results utilizing the following six components: i) analyze and discuss the correlation between disinformation dissemination trend and the types of audience entities; ii) analyze and discuss the correlation between disinformation dissemination trend and propagation time; iii) analyze and compare the impact of different social user circles on the identification results of dissemination trend; iv) compare and discuss the effects of different feature combinations on the identification results of dissemination trend; v) design the epoch parameter experiment of the propagation trend method; vi) evaluate the effectiveness of the propagation trend method.

1) Correlation analysis between the dissemination trend of disinformation and the types of audience entities: According to the propagation scope of disinformation, we divide the audience entities into three types: (1) Local social platforms; (2) Individuals and groups of third-party social platforms (WeChat, Weibo, QQ and LinkedIn, etc.); (3) Circles of friends of third-party social platforms. Specifically, type (1) refers to the dissemination of disinformation in the original social platform, and type (2) and (3) refer to the dissemination of disinformation in the third-party social platform. The spread scope of disinformation from the three audience entity types increases in turn.

First, we select the Lorentz curve index to quantify the difference and inequality of the trend distribution of disinformation dissemination corresponding to three types of audience entities. This index is utilized to measure the cumulative percentage of communication (disinformation shared) on three types of audience entities as a function of the cumulative percentage of communication users. As shown in Fig. 4, the complete equal Lorentz curve is selected as the reference line. The Lorentz curve corresponding to the circle of friends type shared by users to the third-party social platform is the farthest from the complete equal Lorentz curve, and the

Lorentz curve corresponding to the local social platform shared by users is the closest to the complete equal Lorentz curve. Specially, for the local social platform type, we find that when the cumulative proportion of dissemination users is less than 15%, the proportion of sharing disinformation is close to 0. Moreover, 85% of users tend to spread on local social platforms. For the third-party social platforms types, we observe that when the cumulative proportion of dissemination users is less than 65%, the proportion of sharing disinformation in the third-party platform is close to 0. At the same time, only 35% of users prefer to share disinformation by utilizing the third-party platforms. Therefore, our analysis shows that the proportion of disinformation propagated by social users through local platform is greater than that of the third-party social platform, which may be caused by the concealment of disinformation in the dissemination process and the mutual imitation between communicators. In addition, we also found that the two types of curves corresponding to social users sharing to third-party social platforms are very close, which shows that the quantitative trend of spreading disinformation corresponding to individuals, groups and circles of third-party social platforms keeps consistent. In other words, communicators have no obvious tendency to choose individuals, groups and circles in the process of cross-platform communication.

Based on the Lorentz curve, the Gini coefficient of three audience entity types can be calculated using the following formula.

$$\hat{G}=1-\sum_{m=1}^{p}(X_m - X_{m-1})(Y_m + Y_{m-1}) \qquad (29)$$

where X_m (m=1,…,p) represents the cumulative proportion of disinformation disseminators, Y_m (m=1,…,p) refers to the cumulative proportion of audience entities corresponding to communicators. Here, X_0=Y_0=0, X_p=Y_p=1, X_{m-1}<X_m, Y_{m-1}<Y_m. Table III denotes the Gini coefficient for each audience entity type. By analyzing Lorentz curve and Gini coefficient for each audience entity type from Fig. 4 and Table III, we can conclude that while disinformation occurs across OSN platforms, the disinformation is more likely to spread widely in the original OSN platform.

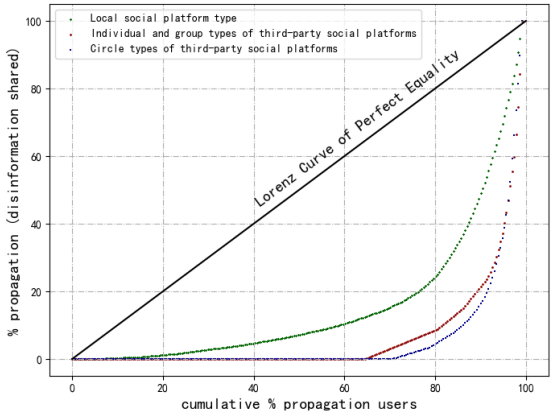


Fig. 4. Lorenz curves of the disinformation propagation inequality for three types of audience entities. Type 1 (local social platform) is shown in green, type 2 (individuals and groups of third-party social platforms) in darkred, and type 3 (circles of friends of third-party social platforms) in blue. This analysis is based on Socialsitu metadata, the local social platform denotes Shareteches, and the third-party social platform represents Weibo, WeChat, QQ and LinkedIn, etc. The Lorenz curve of perfect equality serves as a reference in this figure.

TABLE III
GINI COEFFICIENT FOR EACH AUDIENCE ENTITY TYPE

Propagation audience entity type	Gini coefficient
Local social platform	0.697
Individuals and groups of third-party social platforms	0.881
Circles of friends of third-party social platforms	0.901

2) Correlation analysis between disinformation dissemination trend and propagation time: The disinformation in OSNs usually includes three processes: release, dissemination, and extinction. However, due to the influence of the disseminator's interest and preference, and rumor refutation information, the trend of the quantity of each disinformation may vary at different time stages. To analyze the rule of the propagation trend of disinformation over time, we first employ the Latent Dirichlet allocation topic model to classify the disinformation topic [53] and select the current global hot the COVID-19 topic as a case to study the dissemination trend. Considering the variation amplitude and peak time of the disinformation propagation trend, we divide the propagation trend into the following four types. On the one hand, the spread trend of disinformation can reflect the heat and risk of disinformation as a whole. On the other hand, this provides an effective strategy for social platform managers to further adopt fine-grained and refined schemes to control the large-scale dissemination of disinformation in time. The division standard we adopt is based on the variation amplitude of disinformation dissemination trend and the time corresponding to the peak of disinformation dissemination. Specially, the variation amplitude of the spread trend of disinformation can intuitively reflect the spread range of disinformation. The time corresponding to the peak of disinformation dissemination reflects the propagation speed over a period of time. Fig. 5 shows the propagation trend of representative disinformation under the topic of the COVID-19. Among the four propagation trends, type (2) and type (4) make up the majority (81.2%). Moreover, type (1) accounts for the least (8.9%).

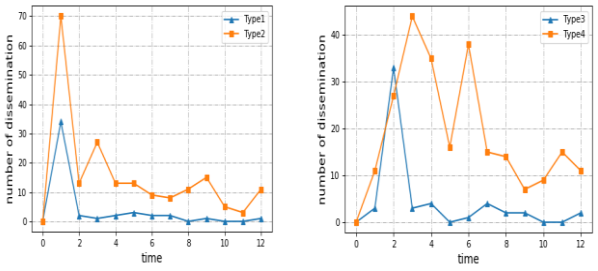
Type (1): The propagation quantity of disinformation increases first and then decreases with time until it finally dies. At the same time, there is only one propagation peak in the middle, and the time t_p to reach the peak is no more than 1h from the release time t_0, that is $|t_p - t_0| \le 1$.

Type (2): The propagation quantity of disinformation increases first and then decreases with time. This process can be repeated multiple times until it finally dies. At the same time, there are multiple propagation peaks in the middle, and the first

peak time t_p is no more than 1h from the release time t_0, that is $|t_p - t_0| \le 1$.

Type (3): The propagation quantity of disinformation first increases and then decreases with time until it finally dies. At the same time, there is only one peak in the middle, and the time t_p to reach the peak is more than 1h from the release time t_0, that is $|t_p - t_0| > 1$.

Type (4): The propagation quantity of disinformation increases first and then decreases with time. This process can be repeated multiple times until it finally dies. At the same time, there are multiple propagation peaks in the middle, and the first peak time t_p is more than 1h from the release time t_0, that is $|t_p - t_0| > 1$.



(a) $|t_p - t_0| \le 1$ (b) $|t_p - t_0| > 1$

Fig.5. Four types of propagation trend for representative disinformation under the COVID-19 topic. **(a)** The two types (type1 and type 2) meet the condition that the first propagation peak time t_p is no more than 1h from the disinformation release time t_0. An example of type 1: "Taking antibiotics can effectively prevent and treat Novel Coronavirus". An example of type 2: "Novel coronavirus pneumonia is confirmed if the throat swabs are positive". **(b)** The two types (type 3 and type 4) meet the condition that the first propagation peak time t_p is more than 1h from the disinformation release time t_0. An example of type 3: "Vaccines against common pneumonia can prevent New Coronavirus infection". An example of type 4: "As long as novel coronavirus pneumonia is exposed to sweat, humans will infect COVID-19".

3) Influence of social user circle division on propagation trend identification results: We select the best clustering number of social user circles by changing the value of the preference parameter (p) in the improved AP clustering algorithm. The value of parameter p is usually set to 2 ~ 6 times the mean of the similarity matrix S, so the clustering number of social user circles is 6, 7, 10, 11 and 13, respectively. In Fig. 6, when the values of MSE, RMSE and MAE evaluation indexes reach the smallest, the parameter p is 4. With the increasing of parameter p, the MSE, RMSE and MAE evaluation indexes of the propagation trend model decrease firstly, and then increase. This phenomenon is mainly because when the number of social user circles is greater than a specific threshold, some social users can not be accurately divided into a certain social circle. At the same time, the social user circle characteristics of this part are also not fully represented.

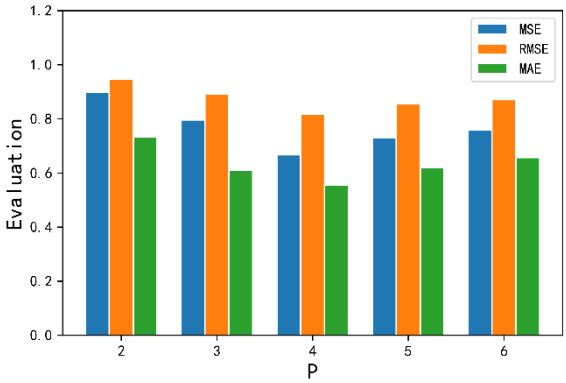


Fig.6. Influence of clustering number of social user circles on communication trend identification results. The horizontal and vertical axes refer to the preferences and evaluation indexes (MSE, RMSE and MAE), respectively. When the value of preference parameter p is 4, the corresponding value of the above three evaluation indexes is the smallest, and the identification result corresponding to the propagation trend model is the best. Therefore, we choose 10 as the optimal number for the social user circles.

4) Influence of different feature combinations on propagation trend identification results: To evaluate the effectiveness of the disinformation propagation trend identification algorithm proposed in this paper, we design five different feature combination methods for comparative experiments, as shown in Table IV.

TABLE IV
CLASSIFICATION OF DIFFERENT FEATURE COMBINATIONS

Control experiment	Feature combination
Combination 1	Social user circle feature + Content feature
Combination 2	Social user circle feature + Crowd response feature
Combination 3	Social user circle feature +Time-series feature
Combination 4	Content feature + Crowd response feature + Time-series feature
Combination 5	All features

According to the analysis of the experimental results of the five combination characteristics shown in Table V, combination 5, that is, the method used in this paper yields the best results on MSE, RMSE and MAE, which are 0.698, 0.835 and 0.601, respectively. Moreover, the evaluation indexes including precision, recall and F1-score are also better than the other four combination methods. According to the experimental results corresponding to combination 1, combination 2 and combination 3, we can observe that content feature, crowd response feature and time-series feature have different impacts on the identification results of disinformation dissemination trend, in which content feature is better than crowd response characteristic and time-series feature. A more interesting finding is that the characteristics of social user circles are of

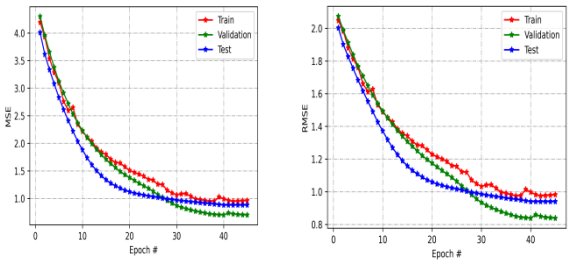
great help to identify the dissemination trend of disinformation through the results of combination 4 and combination 5. This is because disinformation presents the phenomenon of circle clustering in the dissemination process, and some social user circles can better promote the dissemination of disinformation. Therefore, to accurately identify the disinformation dissemination trend, we should consider the characteristics of the social user circle.

In addition, by comparing the five combined features, we find that the best effect is achieved by integrating the social user circle features with content features, crowd response features and time-series features. This is because the multi-feature fusion can effectively reduce the insufficient expression of a single feature on the dissemination trend of disinformation and improve the overall ability to describe the dissemination trend.

TABLE V
COMPARISON OF EXPERIMENTAL RESULTS OF DIFFERENT FEATURE COMBINATIONS

Control experiment	MSE	RMSE	MAE	Precision	Recall	F1-score
Combination 1	0.719	0.848	0.622	0.527	0.801	0.635
Combination 2	0.765	0.875	0.649	0.513	0.764	0.614
Combination 3	0.794	0.891	0.678	0.506	0.664	0.574
Combination 4	0.825	0.908	0.721	0.482	0.615	0.506
Combination 5	0.698	0.835	0.601	0.541	0.879	0.670

5) Effect of the epoch parameters of model performance on propagation trend identification: By setting 45 different epoch parameters, we conduct experiments on the identification effect of disinformation propagation trend in the training set, verification set and test set, respectively. The results are shown in Figure 7. We find that at the beginning of the model training, that is, when epoch is 1, the MSE and RMSE evaluation indexes corresponding to the training set, verification set and test set are relatively large, which indicates that the model is not capable of learning the hidden state feature representation of the disinformation propagation process. So the performance of the model is not ideal. With the increase of the epoch parameters of the model training, when the epoch is 20, the MSE and RMSE evaluation indexes corresponding to the above three sets decrease rapidly, indicating that the model has preliminarily completed the hidden layer feature representation of the propagation process of disinformation. After the 40th epoch, the MSE and RMSE tend to be stable and almost unchanged, indicating that the model yields a good trend identification effect. As the number of epoch continuous increases, the model can reach the convergence state, that is, the optimal propagation trend identification effect is achieved.



(a) MSE (b) RMSE

Fig.7. Influence of the number of epoch on the identification effect of communication trend. The red, green, and blue lines denote the MSE and RMSE evaluation indexes of the model training, cross-validation process, and test process, respectively, in each generation.

6) Propagation trend performance analysis: We analyze the performance of the propagation trend approach designed in this study from the perspective of regression and classification. The quantitative trend and scope of disinformation propagation after 12*h* are identified by utilizing the propagation sequence before 3*h*.

For the regression experiment of disinformation propagation, we compare the propagation trend identification algorithm with baseline methods and select different evaluation indexes as standards to evaluate the effect of different algorithms. Fig. 8 shows the experimental results of different regression methods. It can be concluded that the performance of the deep learning methods including DyDiff-VAE, Inf-VAE and EPAB is better than that of RNe2Vec and NT-EP. In addition, the impact of the characteristics of the social user circles on disinformation dissemination is not considered in the above baseline methods. Therefore, we improve the generalization ability of the model and achieve the optimal identification results by comparing the different evaluation metrics.

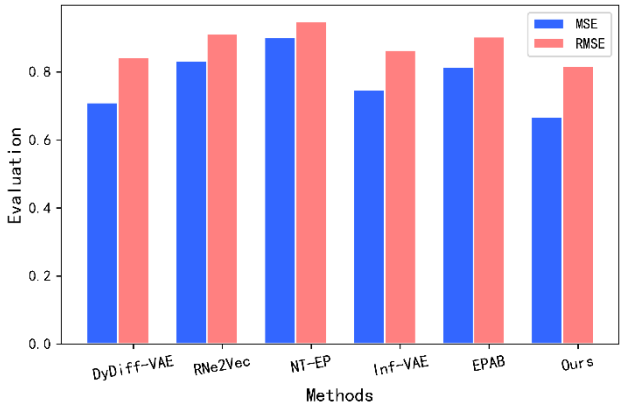


Fig. 8. Comparison of experimental results of different regression methods. The abscissa represents six different methods including DyDiff-VAE, RNe2Vec, NT-EP, Inf-VAE, EPAB and ours. See baseline Methods (V-A) for further details. The ordinate refers to evaluation indexes including MSE and RMSE. We compare the performance of six approaches based

on MSE and RMSE indexes via histograms. Consequently, we can see that the performance of the propagation trend method in this study is better than that of the other five baseline approaches.

For the classification experiment of disinformation dissemination scope, if the identified disinformation propagation scope is greater than the specified threshold, the disinformation is classified into a large-scale propagation tendency category. Otherwise, it is classified into the small-scale propagation tendency category. As shown in Figure 9, the baseline models including DyDiff-VAE, NT-EP, Bi-LSTM and SVM-TS, yield an F1-score of 0.683, 0.638, 0.558 and 0.610 in the test set, respectively. However, we can obtain an F1-score of 0.699 in the test set. As a whole, the experimental results indicate that the proposed approach is superior to the baseline approaches, which further proves the effectiveness of the propagation scope identification approach presented in this article.

To further describe the propagation trend of disinformation, this study utilizes time-slicing during the active period of disinformation dissemination and identifies the propagation trend of disinformation at different time slices. In the experiment, we first take the propagation sequence of the first 3*h* as the input to identify the propagation trend of the 4*h*. Then, according to the propagation sequence of the first 4*h*, the propagation trend of the 5*h* is identified. This process continues until the 12*h* propagation trend is identified. Fig. 10 indicates the MSE, MAE and RMSE indices of the proposed model during the active period of disinformation propagation. We can see that the MSE and RMSE of the proposed model fluctuate 0.3-0.5 and 0.55-0.7 during the 4*h*-12*h* of disinformation propagation, respectively. At the same time, the MAE fluctuates between 0.43 and 0.55. This demonstrates that the model presented in this article can effectively identify the propagation trend of disinformation.

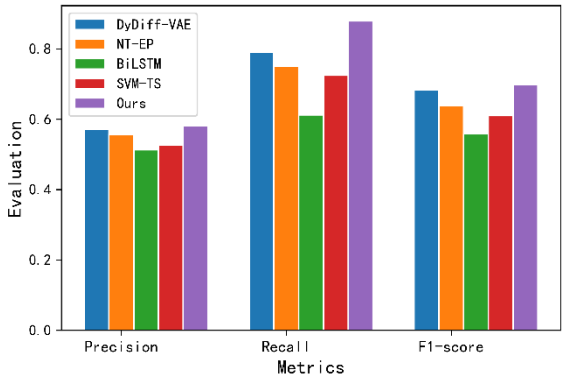


Fig. 9. Comparison of experimental results of different classification methods. The abscissa denotes three evaluation metrics including precision, recall and F1-score. The ordinate represents the evaluation values of different classification approaches.

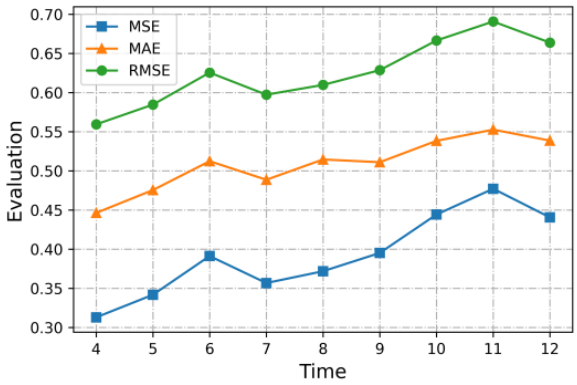


Fig. 10. Trend identification performance comparison for different propagation time lengths. The horizontal axis denotes the time slice during the active period of disinformation dissemination, and the vertical axis denotes the evaluation indexes at different time slices.

VI. CONCLUSION

Compared with the previous study, we are the first to adopt social situation analytics technology in disinformation propagation trend identification. Specially, we construct a trend analysis and identification model of disinformation dissemination, which is based on social situation analytics, based on the social user's propagation sequence and propagation content in social networks. We determine that while disinformation occurs across OSN platforms, the disinformation is more likely to spread widely in the original OSN platform. Additionally, we also identify four typical disinformation propagation trends based on propagation patterns and propagation peak times.

Thus, we propose a social user circle division and representation method, which is based on users' dissemination of disinformation content and social contextual information Then, the disinformation content feature, crowd response feature and time-series feature are represented by utilizing the embedding layer and Bi-LSTM. Furthermore, we present an attention mechanism model based on multi-feature fusion (the content characteristics, crowd response characteristics, time-series characteristics and social user circle characteristics), which can dynamically adjust the weight of each feature. The fused features are fed into the multi-layer perceptron to identify the propagation quantity trend and propagation scope. Utilizing the 1,858,575 Socialsitu metadata collected from online social network platform, the evaluation shows that our model outperforms other comparison approaches and yields the optimal effect.

Based on the identification of disinformation dissemination trend, we will further investigate the relationship between users' propagation behavior, desire and goal to realize the effective control of disinformation dissemination in the future.

REFERENCES

[1] Zhang T, Gong X, Chen C L P. BMT-Net: Broad Multitask Transformer Network for Sentiment Analysis. IEEE Transactions on Cybernetics, 2021, doi: 10.1109/TCYB.2021.3050508

[2] Zhang T, Wang X, Xu X, et al. GCB-Net: Graph Convolutional Broad Network and Its Application in Emotion Recognition. IEEE Transactions

on Affective Computing, 2022, 13(1): 379–388
[3] Zong Y, Zheng W, Hong X, et al. Cross-Database Micro-Expression Recognition: A Benchmark. Proceedings of the 2019 on International Conference on Multimedia Retrieval, 354–363, 2019
[4] Vosoughi S, Roy D, Aral S. The spread of true and false news online. Science, 2018, 359(6380): 1146–1151
[5] Li L, Zhang Q, Wang X, et al. Characterizing the Propagation of Situational Information in Social Media During COVID-19 Epidemic: A Case Study on Weibo. IEEE Transactions on Computational Social Systems, 2020, 7(2): 556–562
[6] Leng Y, Zhai Y J, Sun S J, et al. Misinformation During the COVID-19 Outbreak in China: Cultural, Social and Political Entanglements. IEEE Transactions on Big Data, 2021, 7(1): 69–80
[7] Zhang T, Lei C, Zhang Z, et al. AS-NAS: Adaptive Scalable Neural Architecture Search with Reinforced Evolutionary Algorithm for Deep Learning. IEEE Transactions on Evolutionary Computation, 2021, 25(5): 830–841
[8] Gong X, Zhang T, Chen C L P, et al. Research Review for Broad Learning System: Algorithms, Theory, and Applications. IEEE Transactions on Cybernetics, 2021, doi: 10.1109/TCYB.2021.3061094
[9] Lazer D M J, Baum M A, Benkler Y, et al. The science of fake news. Science, 2018, 359(6380): 1094–1096
[10] Butcher P. COVID-19 as a turning point in the fight against disinformation. Nature Electronics, 2021, 4(1): 7–9
[11] Cho J H, Rager S, John O'Donovan, et al. Uncertainty-based False Information Propagation in Social Networks. ACM Transactions on Social Computing, 2019, 2(2): 1–34
[12] Shrivastava G, Kumar P, Ojha R P, et al. Defensive modeling of fake news through online social networks. IEEE Transactions on Computational Social Systems, 2020, (99):1–9
[13] Dong S, Huang Y C. SIS Rumor Spreading Model With Population Dynamics in Online Social Networks. Proceedings of the 2018 International Conference on Wireless Communications, Signal Processing and Networking, 2018
[14] Xiao Y, Yang Q, Sang C, et al. Rumor Diffusion Model Based on Representation Learning and Anti-Rumor. IEEE Transactions on Network and Service Management, 2020, (99):1910–1923
[15] Wu L, Liu H. Tracing Fake-News Footprints: Characterizing Social Media Messages by How They Propagate. Proceedings of the 11th ACM International Conference on Web Search and Data Mining, 637–645, 2018
[16] Glenski M, Weninger T, Volkova S. Propagation from Deceptive News Sources Who Shares, How Much, How Evenly, and How Quickly?. IEEE Transactions on Computational Social Systems, 2018, 5 (4): 1071–1082
[17] Zhao Z, Zhao J, Sano Y, et al. Fake News Propagate Differently from Real News Even at Early Stages of Spreading. EPJ Data Science, 2020, 9(1): 1–14
[18] Moon S A, Sahneh F D, Scoglio C. Group-Based General Epidemic Modeling for Spreading Processes on Networks: GroupGEM. IEEE Transactions on Network Science and Engineering, 2021: 434–446
[19] Liu S H, Wang B, Deng X J, et al. Self-Attentive Graph Convolution Network with Latent Group Mining and Collaborative Filtering for Personalized Recommendation. IEEE Transactions on Network Science and Engineering, doi: 10.1109/TNSE.2021.3110677, 2021
[20] Chang C, Jiang H, Ming H, et al. Situ: A situation-theoretic approach to context-aware service evolution. IEEE Transactions on Services Computing, 2009, 2(3): 261–275
[21] Chang C. Situation analytics: A foundation for a new software engineering paradigm. Computer, 2016, 49(1):24–33
[22] Chang C. Situation analytics-at the dawn of a new software engineering paradigm. Science China Information Sciences, 2018, 61(05): 050101
[23] Zhang Z, Sun R, Wang X, et al. A Situational Analytic Method for User Behavior Pattern in Multimedia Social Networks. IEEE Transactions on Big Data, 2019, 5(4): 520–528
[24] Zhang Y, Su Y, Li W, et al. Rumor and Authoritative Information Propagation Model Considering Super Spreading in Complex Social Networks. Physica A: Statistical Mechanics and Its Applications, 2018, 506: 395–411
[25] Guo J, Chen T, Wu W. A Multi-Feature Diffusion Model: Rumor Blocking in Social Networks. IEEE Transactions on Networking, 2021, 386–397
[26] Cui L, Xie G, Yu S, et al. An Inherent Property Based Rumor Dissemination Model in Online Social Networks. IEEE Networking Letters, 2020, 2(1): 43–46
[27] Wang C, Wang G, Luo X , et al. Modeling Rumor Propagation and Mitigation across Multiple Social Networks[J]. Physica A: Statistical Mechanics and its Applications, 2019, 535: 122240
[28] Shao C C, Ciampaglia G L, Varol O, et al. The Spread of Low-credibility Content by Social Bots. Nature Communications, 2018, DOI: 10.1038/s41467-018-06930-7
[29] Shao C C, Ciampaglia G L, Varol O, et al. The Spread of Fake News by Social Bots. arXiv preprint arXiv:1707.07592, 2017
[30] Liu Y, Wu Y. FNED: A Deep Network for Fake News Early Detection on Social Media. ACM Transactions on Information Systems, 2020, 38(3): 1–33
[31] Itti L, Koch C, Niebur E. A Model of Saliency-based Visual Attention for Rapid Scene Analysis. IEEE Transaction Pattern Analysis Machine Intelligence. 1998, 20(11): 1254–1259
[32] Yu F , Liu Q , Wu S , et al. Attention-based Convolutional Approach for Misinformation Identification from Massive and Noisy Microblog Posts. Computers & Security, 2019, 83: 106–121
[33] Ni S., Li J, Kao H, MVAN: Multi-View Attention Networks for Fake News Detection on Social Media. IEEE Access, 2021,9: 106907–106917
[34] Chen T, Li X, Yin H, et al. Call Attention to Rumors: Deep Attention Based Recurrent Neural Networks for Early Rumor Detection. In Trends and Applications in Knowledge Discovery and Data Mining. 2018, 40–52
[35] Zhang Z, Jing J, Li F, et al. Survey on Fake Information Detection, Propagation and Control in Online Social Networks from the Perspective of Artificial Intelligence. Chinese Journal of Computers, 2021, 44(11): 2261–2282
[36] Devlin J, Chang M, Lee K, et al. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, 4171–4186
[37] Miller McPherson, Lynn Smith-Lovin, JamesMCook. 2001. Birds of a feather: Homophily in social networks. Annual review of sociology, 2001, 27, (1): 415–444
[38] Fan W Q, Ma Y, Li Q, et al. Graph Neural Networks for Social Recommendation. Proceedings of the 28th International Conference on World Wide Web, 2019: 13–17
[39] Brusco M J, Kohn H F. Comment on Clustering by Passing Messages Between Data Points. Science, 2008, 319(5864):726c
[40] Lin S, Wa Ng X, Xiao G, et al. Hierarchical Representation via Message Propagation for Robust Model Fitting. IEEE Transactions on Industrial Electronics, 2020, DOI 10.1109/TIE.2020.3018074
[41] Vaswani A, Shazeer N, Parmar N. Attention is All you Need. Proceedings of the Annual Conference on Neural Information Processing Systems. NIPS, 2017
[42] Zhang Z, Sun R, Zhao C, et al. CyVOD: A Novel Trinity Multimedia Social Network Scheme. Multimedia Tools and Applications, 2017, 76(18): 18513–18529
[43] Shi P, Zhang Z, Choo K K R. Detecting malicious social bots based on clickstream sequences. IEEE Access, 2019, 7(1): 28855–28862
[44] Zhang Z, Jing J, Wang X, et al. A crowdsourcing method for online social networks security assessment based on human-centric computing. Human-centric Computing and Information Sciences, 2020, 10(1):1–19
[45] Li C, Ma J, Guo X, et al. Deepcas: An end-to-end predictor of information cascades. Proceedings of the 26th International Conference on World Wide Web, 2017: 577–586
[46] Wang R, Huang Z, Liu S, et al. DyDiff-VAE: A Dynamic Variational Framework for Information Diffusion Prediction. Proceedings of the 44th International ACM SIGIR Conference on Research and Development in Information Retrieval, 2021: 163–172
[47] Shang J, Huang S, Zhang D, et al. RNe2Vec: Information Diffusion Popularity Prediction Based on Repost Network Embedding. Computing, 2021, 103: 271–289
[48] Liu Z T, Quan Z W, Mao R B, et al. NT-EP: A Non-Topology Method for Predicting the Scope of Social Message. Journal of Computer Research and Development. 2020, 57(6): 1312–1322
[49] Sankar A, Zhang X, Krishnan A, et al. Inf-VAE: Avariational Autoencoder Framework to Integrate Homophily and Influence in Diffusion Prediction. Proceedings of the 13th International Conference on Web Search and Data Mining, 2020: 510–518
[50] Wu Q, Yang C, Gao X, et al. EPAB: Early pattern aware Bayesian model for social content popularity prediction. Proceedings of the 18th IEEE International Conference on Data Mining, 2018: 1296–1301
[51] Ma J, Wei G, Wei Z, et al. Detect Rumors Using Time Series of Social

Context Information on Microblogging Websites. Proceedings of the 24th ACM International Conference on Information and Knowledge Management, 2015
[52] Guo H, Cao J, Zhang Y, Guo J, et al. Rumor Detection with Hierarchical Social Attention Network. Proceedings of the 27th ACM International Conference on Information and Knowledge Management. 2020: 943–951
[53] Blei D M, Ng A Y, Jordan M J. Latent Dirichlet allocation. Journal of Machine Learning Research, 2003(3): 993–1022

Junchang Jing received his Bachelor and Master degrees in Mathematics and Information Science at Henan Normal University, Xinxiang, China. He is currently pursuing the Ph.D. degree with Information Engineering College, Henan International Joint Laboratory of Cyberspace Security Applications, Henan University of Science and Technology. His research interests include social network security and computing, social situation analytics, and social big data.

Fei Li received the M.S degree in the Lingnan College of Sun Yat-sen University, Guangzhou, China, in 2009. In 2013, she was a visiting scholar with the Department of Electrical Information, MIIT, Beijing, China, for 19 months. After Jan., 2018, she worked as a senior engineer in the fields of AI and database. Now she is a Ph.D candidate with the Computer Research Institute of the University of Chinese Academy of Sciences and Pengcheng Laboratory, Shenzhen, China. Her research interests include video coding, database, and machine learning.

Bin Song received his Master and Ph.D. degrees in computer science from China University of Geosciences and Korea University, respectively. He is currently a Research Fellow with the Henan International Joint Laboratory of Cyberspace Security Applications, China. Moreover, he is also a lecturer of Henan University of Science and Technology, China. His research interests include artificial intelligence, image processing and computer vision for security applications.

Zhiyong Zhang (Senior Member, IEEE), received received his Master, Ph.D. degrees in Computer Science from Dalian University of Technology and Xidian University, P. R. China, respectively. He was ever post-doctoral fellowship at School of Management, Xi'an Jiaotong University, China. Nowadays, he is Director of Henan International Joint Laboratory of Cyberspace Security Applications, Vice-Dean of College of Information Engineering, and full-time Henan Province Distinguished Professor at Henan University of Science and Technology, China. He is also a visiting professor of Computer Science Department of Iowa State University. His research interests include cyber security and computing, social big data, multimedia content security. Recent years, he has published over 120 scientific papers and edited 6 books in the above research fields, and also holds 15 authorized patents. He is Chair of IEEE MMTC DRMIG, IEEE Systems, Man, Cybernetics Society Technical Committee on Soft Computing, World Federation on Soft Computing Young Researchers Committee, Committeeman of China National Audio, Video, Multimedia System and Device Standardization Technologies Committee. And also, he is editorial board member and associate editor of Multimedia Tools and Applications (Springer), Human-centric Computing and Information Sciences (Springer), IEEE Access (IEEE), Neural Network World, EURASIP Journal on Information Security (Springer), leading guest editor or co-guest Editor of Applied Soft Computing (Elsevier), Computer Journal (Oxford) and Future Generation Computer Systems (Elsevier). And also, he is Chair/Co-Chair and TPC Member for numerous international conferences/ workshops on digital rights management and cloud computing security.

Kim-Kwang Raymond Choo (Senior Member, IEEE) received the Ph.D. in Information Security in 2006 from Queensland University of Technology, Australia. He currently holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio (UTSA). He is the founding co-Editor-in-Chief of ACM Distributed Ledger Technologies: Research & Practice, and the founding Chair of IEEE TEMS Technical Committee on Blockchain and Distributed Ledger Technologies. He is an ACM Distinguished Speaker and IEEE Computer Society Distinguished Visitor (2021 - 2023), and a Web of Science's Highly Cited Researcher (Computer Science - 2021, Cross-Field - 2020). He is also the recipient of the 2019 IEEE Technical Committee on Scalable Computing Award for Excellence in Scalable Computing (Middle Career Researcher), the 2021 UTSA Carlos Alvarez College of Business Endowed 1969 Commemorative Award for Overall Faculty Excellence and the 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, the British Computer Society's 2019 Wilkes Award Runner-up, the Fulbright Scholarship in 2009, the 2008 Australia Day Achievement Medallion, and the British Computer Society's Wilkes Award in 2008. He has also received best paper awards from IEEE Systems Journal in 2021, IEEE Computer Society's Bio-Inspired Computing Special Technical Committee Outstanding Paper Award for 2021, IEEE Conference on Dependable and Secure Computing (DSC 2021), IEEE Consumer Electronics Magazine for 2020, Journal of Network and Computer Applications for 2020, EURASIP Journal on Wireless Communications and Networking in 2019, IEEE TrustCom 2018, and ESORICS 2015; the IEEE Blockchain 2019 Outstanding Paper Award; and Best Student Paper Awards from Inscrypt 2019 and ACISP 2005.