This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2022.3165324, IEEE Transactions on Dependable and Secure Computing

Inference of User Desires to Spread Disinformation Based on Social Situation Analytics and Group Effect

Junchang Jing, Zhiyong Zhang, *Senior Member, IEEE,* Kim-Kwang Raymond Choo, *Senior Member, IEEE,* Kefeng Fan, Bin Song, and Lili Zhang

Abstract—The dissemination of digital disinformation in online social networks (OSNs) has been the subject of extensive research, although many challenges remain, including the analysis and control of disinformation dissemination across different platforms (i.e. cross-platform). In this article, we investigate and analyze the spreading patterns and regularities of disinformation both within a single platform and across platforms. To explore the complex relationship between user propagation desire and behaviour within the same group, a user propagation desire inference model based on propagation characteristics (behaviour characteristics and time characteristics) and a bidirectional backpropagation (B-BP) deep neural network are constructed. Then, to avoid overfitting due to the interaction of users' propagation behaviour and the correlation among propagation characteristics, a novel adaptive weighted particle swarm optimization evolutionary algorithm is utilized to further optimize the B-BP deep neural network. We design and conduct a series of evaluation experiments on the current global hot topics including but not limited to novel coronavirus-19 pandemic (COVID-19), food safety, medical and health, and environmental protection. By using a real-world social platform and its social situation metadata analysis, the experimental results show that the proposed method not only accurately predicts the level of user propagation desire under multiple behaviour interactions but also facilitates social platform managers in handling disinformation disseminators. Our findings reveal that the intensity of social users' desires to spread disinformation is related to the topics and groups that users are interested in, while the propagation motivation of social users is not strong under topics that users are not interested in. Our studies also demonstrate that social users with propagation desires tend to utilize their familiar social platforms and local circles for communication, and the behaviour and desire to spread disinformation to the cross-platform are not strong. We posit that these findings can help inform online and, fine-grained governance and mitigation strategies other than "one size fits all" approaches (e.g., "account prohibition and deletion"), and hopefully minimize disinformation dissemination.

Index Terms—Disinformation, Social Situation, Group Effect, User Behaviour, Propagation Desire.

1 Introduction

The proliferation of false information such as false news and rumours on social media platforms (e.g., mobile social networks) has serious impacts on the global economy, society, life order and even political security [1], [2], [3], [4], [5]. For example, during the COVID-19 outbreak, a large amount of false information related to the pandemic has compounded the challenge of social users in distinguishing between legitimate and false information [6]. Taking COVID-19 as an example, postings on Twitter and Weibo in April 2020 reported that a volunteer who received a vaccine injection died in the UK. This resulted in fear and distrust for the vaccine, as well as the promotion of subsequent vaccine injection trials [7]. The extent and consequence of misinformation have prompted the U.S. Centers for Disease Control and Prevention (CDC) to dedicate efforts on vaccine recipient education campaigns (e.g., https://www.cdc.gov/vaccines/covid-19/health-departments/addressing-vaccine-misinformation.html)

False information can be categorized as misinformation or disinformation, where the latter refers to the generation and dissemination of false information while knowing that such news is fake [8], [9]. Misinformation, on the other hand, refers to the unintentional sharing of fake information without malicious intention [10]. In other words, a misinformer (i.e., a person who propagates misinformation) and a disinformer (i.e., a person who propagates disinformation) have different intentions. Misinformers usually change their opinions after being corrected, unlike disinformers [11]. Given the potentially damaging act of disinformation, we mainly focus on disinformation in this paper.

At present, the propagation of false information on OSNs includes the following three main aspects. The first aspect is based on the dynamic propagation model of infectious diseases [12], [13], [14], [15], [16], [17]. Since the spread of false information in OSNs is similar to that of a virus, researchers utilize classical epidemic models to describe the spreading process of rumours based on three states: susceptible (S), infected (I) and removed (R) [12], [13], [14]. However, these methods establish only a macroscopic math-

- *Junchang Jing, Zhiyong Zhang, Bin Song, and Lili Zhang are with the Information Engineering College, Henan University of Science and Technology and and Henan International Joint Laboratory of Cyberspace Security Applications, Luoyang, China, 471023.*
E-mail: xidianzzy@126.com
- *Kim-Kwang Raymond Choo is with the Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, USA, 78249.*
- *Kefeng Fan is with the China Electronics Standardization Institute, Beijing, China, 100007*

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2022.3165324, IEEE Transactions on Dependable and Secure Computing

ematical model and do not include an analysis of various microscopic mechanisms. With the mixed dissemination of true and false information in OSNs, researchers further consider the user's behaviour characteristics on the basis of an infectious disease dynamic propagation model to more comprehensively analyse the influence of various parameters on the propagation dynamic model and the mixed propagation regularity [15]. In addition, on the basis of an infectious disease dynamics model, some researchers study how to utilize appropriate methods to prevent the spread of false information [16], [17].

The second aspect is the dissemination of false information based on the statistical features of social networks [18], [19], [20], [21], [22], [23]. Researchers [18], [19] have utilized the Lorentz curve, Gini coefficient, edge/node ratio and other statistical properties of social networks to describe the patterns of group users spreading false information. Vosoughi et al. [20], for example, analysed a large amount of true and false information on Twitter using a statistical analysis method and found that false information spreads farther, faster, deeper and wider than true information. Analyzing and comparing two types of propagation networks including disinformation and mainstream news in France and Italy, Pierre [21] found that disinformation communication networks show stronger clustering and interconnection than mainstream news communication networks. Moreover, Pierre observed that users who share disinformation news usually have a stronger tendency to share mainstream news. In addition, Barfar [22] analyzed and compared the effects of political disinformation and real information on the cognitive and affective factors of social users. The author [22] found that users' reactions to real news were more anxious, while their reactions to political false information were more angry and rude. To study the propagation regularity of early false information, researchers, such as [23], have established true and false early propagation networks by analysing the forwarding relationship among social users and obtained different topological characteristics of the two kinds of information. The findings provide important theoretical support for the early detection and control of false information.

The third aspect concerns the propaganda mechanism of false information across platforms. False information dissemination across multiple OSN platforms refers to the flow of information among different social network platforms and can be interpreted in two ways [24], [25]. First, the same false information is propagated and integrated across different platforms, and second, the mutual cooperation, symbiosis, interaction and coordination among platforms [24]. For instance, Wang et al. [25] proposed an improved energy model to study the spread of rumours across platforms and selected the connection rate index to analyse the impact of rumour spread between different social platforms.

The related theories of group behaviour, process and dynamics have been studied in the field of social psychology [26], [27], [28]. The research on group behaviour is mainly carried out from two aspects: intergroup (members of different groups) behaviour and intragroup (members of the same group) behaviour. Intragroup assimilation and intergroup differentiation are typical characteristics of group process [29]. Four modes of coexistence of group dynamics and psychology in behaviour description include 1) conflict, 2) hierarchy, 3) niche and 4) cooperation [30]. In addition, to study group behavior from a computational perspective, Adrianna et al. [31] proposed a computational model to predict individual behavior towards members of different social groups by employing social psychology theory. Inspired by the group-based research in the realm of social psychology, scholars have begun to study the behavior, process and dynamics of groups in the process of false information dissemination in social networks recently [32], [33], [34], [35], [36], [37]. Jamieson and Cappella [32], for example, found that social users who have similar views or interests usually gather together and form a homogeneous cluster (i.e. a group of users). The homogeneous cluster greatly amplifies rumor propagation in social networks [33]. Specially, rumours spread through the homogeneous cluster members are often more viral and spread faster than those not spread through the homogeneous cluster members. Xiao et al. [34] presented a group behavior model of rumour information propagation by analyzing the rumour diffusion feature space. Sahafizadeh et al. [35] focused on the influence of group communication on the dynamic model of rumour propagation, and indicated that group propagation greatly increased the propagation speed of rumour and the scale of disseminators. In addition, by comparing the group process and dynamics for disseminating different types of information (e.g. scientific and conspiracy information), Vicario et al. [36] demonstrated that homogeneous clusters were the main driving force of information diffusion. Furthermore, they found that different homogeneous clusters differ in their cascade dynamics for each type of information. Bessi et al. [37] found that social users who are interested in conspiracy theory type information will pay more attention to conspiracy theory type posts, and these users will have a stronger forwarding desire.

In summary, false information dissemination has been widely studied, particularly in recent years. The existing research focuses mainly on the propagation model of false information and the propagation regularity of false information on the same social platform. Although these research results provide an important and valuable reference for disinformation detection and control, a number of challenges remain:

1) The need to consider dividing users into different groups according to the content of user dissemination to study the dissemination of disinformation on the basis of groups.

2) The need to design new mitigation strategies other than "one size fits all" approaches (e.g., "account prohibition and deletion").

3) The need to study cross-platform dissemination trends.

The "situation" concept was originally used in the study of natural language semantics [38]. Subsequently, Chang et al. give the definition of the situation with rich semantics from the viewpoint of computer science and present a novel and effective computational situation model [39]. The situation-theoretic model has been used to model and reason human intentions in context-aware service environments. Specially, a situation is defined as a three-tuple related to the time factor, that is, $Situ(t) = \{M, B, E\}_t$ where M denotes human internal mental contexts (human desires), B

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2022.3165324, IEEE Transactions on Dependable and Secure Computing

denotes human behavioral contexts (access pattern from a user, user's actions), and E refers to human-environmental contexts (locations with time) [39], [40]. Therefore, the situation theory not only contains external observable contexts (behaviors and environments), but also includes hidden contexts (user's desires). Recently, situation analytics, as a new human-centric software engineering computing paradigm, has been widely studied and applied [40], [41], [42], [43]. The advantage of this paradigm is that it fully consider the human situation, human desire and human intention.

On the basis of situation analytics, we further present a social situation analytics (SocialSitu) theory for the specific social network domain [44]. Moreover, the SocialSitu theory can be further utilized to analyze the relationship between social users' behaviors and desires. However, the inference of user desire has not been reported so far in the research of disinformation dissemination; thus, partially motivating this research. Combined with the disinformation dissemination scenario, we give the specific definitions of desire and SocialSitu, respectively (see Section 3 for more detail). The inference model of user propagation desire comprises both feature extraction and model construction. The selection of user propagation characteristics (behaviour characteristics and time characteristics) directly determines the accuracy of the model output. Therefore, the generalization ability of the model can be effectively improved by fully considering the interaction of multiple propagation behaviours and the correlation among propagation characteristics. The complex nonlinear relationships between propagation characteristics and propagation desire can be better handled by a neural network model. A B-BP neural network is a kind of multilayer feedforward neural network that can approximate a continuous function of any complexity with any desired precision [45]. However, to avoid the over-fitting phenomenon caused by the interaction among propagation behaviours and the correlation among propagation characteristics, the adaptive weighted particle swarm optimization (AWPSO) algorithm [46] is used to optimize the parameters of the B-BP neural network to prevent the algorithm from falling into a local minimum and improve the accuracy of the model output. The AWPSO algorithm is based on the principle of bird swarm predation and utilizes the principle of cooperation and information sharing among individuals in a group to find the global optimal solution. That the relative theory can clearly improve the accuracy of prediction results has been shown in the literature [47].

This article studies the inference method of subjective desire and malicious degree of group users to disseminate disinformation and deeply explores the behaviour patterns of cross-platform users to disseminate disinformation. We assume that the stronger the user's desire to spread disinformation, the more obvious the user's malicious degree. The specific contributions of this paper are as follows.

1) To explore the inherent relationship between users propagation desire and behaviour within a group, we build a user propagation desire inference model based on propagation characteristics (behaviour characteristics and time characteristics) and a B-BP neural network on the basis of social situation analysis theory. To improve the accuracy of the model prediction results, a AWPSO evolutionary algorithm is used to optimize the hidden parameters of the B-BP neural network. This method can fit the complex nonlinear relationship between the input user propagation characteristics and the output propagation desire and avoid over-fitting the interaction of user propagation behaviour and the correlation among propagation characteristics on the B-BP neural network.

2) On the basis of the inference model, we employ 1,455,812 Sociasitu metadata, and design and conduct a series of experiments to assess the performance of our proposed inference model. The experimental results show that our proposed inference model are quite accurate compared with other baseline methods. To our knowledge, we are the first to validate a inference method of user propagation desire in a realistic social network scenario.

3) In the process of inference disinformation dissemination desire, we obtain two important and interesting conclusions: a) the intensity of social users' desires to spread disinformation is related to the topics and groups that users are interested in, while the propagation motivation of social users is not strong under topics that are not of interest; b) social users with propagation desires tend to utilize their familiar social platforms and local circles for communication, and users with medium and strong propagation desire occupy a proportion of 68.61%. In addition, the behaviour and desire to spread disinformation to the cross-platform are not strong, and users with medium and strong propagation desire only account for 3.14%.

The rest of this article is structured as follows. Section 2 systematically outlines some previous studies related to the propagation of disinformation in OSNs, and Section 3 formalizes the research definitions. Section 4 presents a group division method of disinformation dissemination. Subsequently, a detailed inference method of user propagation desire is described in Section 5. In section 6, we experimentally evaluate approaches on a real social network. In section 7 and 8, the discussions and conclusions of this article are put forward.

2 Related works

In this section, we systematically and comprehensively summarize the results of existing disinformation dissemination in OSNs research. First, according to the types of social subjects, we analyze and discuss the disinformation dissemination of social bots and social human. Second, from the perspective of the time attribute of propagation, the spread of early disinformation has also been widely concerned by researchers. Therefore, this section mainly introduces the related research work of social bots dissemination, social human dissemination and early dissemination of false information in detail.

The dissemination of false information by social bots in OSNs is a relatively new field [48], [49], [50]. Shao et al. [48] pointed out that social bots played a key role in spreading low-credibility articles, especially after publication and before mass dissemination. Moreover, social bots pay more attention to influential users with a large number of fans. In [49], Shao et al. found that social bots are particularly active in the early stage of false news dissemination, and tend to target influential users, which makes false news widely

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2022.3165324, IEEE Transactions on Dependable and Secure Computing

shared in OSNs.

In the related research on false information dissemination of social human, Vosoughi et al. [20] studied the differences between true and false news in spreading pattern by selecting real news and false news distributed on Twitter from 2006 to 2017 as data sets. They mainly analysed and discussed the depth, scope, width and structure diffusion of false information from the perspective of network structure, the number of nodes and cascades. Furthermore, this study also pointed out several limitations of the research on combating disinformation. In [11], Cho et al. proposed an opinion model based on subjective logic by dividing social users opinions on false information into trust, distrust and uncertainty (ignorance and ambiguity), which can effectively prevent the spread of false information. Bastick [51] focused on the impact of disinformation on individual unconscious behavior, and observed that disinformation was capable of changing an individual's unconscious behavior even within a short period of time. Colliander [52] investigated the impacts of conformity on others when users posted responses or comments to disinformation. The study found that the behaviors of other individuals in the comment area of disinformation significantly affect individuals attitudes, and their intentions to propagate or comment on the disinformation. Liang et al. [53] proposed a rumour detection method based on social users behaviour characteristics. Meanwhile, they found out that the behaviour of rumour publishers and disseminators is different from that of true information disseminators, and rumour generate more responses than true information in the process of spreading, for example, followers comments and forwarding. In [15], Wen et al. proposed a hybrid information (positive and negative information) dissemination dynamic model, which not only considers the characteristics of propagation dynamics, but also considers the behaviour of people making choices when they receive the two kinds of information. Their research results show that spreading positive information to suppress negative information is an effective way to prevent the spread of false information. Yaqub et al. [54] investigated the influence of four types of credibility indicators which include Fact Checkers, News Media, Public, Artificial Intelligence on users' intention to share false information.

The differences between false and true information at early stages of propagation have also been studied by many scholars. Zhao et al [23] established the propagation network of real and false information by analyzing the information forwarding relationship among users, and concluded that there were obvious differences between the topological characteristics of false and true news in the early propagation process. In [55], Liu et al. proposed an early detection model of false information by classifying the information propagation paths of social users.

3 Related definitions

Definition 1: Desire: This represents what social users want to obtain when using a social network service, namely, the user's motivation [44]. It is composed of a series of atom desires (d), namely, $\{d_1, d_2, \cdots, d_n\}$, where d_i denotes the user's atom-desire at i. For instance, when social users want to propagate disinformation that they are interested in, the desire may be defined as the intensity level of users spreading disinformation. The user's atom-desire can be divided into three levels: high, middle and low.

Definition 2: SocialSitu(t): $Socialsitu(t) = \{obj, ID, d, A, E, T\}_t$. On the basis of the social situation analysis theory proposed in [44], we further combine the social scene of disinformation dissemination and add the social object and social target tuple, thus expanding the original four tuples to six tuples. Here, obj refers to social objects, such as disinformation and real information; ID refers to the social user's identity information, which includes the user's group and role; d refers to the social user's atom-desire at t; A refers to the social user's behaviour corresponding to d at the moment; E refers to environmental information, including the terminal information that the user utilized; and T refers to the target of audience entities. For example, the audience entities of disinformation dissemination include individuals, groups, local open platforms, and third-party open platforms (cross platforms) in OSNs.

Definition 3: The disinformation subset, which refers to the collection of disinformation under the same topic, is defined as follows:

$$\begin{cases} f_{ij} \in topic_i \\ i \in [1, K], j \in [1, n] \\ p_{topic} = U_{topic_i}(u_1, u_2, \cdots, u_j) \end{cases} \tag{1}$$

Here, $topic_i$ refers to the ith topic, f_{ij} refers to the jth information that belongs to $topic_i$. p_{topic_i} represents the collection of all propagators corresponding to the ith topic.

Definition 4: The user history behaviour of spreading disinformation is defined as $B = \{(a_i, b_i, c_i, u_i, \Delta t) | u_i \in U, \Delta t \in \phi\}$. By definition, B represents a collection of behaviours when user u_i interacts with disinformation on a social platform during a period of time Δt . a_i, b_i and c_i are the numbers of forwards, likes and comments for disinformation of user u_i during Δt, respectively.

Definition 5: Formal representation of social user groups. In the process of group partitioning, user groups are formalized as $G_U^{k_i} = \{(U, k_i) | U = \{u_1, u_2, \cdots, u_n\}, k_i \in K\}$. Here, $G_U^{k_i}$ refers to the collection of all users of propagation topic k_i on a single platform platform, U represents the collection of users in the same group, and k_i refers to the ith topic in topic set K.

4 Group division of disinformation dissemination

The dissemination of disinformation in OSNs is a form of social behaviour activity of users. Disinformation is usually generated and spread in the form of various topics. Meanwhile, different topics have different effects on social users. The propagation behaviour of social users is affected by their interest in the content and the relationships among users' friends. Therefore, users from the same group tend to follow suit and herd when they are interested in disinformation topics, which results in a series of similar social activity among users. For instance, most people only forward information that they are interested in or approve of.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2022.3165324, IEEE Transactions on Dependable and Secure Computing

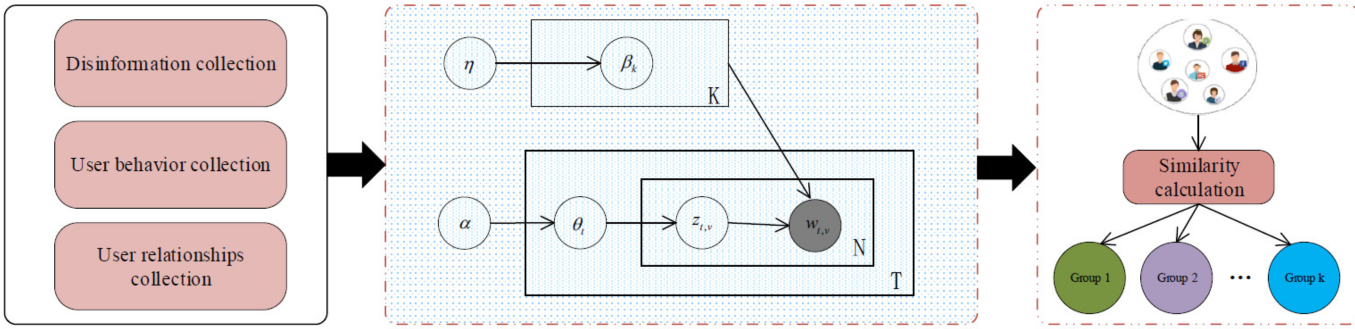


Fig. 1. Flow chart of social user groups division. The flow chart is divided into three phases. The first stage is social network attribute collection, which includes disinformation collection, user behaviour collection and user relationship collection. The second stage is social user topics distribution modelling. The meaning of each symbol is described in detail in this section. The dynamic social user groups distribution is described in stage 3. Each group represents a collection of users who propagate information about a particular topic.

According to the content of the user's historical dissemination of disinformation, we utilize the LDA model [56] to obtain the topic distribution of users spreading disinformation. Thus, users are divided into different groups based on the content and regularity of spreading disinformation under different topics. The formal definition of the user group is presented in definition 5. In each group, a user is either a publisher or forwarder of disinformation. Furthermore, the three stages of social user group division are shown in Fig.1. The first stage is social network attribute collection, the second stage is social user topic distribution modelling, and the third stage is dynamic social user group distribution.

Specifically, LDA is a probabilistic model based on a text set, which is a three-layer Bayesian probabilistic topic model composed of text-topic-word. For a given text set, the model can be used for topic analysis to learn the topic distribution of each text and the word distribution of each topic. First, we integrate the historical content of each social users disinformation spreading into the same text and utilize the Chinese word segmentation technology Jieba to extract stemming and stop listing. According to the social users and the disinformation text set, the disinformation set is divided into K topics and T disinformation texts. The words in the text come from a dictionary containing V words. We utilize T vectors with V dimensions to represent the text set and K vectors (k=1, 2, $\cdots$, K) with V dimensions to represent the topic, where represents the word frequency of word v in text t, represents the word frequency of word v in topic k, and represents the topic of word v in text t. Second, we obtain the hidden parameters using a fast collapsed Gibbs sampling method [57], which can be estimated as follows:

$$\theta_{u_i,k} = \frac{n_{u_i k} + \alpha_k}{\sum_{k=1}^{K}(n_{u_i k} + \alpha_k)} \tag{2}$$

$$\beta_{k,\nu} = \frac{n_{u_i \nu} + \eta_\nu}{\sum_{\nu=1}^{V}(n_{u_i \nu} + \eta_\nu)} \tag{3}$$

where $n_{u_i k}$ and $n_{u_i \nu}$ refer to the numbers of topics and words in the text corresponding to user u_i, respectively, and α_k and η_ν are the Dirichlet prior knowledge. Finally, according to the topic distribution of disinformation propagated by all social users, the content similarity score between the keywords set corresponding to the topic distribution of disinformation propagated by each user and the keywords set corresponding to K topics is calculated by using the cosine similarity formula (4).

$$\begin{aligned} Sim(u_i, Topic_k) &= \frac{\mathbf{V}_i \cdot \mathbf{V}_k}{\|\mathbf{V}_i\| \|\mathbf{V}_k\|} \\ &= \frac{\sum_{m=1}^{M} V_{im} \times V_{km}}{\sqrt{\sum_{m=1}^{M}(V_{im})^2} \times \sqrt{\sum_{m=1}^{M}(V_{km})^2}} \end{aligned} \tag{4}$$

where $\mathbf{V}_i$ and $\mathbf{V}_k$ represent the M dimensional vectors corresponding to u_i and $topic_k$ obtained by using Doc2vec algorithm [58], respectively. The user group partition algorithm is shown in Algorithm 1.

Algorithm 1 User group partition algorithm

Input: User collections U, Disinformation collections T, Number of topics K, Number of words V, Prior knowledge parameters α, η;
Output: Group collections G={Group(1),$\cdots$,Group(i),$\cdots$,Group(p)};

```
Begin
for each u_i ∈ U and i ← 1 to |U| do
    for each topic k ∈ K and k ← 1 to |K| do
        Generate β_{u_i k} ∼ Dir(η), θ_{u_i k} ∼ Dir(α) // Generate the word distribution of topic and topic distribution of text for each user
    end for
    for each word w_ν and ν ← 1 to |V| do
        Generate z_{u_i ν} ∼ Mult(θ_{u_i}), w_{u_i ν} ∼ Mult(φ_{z_{u_i ν}}) // Generate the sequence of words corresponding to text for each user
    end for
end for
Calculate the topic distribution similarity score between user u_i and topic_k according to (4)
Determine the user group collections under different topics according to the similarity score
End
```

5 Construction of a Propagation Desire Inference Model

5.1 Feature extraction and description

In the process of disinformation dissemination, different users may have different propagation behaviour patterns and time characteristics. This section introduces the behaviour characteristics and time characteristics of disinformation spreading in detail. Social user behaviour characteristics are composed of the user's attention, activity,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2022.3165324, IEEE Transactions on Dependable and Secure Computing

propagation influence and transfer probability. The time characteristics of users consist of the average time interval and time interval entropy.

5.1.1 The definition and description of behaviour characteristics

a) The attention of users spreading disinformation: User attention, an important indicator of users' propagation desire, can measure the degree of interaction between users and disinformation as a whole. Meanwhile, user attention accurately portrays the individual performance in OSNs. Here, we investigate three manifestations of user attention in OSNs: retweets, likes and comments. Moreover, we utilize the number of individual behaviours in a certain period of time to represent user attention. The definition of user attention is as follows:

$$Attention(u_i) = \frac{ln(M_{u_i}^{(RT)} + M_{u_i}^{(like)} + M_{u_i}^{(RV)})}{\Delta t \times \frac{1}{N}\sum_{i=1}^{N} ln(M_{u_i}^{(RT)} + M_{u_i}^{(like)} + M_{u_i}^{(RV)})} \tag{5}$$

where $M_{u_i}^{(RT)}$, $M_{u_i}^{(like)}$ and $M_{u_i}^{(RV)}$ are the numbers of retweets, likes and reviews by u_i in time interval Δt, respectively. N indicates the total number of users. Moreover, $\frac{1}{N}\sum_{i=1}^{N} ln(M_{u_i}^{(RT)} + M_{u_i}^{(like)} + M_{u_i}^{(RV)})$ denotes the average number of behaviours for all users.

b) The activity of users spreading disinformation: The quantity of disinformation forwarded by users in a specific time interval can accurately reflect the activity of users. In the course of spreading, forwarding is a common form of interaction and communication among users. Therefore, disinformation sharing is inferred based on the quantity and time of forwarding activity. In general, disinformation spreading is positively correlated with the intensity of users' desire. User activity can be defined as follows:

$$Activity(u_i) = \frac{n_{repost2}^{u_i}}{n_{repost1}^{u_i}}, when \;\; t_1 < t < t_2 \tag{6}$$

where $n_{repost1}^{u_i}$ and $n_{repost2}^{u_i}$ indicate the total number of pieces of information and disinformation forwarded by user u_i during period $[t_1, t_2]$, respectively.

c) The influence of users spreading disinformation: The influence of users participating in spreading disinformation is closely related to their activity and number of friends on the social network platform. Therefore, we take user activity as the base of user propagation influence and the number of friends as the coverage index. The influence of users is expressed as

$$Influence(u_i) = (f_{rr})^{lg|N^{out}(u_i)|+1} \tag{7}$$

where $f_{rr} = n_{repost2}^{u_i}/(|t_1 - t_2|)$ and $N^{out}(u_i)$ represents the number of friends of user u_i.

d) The transfer probability of users spreading disinformation: The audience entities of social users who spread disinformation include individuals, groups, local open platforms and cross platforms in the OSNs environment. These audience entities have a direct relationship with the scope of propagation. Therefore, we infer the scope of users' dissemination of information through the audience entity type. To describe the intensity of users' desire from the scope of disinformation spreading, we define the transition probability of users' spreading information as follows:

$$Transition\ probability(i,j) = \frac{\sum_k \{X(t+1) = j, X(t) = i\}}{\sum_k X(t) = i}, \quad k \in N \tag{8}$$

where $\sum_k X(t) = i$ indicates the total number of transitions that occur in behaviour status i among audience entities. $\sum_k \{X(t+1) = j, X(t) = i\}$ refers to the total number of audience entities for audience entity i at t and audience entity j at t+1. The above definition captures the transition probability of different types of audience entities corresponding to users.

Algorithm 2 Parameter optimization algorithm

Input: Weights and thresholds of the B-BP neural network
Output: Personal best position $\mathbf{p}$, Global best position $\mathbf{p}_g$

Begin
Initialize parameters d, w_1, w_2, k_{max}, n // initialization and construction
Randomly generate particle position $\mathbf{x}_i^{(1)}$ and its corresponding velocity $\mathbf{v}_i^{(1)}$ $(i = 1, 2, \cdots, d)$ // d refers to the number of the initial weights and thresholds of the B-BP neural network
$\mathbf{p}_i^{(1)} = \mathbf{x}_i^{(1)}$, $\mathbf{p}_g^{(1)} = \arg\min_{\mathbf{x} \in \{\mathbf{x}_1^{(1)}, \cdots, \mathbf{x}_d^{(1)}\}} f(\mathbf{x})$ // $f(\mathbf{x})$ refers to the fitness function and $\mathbf{x}$ represents the weights and thresholds
for k = 1 : k_{max} **do**
  for i = 1 : d **do**
    $w = w_1 - (w_1 - w_2) \times k/k_{max}$
    $\mathbf{v}_i^{(k+1)} = w\mathbf{v}_i^{(k)} + F(\mathbf{p}_i^{(k)} - \mathbf{x}_i^{(k)})\mathbf{r}_1(\mathbf{p}_i^{(k)} - \mathbf{x}_i^{(k)}) + F(\mathbf{p}_g^{(k)} - \mathbf{x}_i^{(k)})\mathbf{r}_2(\mathbf{p}_g^{(k)} - \mathbf{x}_i^{(k)})$ // The elements of n-dimensional vectors $\mathbf{r}_1$ and $\mathbf{r}_2$ are random numbers in the interval [0,1]
    $\mathbf{x}_i^{(k+1)} = \mathbf{x}_i^{(k)} + \mathbf{v}_i^{(k+1)}$
    if $f(\mathbf{x}_i^{(k+1)}) < f(\mathbf{p}_i^{(k)})$ **then**
      $\mathbf{p}_i^{(k+1)} = \mathbf{x}_i^{(k+1)}$
    else
      $\mathbf{p}_i^{(k+1)} = \mathbf{p}_i^{(k)}$
    end if
    $i = i + 1$
  end for
  if $\exists\, i \in \{1, 2, \cdots, d\}$ and $f(\mathbf{x}_i^{(k+1)}) < f(\mathbf{p}_g^{(k)})$ **then**
    $\mathbf{p}_g^{(k+1)} = \mathbf{x}_{i^*}^{(k+1)}$ $//i^* = \arg\min_i f(\mathbf{x}_i^{(k+1)})$
  else
    $\mathbf{p}_g^{(k+1)} = \mathbf{p}_g^{(k)}$
  end if
  $k = k + 1$
end for
End

5.1.2 The definition and description of time characteristics

a) The average time interval of users spreading disinformation: Propagators often selectively spread disinformation in a short time. The average time interval of disinformation dissemination is determined by the time that the information is published and the time spent by disseminators to disseminate the information. The time interval is inversely proportional to the intensity of the users' desire. Therefore, we define the time interval of user propagation as follows:

$$Time\ interval(u_i) = \frac{1}{|FN^{u_i}|}\sum_{k=1}^{N}(t_1^{(k)} - t_0^{(k)}) \tag{9}$$

where $|FN^{u_i}|$ refers to the amount of disinformation forwarded by user u_i and $t_1^{(k)}$ and $t_0^{(k)}$ indicate the time when

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2022.3165324, IEEE Transactions on Dependable and Secure Computing

user u_i propagates the kth piece of information and the corresponding release time, respectively.

b) The time interval entropy of users spreading disinformation: Time interval entropy can accurately reflect the temporal distribution of users' propagation behaviour. According to the time interval of information dissemination, we use the definition of information entropy to measure the regularity of information dissemination. The time interval entropy of user u_i spreading disinformation is defined as follows:

$$H_{\Delta t}(u_i) = -\sum_{i=1}^{n_T} p_{\Delta T}(\Delta t_i) log(p_{\Delta T}(\Delta t_i)) \tag{10}$$

where $p_{\Delta T}(\Delta t_i) = n_{\Delta t_i}/(\sum_{k=1}^{n} n_{\Delta t_k})$.

For convenience, the above-mentioned user behaviour features and time features are unified into a term F_{ik} referring to the kth feature of the ith user u_i: F_{i1}=Attention (u_i), F_{i2}=Activity (u_i), F_{i3}=Influence (u_i), F_{i4}=Transition probability (i, j), F_{i5}=Time interval (u_i) and F_{i6}=Time interval entropy (u_i).

5.2 Model construction

The desires of social users who spread disinformation reflect the internal change trends of users in the process of dissemination and lay the foundation for the control of disinformation dissemination. A corresponding relationship exists between user desires and dissemination behaviour. Therefore, based on the division of social user groups, we infer the desire behind the propagation behaviour of users in the same group.

In the process of spreading disinformation, propagators may be affected by their political views or economic interests, which leads to different levels of desire under different topics. Therefore, due to the complexity and variability of user propagation desire, the traditional linear classification model shows poor generalization ability in the process of desire inference. As a classic neural network learning algorithm, the B-BP neural network model has good nonlinear mapping ability and is suitable for classifying the propagation desire intensity level.

The neural network learning process dynamically adjusts the connection weights between neurons and the corresponding threshold of each functional neuron according to the training data. The training process can be seen as a form of parameter optimization. That is, in the parameter space, the optimal parameters to minimize the corresponding training error are determined. Due to the interaction of user propagation behaviour and the correlation between propagation characteristics, the B-BP neural network is prone to falling into local minima and has weak global search ability in parameter optimization. However, the PSO algorithm has global properties and can improve the prediction accuracy of neural networks [59], [60], [61]. Therefore, we introduce a novel adaptive weighted PSO algorithm to optimize the weight and threshold of the neural network such that the trained neural network can better approach the global minimum. The parameter optimization algorithm is shown in Algorithm 2.

The training process of B-BP model can be regarded as minimizing both the forward propagation error E_1 and backward propagation error E_2. Specially, the forward propagation error E_1 can be expressed as

$$E_1 = \frac{1}{2}\sum_{m=1}^{M}(y_m - a_m^y)^2 \tag{11}$$

where y_m and a_m^y represent the real value and activation value of the m-th neuron in the model output layer, respectively. The backward propagation error E_2 can be expressed as

$$E_2 = \frac{1}{2}\sum_{v=1}^{V}(x_v - a_v^x)^2 \tag{12}$$

where x_v and a_v^x refer to the real value and activation value of the v-th neuron in the model input layer, respectively. For a given learning rate parameter ω, the update rules of forward training are as follows:

$$u_{jm}^{(t+1)} = u_{jm}^{(t)} - \omega(a_m^y - y_m)a_j^h \tag{13}$$

$$w_{vj}^{(t+1)} = w_{vj}^{(t)} - \omega(\sum_{m=1}^{M}(a_m^y - y_m)u_{jm}a_j^{h'}x_v) \tag{14}$$

$$b_j^{h(t+1)} = b_j^{h(t)} - \omega(\sum_{m=1}^{M}(a_m^y - y_m)u_{jm}a_j^{h'}) \tag{15}$$

$$b_m^{y(t+1)} = b_m^{y(t)} - \omega(a_m^y - y_m) \tag{16}$$

The update rules for backward training are as follows:

$$u_{jm}^{(t+1)} = u_{jm}^{(t)} - \omega(\sum_{v=1}^{V}(a_v^{xb} - x_v)w_{vj}a_j^{hb'}y_k) \tag{17}$$

Algorithm 3 Propagation desire inference algorithm

Input: The social user groups $G = \{Group(1), Group(2), \cdots, Group(p)\}$
The social user history behaviours $B = \{(a_i, b_i, c_i, u_i, \Delta t)|u_i \in U, \Delta t \in \phi\}$,
The collection of social user behaviour characteristics and time characteristics $F = \{F_{i1}, F_{i2}, \cdots, F_{i6}\}$
The social user tags $L = \{(d_j, u_i)|u_i \in U)\}$
Output: The prediction matrix of desire inference $Y^* = \arg\max_i P_i(Y_i|G, B, F, L)$

Begin
Initialize learning rate parameter ω
for $g_j \in$ G and $j \leftarrow 1$ to p **do**
  repeat
    for *all training data* **do**
      Phase 1: forward training
      Calculate the forward propagation error E_1 according to formula (11)
      Update connection weights u_{jm} and w_{vj} according to (13)-(14)
      Update biases b_j^h and b_m^y of hidden layer and output layer neurons according to (15)-(16)
      Phase 2: backward training
      Calculate the forward propagation error E_2 according to formula (12)
      Update connection weights u_{jm} and w_{vj} according to (17)-(18)
      Update biases b_v^x and b_j^h of hidden layer and output layer neurons according to (19)-(20)
    end for
  until converge
  for *all testing data* **do**
    predict $Y^* = \arg\max_i P_i(Y_i|G, B, F, L)$
  end for
end for
End

$$w_{vj}^{(t+1)} = w_{vj}^{(t)} - \omega(a_v^{xb} - x_v)a_j^{hb} \tag{18}$$

$$b_v^{x(t+1)} = b_v^{x(t)} - \omega(a_v^{xb} - x_v) \tag{19}$$

$$b_j^{h(t+1)} = b_j^{h(t)} - \omega(\sum_{v=1}^{V}(a_v^{xb} - x_v)w_{vj}a_j^{hb'}) \tag{20}$$

The updating rules are repeated until the training error of the model reaches a sufficiently small value. Moreover, to optimize the weights and thresholds of the neural network, a multilayer deep neural network based on the AWPSO algorithm is constructed. The test samples are then input into the above model, and the propagation desire intensity matrix of users is obtained. The specific process is shown in algorithm 3.

6 Experiments

6.1 Experimental Dataset

In this section, we mainly show the experimental dataset from the following three aspects. 1) We briefly introduce the Shareteches platform. 2) We provide the process of dataset collection and division criteria of disinformation topic. 3) We present the ethical process and approvals in detail.

1) Brief introduction of Shareteches platform: We select the online social network platform Shareteches (formerly CyVOD) [62] (http://www.shareteches.com) as the experimental platform that comprises website platform and mobile applications (Android and iOS). Shareteches is an online technology community with social functions, which can provide users with real-time communication, discussion and services. Users can exchange and share technology topics and nearby technology information anytime and anywhere by utilizing Shareteches APPs. The platform frame integrates multiple functions such as multimedia content management [63], copyright protection, security assessment [64] and malicious social bot detection [65], and so forth.

2) Dataset collection and description: On Shareteches, the propagation behaviour of users is acquired by a data burying point, and the Sociasitu metadata are collected on the server side. We collect 1,455,812 Sociasitu metadata from the beginning of social users' first appearance on Shareteches until December 20, 2021. Moreover, these metadata record every complete session of social users using Shareteches in real-time. On the basis of Sociasitu metadata, we build a complete dataset that can be used for disinformation dissemination research. The disinformation in the dataset has been verified from five reputable fact-checking organizations in China, including China Internet joint rumour-refuting platform (piyao.org.cn), science rumour-refuting platform (piyao.kepuchina.cn), jiaozhen rumour-refuting platform (news.qq.com), toutiao rumour-refuting platform (toutiao.com), and sina rumour-refuting platform (piyao.sina.cn). Among them, the China Internet joint rumour refutation platform integrates the rumour refutation data resources provided by more than 40 rumor refutation platforms in China's provinces. These rumour-refuting platforms identify and verify rumours, and provide authoritative rumour refutation information of relevant departments and experts. Furthermore, these organizations can also fully present and parse the content (title, body), veracity (true, false, or mixed), description of evidence and official certification authority of each disinformation.

The disinformation dataset contains 5,175 disinformation propagated by 22,086 users, of which each disinformation includes Sociasitu metadata information, text content (pictures), number of forwards, number of comments, number of likes and all comment texts. Moreover, the personal profiles of disinformation publishers/spreaders are also included in this dataset. Given that both kinds of information (disinformation and misinformation) pose a threat to effective communication in practice [10] and the malicious intent of disinformation is difficult to distinguish from the true description of a controversial point of view [51], this dataset does not check between disinformation and misinformation. Table 1 gives the detailed statistics of the disinformation dataset. Since Socialsitu metadata can record the complete session of users accessing disinformation, this statistic is much larger than other statistics.

TABLE 1
Statistics of the experimental dataset

Statistic	Total amount
# of Socialsitu metadata	1,455,812
# of Socialsitu six-tuple metadata	579,698
# of true information	17,948
# of disinformation	9,105
# of users	25,974
# of forwards	18,737
# of likes	21,446
# of comments	6,866

The division criteria of disinformation corresponding to four topics (COVID-19, food safety, medical care and health, and environmental protection) in the dataset can be expressed as follows. First, we employ the LDA topic model to obtain the keyword sets corresponding to four topics. The distributions of keyword sets vary among four topics. Then, the term frequency-inverse document frequency (TF-IDF) values of the keywords corresponding to each disinformation are calculated by applying the TF-IDF algorithm [66], and these keywords are ranked in descending order according to the TF-IDF values. At last, the content similarity score between the top-50 keywords set corresponding to each disinformation and the top-50 keywords set corresponding to each topic is calculated by employing cosine similarity from formula (21).

$$\begin{aligned} Sim(Topic_i, disinformation_j) &= \frac{\tilde{\mathbf{V}}_i \cdot \tilde{\mathbf{V}}_j}{\|\tilde{\mathbf{V}}_i\|\|\tilde{\mathbf{V}}_j\|} \\ &= \frac{\sum_{k=1}^{n} \tilde{V}_{ik} \times \tilde{V}_{jk}}{\sqrt{\sum_{k=1}^{n}(\tilde{V}_{ik})^2} \times \sqrt{\sum_{k=1}^{n}(\tilde{V}_{jk})^2}} \end{aligned} \tag{21}$$

In the above, where $\tilde{\mathbf{V}}_i$ and $\tilde{\mathbf{V}}_j$ represent the n dimensional vectors corresponding to $topic_i$ and $disinformation_j$ obtained by using Doc2vec algorithm, respectively. The intensity level of users' propagation desire is usually related to the propagation theme (group). Therefore, to infer the strength of group users' propagation desire, it is necessary to label the strength of all users' propagation desire in each group. The annotation results are divided into C_{high}, C_{middle} and C_{low}, which correspond to strong, medium and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2022.3165324, IEEE Transactions on Dependable and Secure Computing

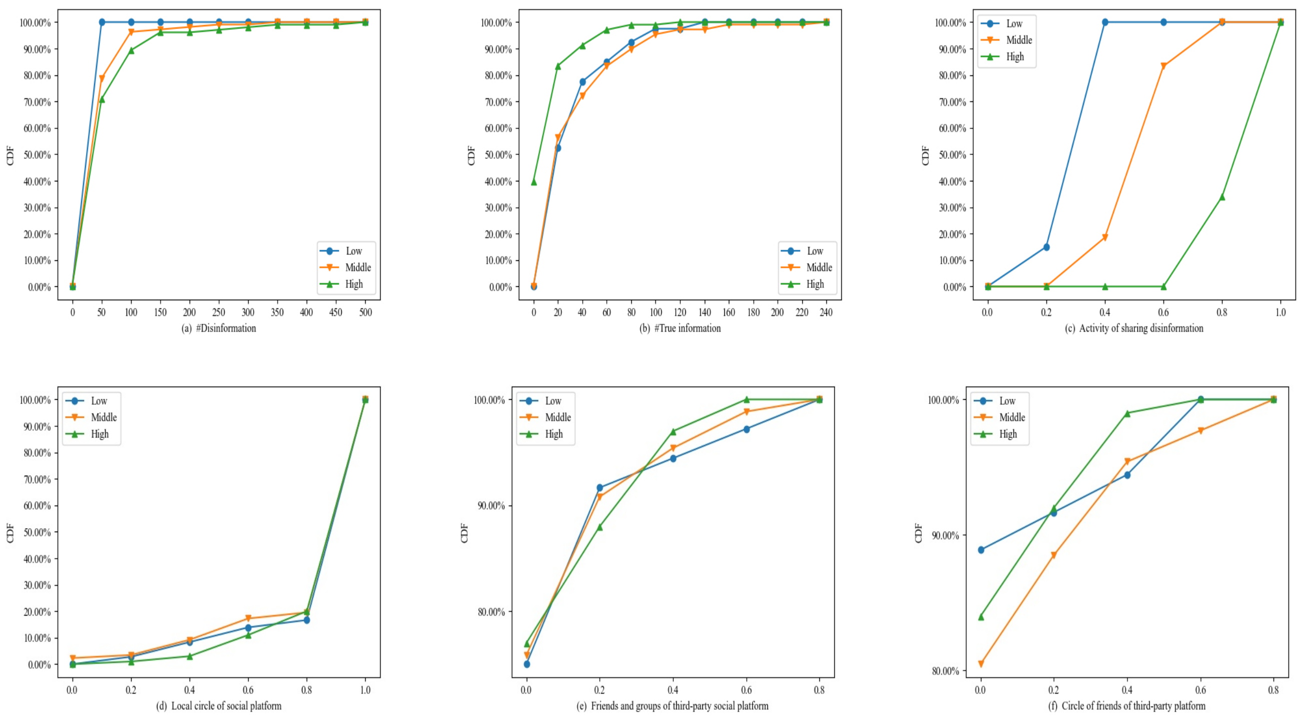
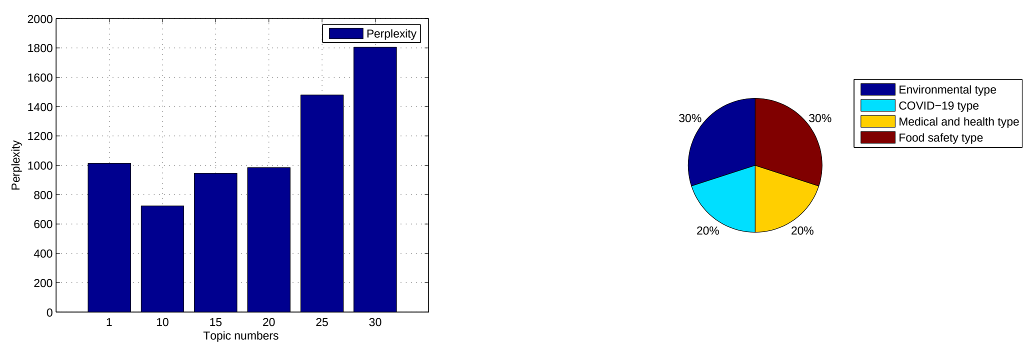


Fig. 2. Cumulative distribution function curve of factors influencing users' desires to spread disinformation. This analysis is based on the Shareteches social platform, and the third-party social platform refers to WeChat, QQ, LinkedIn and Weibo. Cumulative distribution of each factor influencing user propagation desires at three different levels: high (green triangles), middle (orange triangles) and low (blue circles). The hierarchical distributions of spreading desire from (a) the quantity of disinformation, (b) the quantity of true information, (c) the activity of sharing disinformation, (d) the local circle of the social platform, (e) the friends and groups of a third-party social platform and (f) the circle of friends of a third-party platform are quite different.



(a) (b)

Fig. 3. The distribution of topic numbers and types. (a) The distribution between the number of different topics and perplexity. The horizontal and vertical coordinates denote the topic numbers and perplexity indicators, respectively. When the number of topics is 10, the perplexity is the smallest. Therefore, we choose the number of topics k = 10; (b) The distribution of the four topics. Food safety and environment type account for 30%, while COVID-19 and medical and health account for 20%.

weak grades, respectively.

3) Ethical considerations: In the process of collecting individuals' information, we strictly abide by the privacy terms and policies of Shareteches user agreement. These privacy terms and policies have been reviewed and approved by China's network security regulatory authorities. Moreover, these user privacy terms and policies comply with the network security law of the people's Republic of China, the data security law of the people's Republic of China, the consumer rights and interests protection law, the provisions on the protection of personal information of Telecom and Internet users, the personal information protection law of the people's Republic of China and other relevant legal requirements. We respect and protect the personal privacy of all users using the Shareteches service. In other words, we only collect and use publicly available user metadata anonymously. Note that user metadata with privacy restrictions is beyond the scope of our collection and use.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2022.3165324, IEEE Transactions on Dependable and Secure Computing

TABLE 2
Statistical results for desire inference over Group A

Group A	LR	BPNN	SVM-TS	FNED	XGBoost	PCA+RF	AWPSO+B-BPNN
Attributes	8	8	8	8	8	8	8
Correctly classified instances	0.6889	0.7727	0.7046	0.7692	0.8148	0.7037	0.8392
Incorrectly classified instances	0.3111	0.2273	0.2954	0.2308	0.1851	0.2963	0.1608
Kappa statistic	0.5302	0.6210	0.4743	0.5903	0.7013	0.5731	0.7521
Mean absolute error	0.3333	0.2500	0.3409	0.2307	0.1852	0.3518	0.1607
Root mean squared error	0.6146	0.5436	0.6571	0.4803	0.4303	0.6804	0.4009

TABLE 3
Statistical results for desire inference over Group B

Group B	LR	BPNN	SVM-TS	FNED	XGBoost	PCA+RF	AWPSO+B-BPNN
Attributes	8	8	8	8	8	8	8
Correctly classified instances	0.6037	0.7346	0.6590	0.7111	0.8182	0.6364	0.8637
Incorrectly classified instances	0.3963	0.2654	0.3410	0.2889	0.1818	0.3636	0.1363
Kappa statistic	0.4533	0.5514	0.4545	0.5038	0.7143	0.3623	0.7664
Mean absolute error	0.3962	0.2653	0.4318	0.2888	0.1819	0.4090	0.1364
Root mean squared error	0.6295	0.5150	0.7833	0.5375	0.4264	0.7071	0.3692

TABLE 4
Statistical results for desire inference over Group C

Group C	LR	BPNN	SVM-TS	FNED	XGBoost	PCA+RF	AWPSO+B-BPNN
Attributes	8	8	8	8	8	8	8
Correctly classified instances	0.6842	0.7273	0.6667	0.7500	0.7333	0.7000	0.8333
Incorrectly classified instances	0.3158	0.2727	0.3333	0.2500	0.2667	0.3000	0.1667
Kappa statistic	0.4950	0.4803	0.2623	0.5556	0.4737	0.4340	0.6565
Mean absolute error	0.4474	0.3182	0.4667	0.3330	0.3333	0.4000	0.1666
Root mean squared error	0.8429	0.6396	0.7746	0.7071	0.6831	0.7746	0.4082

TABLE 5
Statistical results for desire inference over Group D

Group D	LR	BPNN	SVM-TS	FNED	XGBoost	PCA+RF	AWPSO+B-BPNN
Attributes	8	8	8	8	8	8	8
Correctly classified instances	0.5000	0.6428	0.5263	0.6923	0.5833	0.6667	0.7142
Incorrectly classified instances	0.5000	0.3572	0.4737	0.3077	0.4167	0.2623	0.2858
Kappa statistic	0.2437	0.4815	0.2830	0.4851	0.3878	0.5151	0.5385
Mean absolute error	0.5455	0.3571	0.4211	0.3076	0.5000	0.4167	0.2857
Root mean squared error	0.7977	0.5976	0.6488	0.5547	0.8165	0.7637	0.5345

6.2 Analysis and discovery of spreading patterns

To analyse the factors that affect the intensity of users' propagation desire, we examine the quantity of disinformation and true information, the activity of users spreading disinformation, and the types of audience entities that users share disinformation. In this experiment, the audience entity types include local circles of social platforms, friends and groups of third-party social platforms (WeChat, QQ, LinkedIn, Weibo, etc.), and circles of friends of third-party platforms. We plot the cumulative distribution function (CDF) curves of the relevant factors that affect the intensity of users' propagation desire, as shown in Fig.2. In Fig.2(a), when the number of users spreading disinformation is less than 50, the proportion of users with a strong propagation desire is much close to that of users with medium propagation desires. However, when the number of users spreading disinformation is more than 50, the proportion of users with strong propagation desire is more than that of users with medium and weak propagation desire. Fig.2(b) shows that 40% of the users spread no real information, which indicates that some users with strong propagation desire only spread disinformation in the social platform for specific malicious purposes. The sharing activity of users with strong propagation desire is significantly higher than that of users with medium and weak propagation desire, as shown in Fig.2(c). In Fig.2(d), with respect to the factor local circle of social platform, there is not much difference among the types of audience entities. Moreover, in Fig.2(e), when the entity type of the sharing audience is third-party platform friends and groups, the number of users with medium intensity propagation desire is always between those of the users with strong and weak propagation desire. Finally, as shown in Fig.2(d), 2(e), and 2(f), social users with propagation desires tend to utilize their familiar social platforms and local circles for communication, and users with medium and strong propagation desire occupy a proportion of 68.61%. In addition, the behaviour and desire to spread disinformation to the cross-platform are not strong, and users with medium and strong propagation desire only account for 3.14%.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2022.3165324, IEEE Transactions on Dependable and Secure Computing

6.3 Inference results and analysis

In this section, we mainly show the experimental results from the following two aspects. 1) We describe and analyze the result of user groups division according to the disinformation topics spread by social users. 2) We design a comparative experiment by using some baseline methods to further test the performance of our method.

1) Social user groups division results: The division of user groups depends on the disinformation topics spread by social users. It is difficult for LDA to determine the appropriate number of topics in a sample. Moreover, in the process of calculating the topic distribution, the selection of topic number directly affects the generalization ability of the LDA model. We apply perplexity as the evaluation index to judge the generalization ability of the model [56]. Generally, the lower the perplexity of a model is, the better the generalization ability. Figure 3(a) shows the relationship between the number of topics and perplexity: the perplexity is the lowest when the number of topics is 10. Therefore, we choose the number of topics k = 10. The initial hyperparameters in the model iteration are α =50/K and β =0.01, and the number of iterations of Gibbs sampling is 5000. Finally, the potential topic distribution and the probability distribution of the corresponding words are calculated. From the perspective of topic distribution content, we find similarities in some topics. For example, the disinformation of vaccine injection events and COVID-19 event outbreaks in Qingdao, China, are topics related to COVID-19. Therefore, all disinformation related to COVID-19 is classified as the COVID-19 topic type. Through further integration, we divided all the topics spread by users on the social platform Shareteches (formerly CyVOD) into the following four types: COVID-19, food safety, medical care and health, and environmental protection. Figure 3(b) shows the proportion distribution of 10 topics output by the LDA model under the above four categories. The food safety and environment types account for 30%. Meanwhile, COVID-19 and medical and health account for 20%.

On the basis of topics division, we further employ the cosine similarity formula (21) to calculate the content similarity score between the top-50 keywords set corresponding to each user's topic distribution of spreading disinformation and the top-50 keywords set corresponding to the above four topics. Note that we utilize a threshold of the similarity score 0.95 to classify the four types of topics. Finally, we regard the groups composed of users who propagate the above four types of information as group A, group B, group C and group D. On the basis of group division, combined with the intensity of users' desires to spread disinformation, we can conclude that the intensity of social users desires to spread disinformation is related to the topics and groups that users are interested in, while the propagation motivation of social users is not strong under non-concerned topics.

2) Inference results and performance analysis: The inference of user desires to spread disinformation can be considered as a multi-class classification problem. As some baseline approaches for the comparisons in this experiment, we used the following several representative methods.

BPNN: BPNN is a classical neural network model, which has good nonlinear mapping ability. The model can be applied to solve the classification problem of user propagation desire intensity level through an activation function.

XGBoost: XGBoost is an advanced supervised learning model for identifying fake news in social media [67]. We take the propagation characteristics as the model input, and obtain the prediction results of the user's propagation desire intensity level.

SVM-TS: The SVM-TS presented by Ma et al [68] is a classification algorithm based on dynamic sequence time structure. The algorithm employs the time characteristics of content features, user features and propagation features as the input of the support vector machine (SVM) model, and then outputs the classification results of rumors. We implement this algorithm to classify propagation desire intensity level.

PCA+Random Forest: Al-Qurishi et al. [69] utilized the principal component analysis (PCA) method to rank the importance of user features and obtained the weights of different user characteristics. On the basis of it, these features are fed into the random forest classifier to accomplish the user classification task. We choose it as a classification method for comparison.

FNED: The FNED proposed by Liu et al. [70] is a classification method based on a deep neural network. We utilize it as a baseline method to predict propagation desire intensity level.

In addition, we also select several classical machine learning algorithms, such as logistic regression (LR) as a basic baseline method for comparison.

In order to accurately assess the intensity level of users' desire to spread disinformation, we firstly utilize the correctly classified instances, kappa statistics, mean absolute error and root mean square error to compare the performance of the model. In addition, to make a more comprehensive analysis of the advantages of the proposed propagation desire reasoning method, we also employ Macro-P, Macro-R and Macro-F1 to measure the performance of different methods. The specific calculation formulas are expressed as follows:

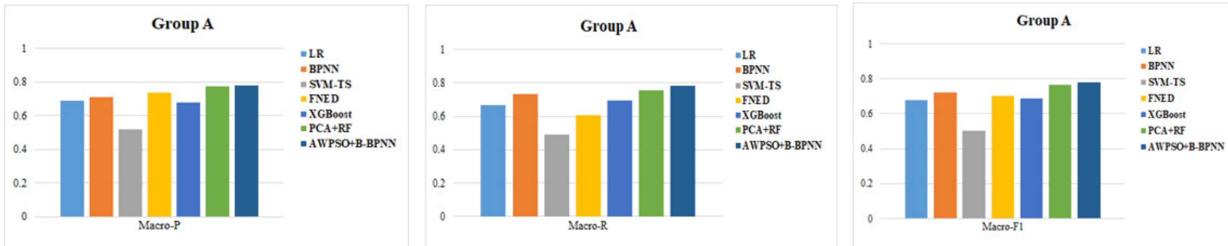
$$Macro-P=\frac{1}{n}\sum_{i=1}^{n}P_i \tag{22}$$

$$Macro-R=\frac{1}{n}\sum_{i=1}^{n}R_i \tag{23}$$

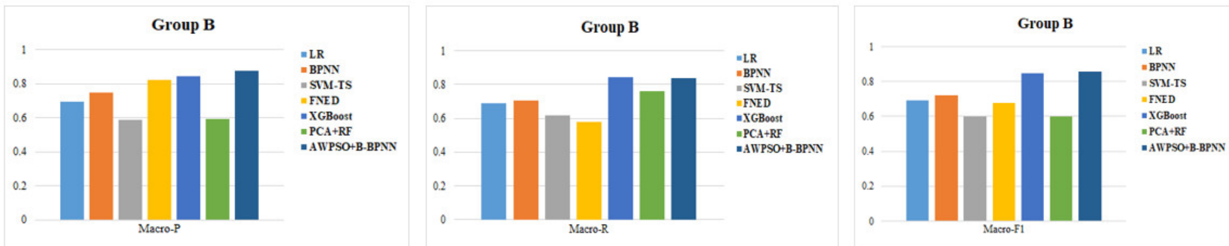
$$Macro-F_1=\frac{2\times macro-P\times macro-R}{macro-P+macro-R} \tag{24}$$

where $P_i = TP_i/(TP_i + FP_i)$, $R_i = TP_i/(TP_i + FN_i)$, $F_{1i} = 2P_iR_i/(P_i+R_i)$. In addition, TP_i refers to the number of positive categories predicted correctly in category i, FN_i represents the number of negative categories with prediction errors in category i, and FP_i refers to the number of positive classes with prediction errors in category i.

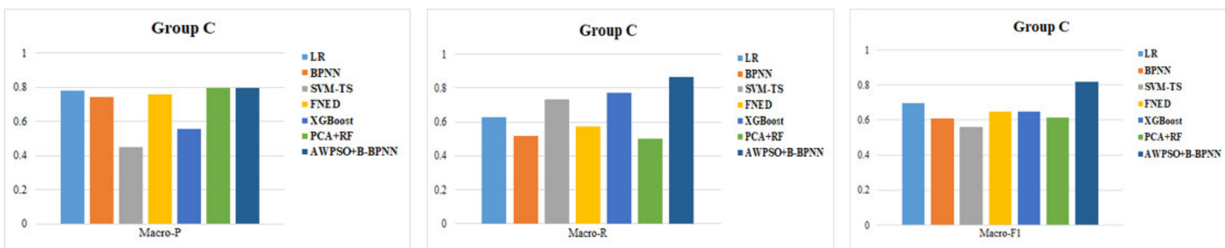
Using group partitioning, we first compare the proposed algorithm with six other baseline methods for groups A to D. According to findings outlined in Table 2, the prediction accuracy of the AWPSO+B-BPNN algorithm in the test set reaches 84%, and for the other algorithms, except for the XGBoost algorithm, the accuracy is between 60% and 70%. The corresponding kappa statistic of the AWPSO+B-BPNN



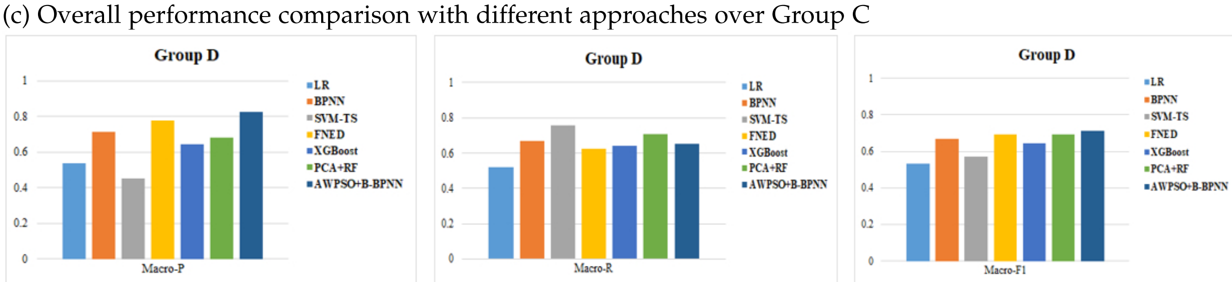
(a) Overall performance comparison with different approaches over Group A



(b) Overall performance comparison with different approaches over Group B



(c) Overall performance comparison with different approaches over Group C



(d) Overall performance comparison with different approaches over Group D

Fig. 4. Overall performance comparison with different approaches over Groups A, B, C and D. The horizontal and vertical coordinates in (a)-(d) denote three evaluation indexes (Macro-P, Macro-R and Macro-F1) and the corresponding probability values. The definitions of the evaluation metrics are provided in section 6.3. In addition to the proposed AWPSO+B-BPNN method, BPNN, SVM-TS, FNED, PCA+RF, XGBoost and logistic regression are chosen as comparison methods. For each group, we analysed and compared the performance of each method based on these three indicators via histograms. Consequently, from (a)-(d), we can observe that the performance of desire inference using the AWPSO+B-BPNN method is better than that of the other six methods.

algorithm is 0.75, while those of the other six algorithms are 0.53, 0.62, 0.47, 0.59, 0.70 and 0.57. In Table 3, the accuracy of the AWPSO+B-BPNN algorithm in the test set is 86%, while the accuracies of the other six algorithms are 60%, 73%, 66%, 71%, 82%,and 64%. The kappa statistic of the AWPSO+B-BPNN algorithm is 0.76, and those of the other six algorithms are basically between 0.4 and 0.7. In addition, the corresponding mean absolute error and root mean squared error of the AWPSO+B-BPNN algorithm are significantly better than those of the other five algorithms. In table 4 and table 5, we can also observe that the AWPSO+B-BPNN algorithm obtained the optimal result by comparing different baseline methods.

The other evaluation metrics utilized in this experiment to assess our model are Macro-P, Macro-R and Macro-F1. The results are shown in Fig.4. The horizontal and vertical coordinates in Fig.4 denote the above three evaluation indexes and the corresponding probability values. The Macro-P of the AWPSO+B-BPNN algorithm is 0.778, 0.874, 0.777 and 0.824 in group A, group B, group C and group D, respectively, significantly higher than those of the BPNN algorithm and the other five machine learning methods. The Macro-F1 values of 0.781 for group A, 0.855 for group B, 0.820 for group C, and 0.711 for group D illustrate that the AWPSO+B-BPNN algorithm obtains a good balance in terms of the Macro-P-Macro-R trade-off. From Fig.4(a)-(d), we can observe that the performance of desire inference using the AWPSO+B-BPNN algorithm is better than those of the other six algorithms.

7 Discussion

The inference of user desires to spread disinformation is the primary link for researchers in academia and industry to study the dissemination and control of disinformation. At present, social platform managers mainly adopt ”one size fits all” approaches for disinformation disseminators, and lack fine-grained schemes and refined management for disinformation governance. As disinformation campaigns become more widespread on OSNs, governments and social platform managers urgently need a complete set of fine-grained schemes to counter the spread of disinformation. In order to fill this gap, this paper provides a fine-grained hierarchical processing method for social platform managers by grading the desire intensity of users to spread disinformation and the subjective malicious degree of communicators under different topics and groups.

According to the results provided by the propagation desire inference model under different topics and groups, social platform managers can implement timely and effective fine-grained space-time usage control before and during communication for users flagged for strong propagation possibility, and finally realize the active control ability of disinformation transmission. The technology proposed in this paper has been applied in the social network platform Shareteches. Furthermore, this technology has certain universality and versatility, and can also be further applied to the governance and control of disinformation in third-party social platforms.

8 Conclusion

Existing measures to counter the spread of false information online focus on “one size fits all” approaches (e.g., “account prohibition and deletion”). In this paper, we presented fine-grained governance and mitigation strategies, and hopefully such strategies can minimize disinformation dissemination. We determined that the intensity of social users’ desires to spread disinformation is related to the topics and groups that users are interested in (i.e., the stronger the interest, the more likely the user will be to engage in disinformation). Additionally, social users with propagation desires tend to utilize their familiar social platforms and local circles for communication, and users with medium and strong propagation desire occupy a proportion of 68.61%. The behaviour and desire to spread disinformation to the cross-platform are not strong, and users with medium and strong propagation desire only account for 3.14%.

Specially, we proposed a user group partition method that divides disseminators into different groups according to the content and regularity of spreading disinformation. Then, according to the internal relationship between the user’s propagation desire and behaviour, a user’s propagation desire inference model based on propagation characteristics (behaviour characteristics and time characteristics) and a B-BP neural network are constructed for each group. Due to the interaction of user propagation behaviour and the correlation among propagation characteristics, the B-BP neural network may over-fit. Therefore, we utilize the AWPSO evolutionary algorithm to further optimize the B-BP neural network. Compared to the other six methods, our model has obvious advantages in terms of accuracy and robustness. For example, our approach allows us to accurately quantify the malicious degree of user propagation desire and determine the internal relationship between group user propagation behaviour and desire.

Building on the understanding of the inference of group users’ propagation desires, we will further analyse user propagation trends and identify user propagation goals and intentions with the aim of mitigating disinformation propagation more effectively in the future.

Acknowledgments

The authors appreciated the constructive feedback from the associate editor and the three reviewers during the review process. 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, Program for Henan Province Key Science and Technology No.212102210383, which are titled by “Social Situational Analytics Based Fake Information User Propagation Intention Detection and Usage Control”, “Research on SocialSitu Security Theory and Key Technologies”, and “Research on Privacy Protection Mining Methods for Multimedia Social Networks”, respectively. The work of K.-K. R. Choo was supported only by the cloud technology endowed professorship.

References

[1] Smith S T, Kao E K, Mackin E D, et al. Automatic detection of influential actors in disinformation networks. Proceedings of the National Academy of Sciences, 2021, 118(4): e2011216118.
[2] Bovet A, Makse H A. Influence of fake news in Twitter during the 2016 US presidential election. Nature Communications, 2019, 10(1): 7
[3] Ferrara E. Disinformation and social bot operations in the run up to the 2017 french presidential election. First Monday, 2017, 22(8): 1-2
[4] Bondielli A, Marcelloni F. A survey on fake news and rumour detection techniques. Information Sciences, 2019, 497: 38-55
[5] Berghel H. The online disinformation opera, Computer, 2021, 54(12): 109-115
[6] 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
[7] Le T T, Andreadakis Z, Kumar A, et al. The COVID-19 vaccine development landscape. Nature Reviews Drug Discovery, 2020,19: 305-306
[8] Lazer D M J, Baum M A, Benkler Y, et al. The science of fake news. Science, 2018, 359(6380): 1094-1096
[9] Ahmad N, Milic N, Ibahrine M. Data and Disinformation. Computer, 2021, 54(7): 105-110
[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 ODonovan, et al. Uncertainty-based false information propagation in social networks. ACM Transactions on Social Computing, 2019, 2(2): 1-34
[12] Moreno Y, Pastor-Satorras R, Vespignani A. Epidemic out-breaks in complex heterogeneous networks. The European Physical Journal B-Condensed Matter and Complex Systems, 2001, 26(4): 521-529
[13] Pastor-Satorras R, Vespignani A. Epidemic spreading in scale-free networks. Physical Review Letters, 2000, 86(14): 3200-3203
[14] Zheng M, Lu L, Zhao M. Spreading in online social networks: The role of social reinforcement. Physical Review E, 2013, 88(1): 12818

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2022.3165324, IEEE Transactions on Dependable and Secure Computing

[15] Wen S, Haghighi M S, Chen C, et al. A sword with two edges: propagation studies on both positive and negative information in online social networks. IEEE Transactions on Computers, 2015, 64(3): 640-653
[16] 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
[17] He Z B, Cai Z P, Yu J G, et al. Cost-efficient strategies for restraining rumor spreading in mobile social networks. IEEE Transactions on Vehicular Technology, 2017, 66(3): 2789-2800
[18] 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
[19] Kumar K, Geethakumari G. Detecting misinformation in online social networks using cognitive psychology. Human-centric Computing and Information Sciences, 2014, 4(1): 14-26
[20] Vosoughi S, Roy D, Aral S. The spread of true and false news online. Science, 2018, 359(6380): 1146-1151
[21] Pierri F. The Diffusion of Mainstream and Disinformation News on Twitter: The Case of Italy and France. Proceedings of the World Wide Web Conference 2020 (WWW 20). Association for Computing Machinery, New York, NY, USA, 617-622.
[22] Barfar A. Cognitive and affective responses to political disinformation in Facebook. Computers in Human Behavior, 2019, 101(12): 173-179.
[23] Zhao Z, Zhao J, Sano Y, et al. Fake news propagates differently from real news even at early stages of spreading. EPJ Data Science, 2020, 9(1): 1-14
[24] Rao Y, Wu L, Zhang J. A survey of information propaganda mechanism under the cross-medium. Science China Information Sciences, 2017, 47(12): 27-49
[25] Wang C, Wang G, Luo X, et al. Modeling rumor propagation and mitigation across multiple social networks. Physica A: Statistical Mechanics and its Applications, 2019, 535: 122240
[26] Knippenberg A D. Social Identifications: A Social Psychology of Intergroup Relations and Group Processes. British Journal of Social Psychology, 1991, 30(3):271-272
[27] Gibb, Cecil. The Influence of Cattell in Social Psychology and Group Dynamics. Multivariate Behavioral Research, 1984, 19: 193-206
[28] Paulus P B. Psychology of group influence. Psychology Press, 2015
[29] Brown R. Group Processes: Dynamics Within and Between Groups, 2e. Oxford: Blackwell, 2000
[30] Nechansky H. The four modes of coexistence in psychology and group dynamics. Kybernetes, 2016, 45(3): 371-392
[31] Adrianna C. Jenkins, Pierre Karashchuk, Lusha Zhu. Predicting human behavior toward members of different social groups. Proceedings of the National Academy of Sciences Sep 2018, 115(39) 9696-9701
[32] Jamieson K H, Cappella J N. Echo chamber: Rush Limbaugh and the conservative media establishment. Oxford University Press, 2008
[33] Choi D, Chun S, Oh H, et al. Rumor Propagation is Amplified by Echo Chambers in Social Media. Scientific Reports, 2020, 10(1): 310-320
[34] 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, 17(3): 1910-1923
[35] Sahafizadeh E, Ladani B T. The impact of group propagation on rumor spreading in mobile social networks. Physica A: Statistical Mechanics and its Applications, 2018, 506: 412-423
[36] Vicario M D, Bessi A, Zollo F, et al. The spreading of misinformation online. Proceedings of the National Academy of Sciences of the United States of America, 2016, 113(3): 554-559
[37] Bessi A, Coletto M, Davidescu G A, et al. Science vs conspiracy: collective narratives in the age of misinformation. Plos One, 2014, 10(2): e0118093
[38] Barwise J, Perry J. The situation underground. Stanford Working Papers in Semantics, 1980
[39] 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
[40] Chang C. Situation analytics: A foundation for a new software engineering paradigm. Computer, 2016, 49(1):24-33
[41] Chang C. Situation analytics-at the dawn of a new software engineering paradigm. Science China Information Sciences, 2018, 61(05): 050101
[42] Yang J, Chang C, Hua M. A situation-centric approach to identifying new user intentions using the MTL method. Proceedings of the 41nd Annual Computer Software and Applications Conference (COMPSAC). IEEE, 2017.
[43] Peng S, Yang J, Hua M, et al. A Multi-layered Desires Based Framework to Detect Users' Evolving Non-functional Requirements. Proceedings of the 42nd Annual Computer Software and Applications Conference (COMPSAC). IEEE, 2018.
[44] 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
[45] Adigun O, Kosko B. Bidirectional Backpropagation. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2020, 50(5): 1982-1994
[46] Liu W, Wang Z, Yuan Y, et al. A Novel Sigmoid-Function-Based Adaptive Weighted Particle Swarm Optimizer. IEEE Transactions on Cybernetics, 2021, 51(2): 1085-1903
[47] Bohaienko V, Gladky A, Romashchenko M, et al. Identification of fractional water transport model with ψ-Caputo derivatives using particle swarm optimization algorithm. Applied Mathematics and Computation, 2021, 390: 125665
[48] Shao C C, Ciampaglia G L, Varol O, et al. The spread of low-credibility content by social bots. Nature Communications, 2018, 9: 4787
[49] Shao C C, Ciampaglia G L, Varol O, et al. The spread of fake news by social bots. arXiv preprint arXiv:1707.07592, 2017
[50] Starbird K. Disinformation's spread: bots, trolls and all of us. Nature, 2019, 571(7766): 449
[51] Bastick Z. Would you notice if fake news changed your behavior? An experiment on the unconscious effects of disinformation. Computers in Human Behavior, 2021, 116:106633. doi.org/10.1016/j.chb.2020.106633
[52] Colliander J. "This is fake news": Investigating the role of conformity to other users' views when commenting on and spreading disinformation in social media. Computers in Human Behavior, 2019, 97(8): 202-215.
[53] Liang G , He W , Xu C , et al. Rumor Identification in Microblogging Systems Based on Users' Behavior. IEEE Transactions on Computational Social Systems, 2015, 2(3): 99-108
[54] Yaqub W, Kakhidze O, Brockman M L, et al. Effects of credibility indicators on social media news sharing intent. Proceedings of the 2020 ACM CHI Conference on Human Factors in Computing Systems, Honolulu, USA, 2020
[55] Liu Y, Wu Y F. Early Detection of fake news on social media through propagation path classification with recurrent and convolutional networks. Proceedings of the 32th AAAI Conference on Artificial Intelligence. Hong Kong, China, 2018: 354-361
[56] Blei D M, Ng A Y, Jordan M J. Latent Dirichlet allocation. Journal of Machine Learning Research, 2003(3): 993-1022
[57] Porteous I, Newman D, Ihler A T, et al. Fast collapsed Gibbs sampling for latent Dirichlet allocation. Proceedings of the 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Nevada, USA, 2008
[58] Kim D, Seo D, Cho S, et al. Multi-co-training for document classification using various document representations: TF-IDF, LDA, and Doc2Vec. Information sciences, 2019, 477: 15-29
[59] Cui L, Tao Y, Deng J, et al. BBO-BPNN and AMPSO-BPNN for multiple-criteria inventory classification. Expert Systems with Applications, 2021, 175(5): 114842
[60] Dong X, Lian Y, Liu Y. Small and Multi-Peak Nonlinear Time Series Forecasting Using a Hybrid Back Propagation Neural Network. Information Sciences, 2018,424: 39-54
[61] Jethmalani C R, Simon S P, Sundareswaran K, et al. Auxiliary Hybrid PSO-BPNN based Transmission System Loss Estimation in Generation Scheduling. IEEE Transactions on Industrial Informatics, 2017, 13(4): 1692-1703
[62] Zhang Z, Sun R, Zhao C, et al. CyVOD: a novel trinity multi-media social network scheme. Multimedia Tools and Applications, 2016: 1-17
[63] Zhang Z, Cheng L, Gupta B B, et al. Efficient compressed ciphertext length scheme using multi-authority CP-ABE for hierarchical attributes. IEEE Access, 2018, 6(1): 38273-38284
[64] Zhang Z , Jing J , Wang X , et al. A crowdsourcing method for online social networks security assessment based on human-centric

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2022.3165324, IEEE Transactions on Dependable and Secure Computing

computing. Human-centric Computing and Information Sciences, 2020, 10(1):1-19

[65] Shi P, Zhang Z, Choo K K R. Detecting Malicious Social Bots Based on Clickstream Sequences. IEEE Access, 2019, 7(1): 28855-28862

[66] Paik J H. A novel TF-IDF weighting scheme for effective ranking. Proceedings of the 36th international ACM SIGIR conference on Research and development in information retrieval. 2013, 343-352

[67] Reis J, Correia A, Murai F, et al. Supervised Learning for Fake News Detection, IEEE Intelligent Systems, 2019, 34(2): 76-81

[68] Ma J, Gao W, Wei Z, et al. Detect Rumors Using Time Series of Social Context Information on Microblogging Websites. ACM International Conference on Information and Knowledge Management, 2015, 1751-1754

[69] Al-Qurishi M, Hossain M S, Alrubaian M, et al. Leveraging Analysis of User Behavior to Identify Malicious Activities in Large-scale Social Networks. IEEE Transactions on Industrial Informatics, 2018, 14(2): 799-813

[70] Liu Y, Wu Y. FNED: A Deep Network for Fake News Early Detection on Social Media. ACM Transactions on Information Systems, 38(3): 25-57, 2020

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 College of Information Engineering, Henan University of Science and Technology and Henan International Joint Laboratory of Cyberspace Security Applications, Luoyang, China. His research interests include social network security and computing, social situation analytics, and social big data.

Zhiyong Zhang 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 & 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. Contact him at xidianzzy@126.com.

Kim-Kwang Raymond Choo 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 Societys 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.

Kefeng Fan received Ph.D degree in test signal processing from Xidian University, Shaanxi, China. From Feb., 2008 to Nov., 2010, he was doing the postdoctoral in State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, China. After Feb., 2010, he worked as a senior engineer in the field of multimedia technology standardization in China Electronics Standardization Institute(CESI), Beijing, China. Since November 2018, he worked as the director of the Research Center of Digital Technology, CESI. His current research interests include data security and intelligent signal processing. He is member of ISO/IEC JTC1/SC27 & SC29 and IEC/ACSEC. He was appointed as the Young Professional of IEC in 2011.

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.

Lili Zhang received her Master and Ph.D. degrees in Computer Network at Xidian University, Shaanxi, China. She is currently a Research Fellow with the Henan International Joint Laboratory of Cyberspace Security Applications, China. Moreover, she is also a lecturer of Henan University of Science and Technology, China. Her research interests include social network security and cloud computing.