Robust Spammer Detection Using Collaborative Neural Network in Internet of Thing Applications

Zhiwei Guo, Yu Shen, Ali Kashif Bashir, *Senior Member, IEEE,* Muhammad Imran, *Member, IEEE,* Neeraj Kumar, *Senior Member, IEEE,* Di Zhang, *Senior Member, IEEE,* and Keping Yu, *Member, IEEE*

Abstract—**Spamming is emerging as a key threat to Internet of Things (IoT)-based social media applications. It will pose serious security threats to the IoT cyberspace. To this end, artificial intelligence-based detection and identification techniques have been widely investigated. The literature works on IoT cyberspace can be categorized into two categories: 1) behavior pattern-based approaches; and 2) semantic pattern-based approaches. However, they are unable to effectively handle concealed, complicated, and changing spamming activities, especially in the highly uncertain environment of the IoT. To address this challenge, in this paper, we exploit the collaborative awareness of both patterns, and propose a <u>Co</u>llaborative neural network-based <u>Spam</u>mer detection mechanism (Co-Spam) in social media applications. In particular, it introduces multi-source information fusion by collaboratively encoding long-term behavioral and semantic patterns. Hence, a more comprehensive representation of the feature space can be captured for further spammer detection. Empirically, we implement a series of experiments on two real-world datasets under different scenario and parameter settings. The efficiency of the proposed Co-Spam is compared with five baselines with respect to several evaluation metrics. The experimental results indicate that the Co-Spam has an average performance improvement of approximately 5% compared to the baselines.**

Index Terms—**Internet of Things, spammer detection, neural network, collaborative awareness**

Zhiwei Guo and Yu Shen are with National Research Base of Intelligent Manufacturing Service, Chongqing Technology and Business University, Chongqing 400067, China. (e-mail: {zwguo, shenyu}@ctbu.edu.cn).

Ali Kashif Bashir is with the Department of Computing and Mathematics, Manchester Metropolitan University, UK. (e-mail: Dr.alikashif.b@ieee.org).

Muhammad Imran is with the College of Applied Computer Science, King Saud University, Riyadh, Saudi Arabia. (e-mail: dr.m.imran@ieee.org).

Neeraj Kumar is with the Department of Computer Science and Engineering, Thapar Institute of Engineering, India and Department of Computer Science and information engineering, Asia University, Taiwan and King Abdul Aziz University, Jeddah, Saudi Arabia and Charles Darwin University, Australia. (e-mail: neeraj.kumar@thapar.edu).

Di Zhang is with the School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China. (e-mail: dr.di.zhang@ieee.org).

Keping Yu is with the Global Information and Telecommunication Institute, Waseda University, Tokyo, Japan. (e-mail: keping.yu@aoni.waseda.jp).

I. INTRODUCTION

THE past decade has witnessed the great progress in artificial intelligence and communication networks. Predictably, cyberspace of the Internet of Things (IoT) will become an important living space for human beings in the 5G era [1]. Accordingly, cyberspace security will be of great importance to the economic prosperity and social stability, such as the spammer detection. Online spamming is gradually becoming a remarkable security threat to the IoT-based social media applications [2]. In literature, spammers refer to communities that publish tendentious statements in a variety of media to satisfy their commercial or political goals [9]. To ensure a secure and reliable environment, effective detection or identification mechanisms for spammers hold significant importance [17]. Nevertheless, precise spammer detection for IoT-based social media is usually regarded as a challenging task in actual practice for two reasons. First, online spamming is highly associated with social networks; thus, contextual information such as social relations and even financial relations needs to be deeply analyzed as an auxiliary. Second, excellent modeling schemes for semantic features play an important role. This is because the main purpose of online spamming is to create specific directions for public opinion [24]. Considering more complicated environment in IoT applications, establishing more fine-grained feature spaces will greatly influence the effect of spammer detection [34].

In fact, in recent years, a considerable number of studies have been devoted to spammer detection. Relevant studies can be classified into two types: behavioral pattern-based approaches [3]-[19] and semantic pattern-based approaches [20]-[30]. The former concentrate on the pattern characteristics of primary behaviors such as social behaviors, comment behaviors, and forwarding behaviors. For example, Cao *et al.* [6] set up two different detection methods for individuals and groups respectively. In particular, they proposed to identify hidden spammers by leveraging collusive relations between spammers and business competition between locations. In contrast, the latter emphasize the semantic features of speech contents from the perspective of language statistics. For instance, Wang *et al.* [26] proposed a detection framework named GSLDA for group spamming detection in product review data. The GSLDA first adapts LDA (Latent Dirichlet Allocation) algorithm to the product review context to cluster similar reviewers, and deviated suspicious groups. However,

both types suffer from some limitations or drawbacks. On the one hand, the concealment of spamming activities is becoming mature over the course of long-term confrontations with regulatory mechanisms, resulting in difficulties for recognition. For instance, many spammers generally perform normal browsing and speaking behaviors like ordinary users. In this case, only a small number of spamming operations are involved. On the other hand, most semantic pattern-based approaches are endowed with a good ability to analyze and understand only regular machine speech. Such approaches are not suitable for complicated and changeable contents. In summary, global insights into multisource information fusion are urgently needed to improve the accuracy of spammer identification.

To address this challenge, this paper manages to capture a more comprehensive representation of the feature space. It does so by combining behavior patterns and semantic patterns. Such an idea of multisource information integration is likely to become a more promising solution, especially under IoT environment. Although Yuan *et al.* [31] and Wang *et al.* [32] once dealt with spammer detection problems by simultaneously considering semantic and behavioral patterns, they still neglected the dynamic characteristics of social activities. In particular, their approaches were established based on the assumption that social activities at different timestamps are mutually independent, and the evolving nature of social activities was not considered.

In this paper, a **Co**llaborative neural network-based **Spam**mer detection mechanism (Co-Spam) is proposed to solve the problem above. Co-Spam combines both semantic and behavioral patterns to solve spammer detection problems. In addition, the evolving environments of social activities are included. In our work, the speech contents and behavior records of users at different timestamps are first viewed as their feature sequences. At each timestamp, a bidirectional autoencoder (Bi-AE) is developed to model semantic characteristics, and a graph convolutional network (GCN) is designed to learn the embeddings of behavior patterns. After that, the feature space at each timestamp is obtained through a hybrid mapping of the two components, and a long short-term memory (LSTM) model is introduced to express the evolving characteristics of the feature sequence. At last, we implement a series of experiments on two real-world datasets. Five typical baselines are selected as comparison to assess efficiency of the proposed Co-Spam under several common metrics. The main contributions of this paper are summarized as follows:

a) We recognize the limitations of existing spammer detection methods, especially under the schemes of IoT-based social media.

b) We manage to construct a fine-grained feature space combining semantic and behavioral patterns, and we propose the Co-Spam for IoT-based social media.

c) Based on our simulation results, we find that the Co-Spam has an average performance improvement of approximately 5% compared to the baselines.

II. PROBLEM STATEMENT

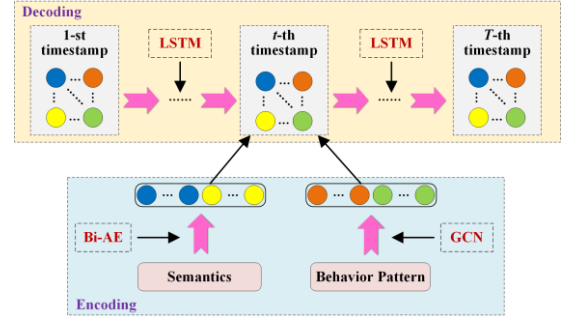The primary architecture of the proposed Co-Spam is

Fig. 1. Architecture of the spammer detection mechanism Co-Spam.

illustrated in Fig. 1. It is assumed that $u_i (i = 1,2,\cdots,|u|)$ denotes the set of users in IoT-based social media. Each user is assumed to able to perform various online activities inside it. Considering the time-varying characteristics in IoT environment, long-term activities are separated into a number of parts with respect to a total of T timestamps whose index symbols are denoted as $t(t = 1,2,\cdots,T)$. For user u_i at the t-th timestamp, it is necessary to construct a global feature space $\boldsymbol{\mathcal{G}}_i^{(t)}$ by exploiting the collaborative awareness of semantic factor $\boldsymbol{S}_i^{(t)}$ and behavior pattern factor $\boldsymbol{Y}_i^{(t)}$. Finally, the long-term evolving characteristics of the global feature space are modeled via a recurrent neural network approach to calculate the nature of user u_i. In a word, the whole workflow of the Co-Spam can be viewed as two types of procedures: encoding and decoding. At each timestamp, semantic and behavioral patterns of a user are respectively encoded into abstract feature factors through Bi-AE and GCN. After long-term feature factors constitute a sequence, LSTM is employed to encode such a pattern sequence.

At the t-th timestamp, the textual contents associated with user u_i are denoted as $c_i^{(t)}$. Because the span of each timestamp does not last very long (one day or even one hour), the textual contents within a timestamp are assumed to constitute one sentence. Then, a Bi-AE model is formulated to obtain the encoding of semantics factor $\boldsymbol{S}_i^{(t)}$. In addition, a series of behavior patterns correlated to user u_i constitute a GCN model, where specific behaviors are regarded as nodes and their relations are viewed as edges. Then, a GCN model is developed to learn the graph embedding of behavior patterns denoted as $\boldsymbol{Y}_i^{(t)}$. Correspondingly, the global feature space $\boldsymbol{\mathcal{G}}_i^{(t)}$ of this timestamp is formulated by concatenating semantic factor $\boldsymbol{S}_i^{(t)}$ and behavior pattern factor $\boldsymbol{Y}_i^{(t)}$ together. Generalized to the whole time domain, an LSTM model is established to model the evolving characteristics of the series of activities and, finally, to identify the nature of user u_i.

III. METHODOLOGY

This section fully considers characteristics of IoT situations, and presents mathematical descriptions of the Co-Spam. It is composed of three parts corresponding to three subsections: semantic pattern modeling, behavioral pattern modeling and prediction.
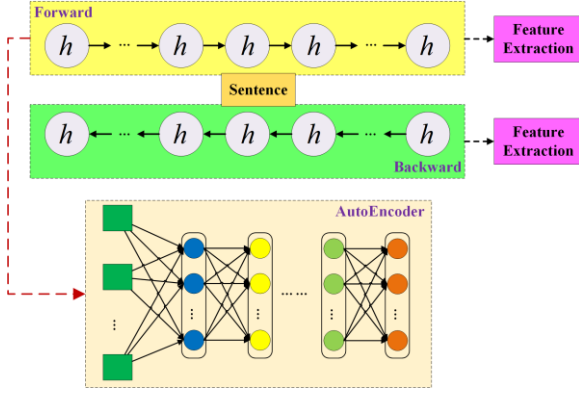
Fig. 2. Flowchart of the Bi-AE process at each timestamp.

A. Semantic Pattern Modeling

It is necessary to model the semantic patterns of sentences to consider vectorized expressions from both forward and backward directions. Bi-AE is developed to encode semantic characteristics at different timestamps, as illustrated in Fig. 2. At the t-th timestamp, Bi-AE tries to capture semantic embedding through the following two formulas:

$$\overrightarrow{\boldsymbol{h}}_{ij}^{(t)} = \overrightarrow{\Phi}\big[c_i^{(t)}, \overrightarrow{h}_{i,j-1}^{(t)}\big] \qquad (1)$$

$$\overleftarrow{\boldsymbol{h}}_{ij}^{(t)} = \overleftarrow{\Phi}\big[c_i^{(t)}, \overleftarrow{h}_{i,j+1}^{(t)}\big] \qquad (2)$$

where $\overrightarrow{\Phi}(\cdot)$ and $\overleftarrow{\Phi}(\cdot)$ denote the forward and backward activation operators for the sequence $c_i^{(t)}$, respectively, and j is the index number of words ranging from 1 to $N_i^{(t)}$. Specifically, the former models the sequence with j changing from 1 to $N_i^{(t)}$, while the latter models the sequence with j changing from $N_i^{(t)}$ to 1. $\overrightarrow{\boldsymbol{h}}_{ij}^{(t)}$ and $\overleftarrow{\boldsymbol{h}}_{ij}^{(t)}$ denote the forward and backward hidden states, respectively, and they are concatenated into a novel hidden state vector, $\boldsymbol{h}_{ij}^{(t)} = \big[\overrightarrow{\boldsymbol{h}}_{ij}^{(t)}, \overleftarrow{\boldsymbol{h}}_{ij}^{(t)}\big]$.

This work categorizes all words into two types, crucial words and background words, as each word is likely to play different roles concerning the meaning of a sentence. Clearly, crucial words are the main contributors of meanings, and background words are the auxiliary parts with regard to sentence integrity.

Hence, an attention mechanism is introduced to automatically extract crucial words from sentences at each timestamp. Then, all the selected key words are transferred into a central vector:

$$\boldsymbol{C}_{i\alpha}^{(t)} = \big\{\boldsymbol{h}_{i\alpha}^{(t)} \big| \alpha = 1,2,\cdots,\omega_i^{(t)}\big\} \qquad (3)$$

where $\boldsymbol{h}_{i\alpha}^{(t)}$ is the hidden state of the α-th crucial word and α is the index number of crucial words ranging from 1 to $\omega_i^{(t)}$. Accordingly, the remaining background words are transferred into an edge vector:

$$\boldsymbol{E}_{i\beta}^{(t)} = \big\{\boldsymbol{h}_{i\beta}^{(t)} \big| \beta = 1,2,\cdots,\big(N_i^{(t)} - \omega_i^{(t)}\big)\big\} \qquad (4)$$

where $\boldsymbol{h}_{i\beta}^{(t)}$ is the hidden state of the β-th background word and β is the index number of background words ranging from 1 to $\big(N_i^{(t)} - \omega_i^{(t)}\big)$. The concatenation of the central vector and edge
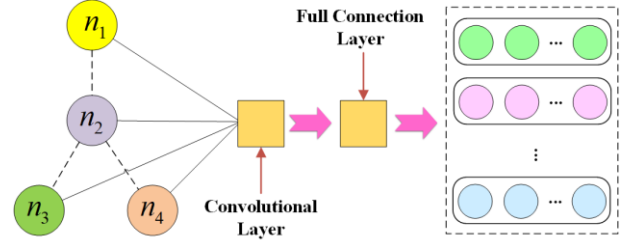

Fig. 3. Flowchart of the GCN process at each timestamp.

vector results in the hidden vector at the t-th timestamp:

$$\boldsymbol{H}_i^{(t)} = \boldsymbol{C}_{i\alpha}^{(t)} \oplus \boldsymbol{E}_{i\beta}^{(t)} \qquad (5)$$

To encode the semantic feature space, the attention weight for crucial words and background words needs to be deduced. The attention weight of crucial words is defined as:

$$\mathcal{A}_{iC}^{(t)} = \sigma_1\big[\boldsymbol{W}_{i1}\sigma_2\big(\boldsymbol{W}_{iH}\boldsymbol{H}_i^{(t)} + \boldsymbol{W}_{iC}\boldsymbol{C}_{i\alpha}^{(t)} + \boldsymbol{b}_{i1}\big)\big] \qquad (6)$$

where $\boldsymbol{W}_{i1}$, $\boldsymbol{W}_{iH}$ and $\boldsymbol{W}_{iC}$ are weight matrices, $\boldsymbol{b}_{i1}$ is the bias parameter, $\sigma_1(\cdot)$ is the softmax activation function, and $\sigma_2(\cdot)$ is the tanh activation function. For user u_i, the enhanced hidden state vector for crucial words at the t-th timestamp is deduced as:

$$\boldsymbol{S}_{iC}^{(t)} = \sum_{j=1}^{N_i^{(t)}} \mathcal{A}_{iC}^{(t)} \boldsymbol{h}_{ij}^{(t)} \qquad (7)$$

Similarly, attention weight for background words is defined as:

$$\mathcal{A}_{iE}^{(t)} = \sigma_1\big[\boldsymbol{W}_{i2}\sigma_2\big(\boldsymbol{W}_{ih}\boldsymbol{H}_i^{(t)} + \boldsymbol{W}_{ie}\boldsymbol{E}_{i\alpha}^{(t)} + \boldsymbol{b}_{i2}\big)\big] \qquad (8)$$

where $\boldsymbol{W}_{i2}$, $\boldsymbol{W}_{iH}$ and $\boldsymbol{W}_{iE}$ are weight matrices and $\boldsymbol{b}_{i2}$ is the bias parameter. The enhanced hidden state vector for background words at the t-th timestamp is deduced as:

$$\boldsymbol{S}_{iE}^{(t)} = \sum_{j=1}^{N_i^{(t)}} \mathcal{A}_{iE}^{(t)} \boldsymbol{h}_{ij}^{(t)} \qquad (9)$$

Therefore, the goal of semantic modeling is to learn a mapping function $S_i^{(t)}$ that best expresses the semantic embeddings for user u_i at the t-th timestamp:

$$\boldsymbol{S}_i^{(t)} = \tau \boldsymbol{W}_{i3}\boldsymbol{S}_{iC}^{(t)} + (1 - \tau)\boldsymbol{W}_{i4}\boldsymbol{S}_{iE}^{(t)} \qquad (10)$$

where $\boldsymbol{W}_{i3}$ and $\boldsymbol{W}_{i4}$ are weight matrices and τ is the trade-off parameter.

B. Behavior Pattern Modeling

This subsection proposes to encode the behavior pattern features of users through GCN. As is shown in Fig. 3, behavior pattern types are viewed as nodes and the relations among them are regarded as edges. Given that the initial contents of these nodes are mostly unsuitable for direct calculation, they are

TABLE I
EXAMPLES OF STRUCTURED ATTRIBUTES

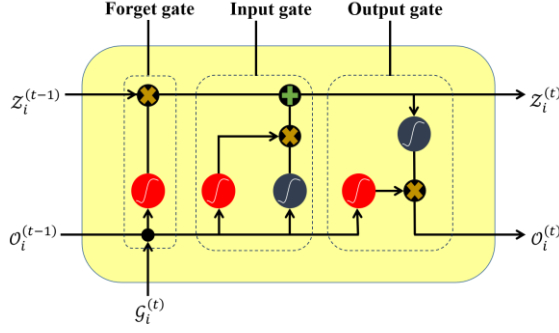| Behavior Pattern Names	Encoded Formats
Vector of Social Relations	$[1,0,\cdots,0]$
Personal Tags	$[0,1,\cdots,0]$
User Level	$[0,0,\cdots,1]$

Fig. 4. Flowchart of the LSTM process at each timestamp.

expected to be mapped into vectorized numerical data. Data categories are generally structured data, and their contents can be encoded into feature vectors via one-hot encoding. Examples of some attributes are shown in TABLE I.

In addition, there are some attributes whose data structures are initially numerical, namely, the registration time and number of speeches. The contents of these attributes are directly transferred into vectors without extra operations. Because the dimensions of different attributes are usually diverse, the attribute with the most dimensions is selected as uniformity, which is assumed to be $\mathcal{D}$. Then, the dimensions of other attributes are extended to $\mathcal{D}$ by adding a certain number of zeros.

For user u_i, his or her behavior pattern vector at the t-th timestamp can be represented as the following format:

$$\mathcal{P}_i^{(t)} = \left\{ q_{i1}^{(t)}, q_{i2}^{(t)}, \cdots, q_{iz}^{(t)} \right\} \tag{11}$$

where z is the actual number of behavior patterns. The GCN manages to learn the graph embedding of the γ-th behavior pattern:

$$\mathcal{B}_{i\gamma}^{(t)} = \sum_{\gamma=1}^{z} \sum_{\substack{\eta=1 \\ \eta \neq \gamma}}^{z} \mathcal{R}_{i\gamma}^{(t)}(\gamma, \eta) \, \mathbf{Q}_i^{\eta \to \gamma} q_{i\gamma}^{(t)} + \boldsymbol{e}_{i\gamma}^{(t)} \tag{12}$$

where $\mathcal{R}_{i\gamma}^{(t)}(\gamma, \eta)$ is the adjacency matrix at the t-th timestamp, $\mathbf{Q}_i^{\eta \to \gamma}$ is the set of transition matrices into the γ-th behavior pattern, and $\boldsymbol{e}_{i\gamma}^{(t)}$ is the bias vector. Among them, $\mathcal{R}_{i\gamma}^{(t)}(\gamma, \eta)$ is defined as:

$$\delta_i^{(t)}(\gamma, \eta) = \frac{\psi(\tilde{q}_{i\gamma}^{(t)} \cap \tilde{q}_{i\eta}^{(t)}) / \psi(\tilde{q}_{i\eta}^{(t)})}{\sum_{\xi} \psi\left(\tilde{q}_{i\gamma}^{(t)} \cap \tilde{q}_{i\xi}^{(t)}\right) / \psi\left(\tilde{q}_{i\gamma}^{(t)}\right)} \tag{13}$$

$$\mathcal{R}_i^{(t)}(\gamma, \eta) = \begin{cases} \delta_i^{(t)}(\gamma, \eta) & \gamma \neq \eta \\ 0 & \text{else} \end{cases} \tag{14}$$

where $\psi(\cdot)$ is the counting operator and ξ is the index number of a behavior pattern different from γ and η. $\psi(\tilde{q}_{i\gamma}^{(t)})$ and $\psi(\tilde{q}_{i\eta}^{(t)})$ denote the change frequency of the γ-th and η-th behavior patterns during the timestamp, respectively. Similarly, $\psi(\tilde{q}_{i\gamma}^{(t)} \cap \tilde{q}_{i\eta}^{(t)})$ denotes the cooccurrence frequency of the γ-th and η-th behavior patterns, and $\psi\left(\tilde{q}_{i\gamma}^{(t)} \cap \tilde{q}_{i\xi}^{(t)}\right)$ denotes the cooccurrence frequency of the γ-th and ξ-th behavior patterns during the timestamp.

For the γ-th behavior pattern, we follow [33] to divide the

transition matrix into two transition factors with respect to two directions: input factor $\mathbf{Q}_{i\gamma}^{(In)}$ and output factor $\mathbf{Q}_{i\gamma}^{(Out)}$. For a directed edge from the γ-th to η-th behavior pattern, the relation state is essentially transmitted from $\mathbf{Q}_{i\gamma}^{(Out)}$ to $\mathbf{Q}_{i\eta}^{(In)}$, which is represented as:

$$\mathbf{Q}_i^{\gamma \to \eta} = \mathbf{Q}_{i\gamma}^{(Out)} \mathbf{Q}_{i\eta}^{(In)} \tag{15}$$

Thus, the learning goal in Eq. (12) can be rewritten as:

$$\mathcal{B}_{i\gamma}^{(t)} = \sum_{\gamma=1}^{z} \sum_{\substack{\eta=1 \\ \eta \neq \gamma}}^{z} \mathcal{R}_{i\gamma}^{(t)}(\gamma, \eta) \, \mathbf{Q}_{i\gamma}^{(Out)} \mathbf{Q}_{i\eta}^{(In)} c_{i\gamma}^{(t)} + \boldsymbol{e}_{i\gamma}^{(t)} \tag{16}$$

The graph embedding vector of behavior patterns is supposed to be transferred into the convolutional layer and full connection layer of the GCN to generate encoding results. Convolutional operation maps the embedding vectors into a high-order feature, which is described as:

$$\mathcal{X}_i^{(t)} = \sigma_3 \left[\sum_{\gamma=1}^{z} \left(\mathbf{W}_{i4} \otimes \mathcal{B}_{i\gamma}^{(t)} + \boldsymbol{b}_{iX} \right) \right] \tag{17}$$

where $\sigma_3(\cdot)$ is the ReLU activation function, $\otimes$ is the convolution operator, $\mathbf{W}_{i4}$ is the weight parameter, and $\boldsymbol{b}_{i2}$ is the bias vector. The full connection layer manages to map $\mathcal{X}_i^{(t)}$ into a deeper vectorized format, which is represented as:

$$\mathbf{Y}_i^{(t)} = \sigma_3 \left\{ \mathbf{W}_{i6} \sigma_3 \left[\mathbf{W}_{i5} \otimes \mathcal{X}_i^{(t)} + \boldsymbol{b}_{iY} \right] + \boldsymbol{b}_{iY}' \right\} \tag{18}$$

where $\mathbf{W}_{i5}$ and $\mathbf{W}_{i6}$ are weight matrices and b_{iY} and b_{iY}' are bias vectors.

C. Prediction

The global embedding of the feature space at the t-th timestamp is supposed to be established by combining encoded semantic feature factor $\mathbf{S}_i^{(t)}$ with behavior pattern feature factor $\mathbf{Y}_i^{(t)}$, which can be expressed as:

$$\mathcal{G}_i^{(t)} = \sigma_3 \left\{ \mathbf{Y}_1^{\mathrm{T}} \mathbf{S}_i^{(t)} \oplus \mathbf{Y}_2^{\mathrm{T}} \mathbf{Y}_i^{(t)} \right\} \tag{19}$$

where $\mathbf{Y}_1$ and $\mathbf{Y}_2$ are two mapping matrices that match the dimensions of those two factors and $\oplus$ denotes the concatenation operation. Thus far, the collaborative feature matrices of user u_i at different timestamps constitute a time-series feature sequence. This subsection manages to model the time-varying evolution of collaborative feature embedding $\mathcal{G}_i^{(t)}$ with the utilization of the LSTM, whose architecture is shown in Fig. 4. At each timestamp, it takes both the collaborative feature embedding $\mathcal{G}_i^{(t)}$ and the status output from previous timestamp $\mathcal{O}_i^{(t-1)}$ as inputs. Status encoding is output after the processing of three main components: the forget gate, input gate and output gate.

The control factor of the forget gate at the t-th timestamp is computed as:

$$\boldsymbol{f}_i^{(t)} = \sigma_4 \left\{ \mathbf{W}_{if} \left[\mathcal{O}_i^{(t-1)}, \mathcal{G}_i^{(t)} \right] + \boldsymbol{b}_{if} \right\} \tag{20}$$

where $\mathbf{W}_{if}$ and $\boldsymbol{b}_{if}$ are the weight matrix and bias matrix, $\mathcal{O}_i^{(t-1)}$ is the encoding output of the previous timestamp, and $\sigma_4(\cdot)$ is the sigmoid activation function:

$$\sigma_4(x) = \frac{1}{1 + e^{-x}} \tag{21}$$

The cell state factor of the input gate at the timestamp is computed as:

$$\boldsymbol{\mathcal{V}}_i^{(t)} = \sigma_4\left\{\boldsymbol{W}_{i\mathcal{V}}\left[\boldsymbol{O}_i^{(t-1)}, \boldsymbol{G}_i^{(t)}\right] + \boldsymbol{b}_{i\mathcal{V}}\right\} \tag{22}$$

$$\widetilde{\boldsymbol{\mathcal{Z}}}_i^{(t)} = \sigma_2\left\{\boldsymbol{W}_{i\mathcal{Z}}\left[\boldsymbol{O}_i^{(t-1)}, \boldsymbol{G}_i^{(t)}\right] + \boldsymbol{b}_{i\mathcal{Z}}\right\} \tag{23}$$

$$\boldsymbol{\mathcal{Z}}_i^{(t)} = \boldsymbol{f}_i^{(t)}\boldsymbol{\mathcal{Z}}_i^{(t-1)} + \boldsymbol{\mathcal{V}}_i^{(t)}\widetilde{\boldsymbol{\mathcal{Z}}}_i^{(t)} \tag{24}$$

where $\boldsymbol{W}_{i\mathcal{V}}$ and $\boldsymbol{W}_{i\mathcal{Z}}$ are weight matrices and $\boldsymbol{b}_{i\mathcal{V}}$ and $\boldsymbol{b}_{i\mathcal{Z}}$ are bias parameters.

The control factor of the output gate at the t-th timestamp is computed as:

$$\boldsymbol{O}_i^{(t)} = \sigma_4\left\{\boldsymbol{W}_{i\mathcal{O}}\left[\boldsymbol{O}_i^{(t-1)}, \boldsymbol{G}_i^{(t)}\right] + \boldsymbol{b}_{i\mathcal{O}}\right\} \cdot \sigma_2\left[\boldsymbol{\mathcal{Z}}_i^{(t)}\right] \tag{25}$$

where $\boldsymbol{W}_{i\mathcal{O}}$ and $\boldsymbol{b}_{i\mathcal{O}}$ are the weight matrix and bias parameter, respectively. Output matrix $\boldsymbol{O}_i^{(T)}$ is the final output of the LSTM for user u_i at the last timestamp T.

For spammer detection as a binary classification scheme, a sigmoid function-based attentive expression is introduced here to predict the nature of users:

$$\boldsymbol{\mathcal{F}}_i = \sigma_4\left\{\boldsymbol{W}_{i\mathcal{F}}\sigma_3\left[\boldsymbol{O}_i^{(T)}\right] + \boldsymbol{b}_{i\mathcal{F}}\right\} \tag{26}$$

where $\boldsymbol{W}_{i\mathcal{F}}$ and $\boldsymbol{b}_{i\mathcal{F}}$ are the weight matrix and bias vector, respectively. The values of $\mathcal{F}_i$ are located in the range of $(0,1)$, and Shannon entropy is adopted here to set up the following optimization objective:

$$\mathcal{L} = \frac{1}{|u|}\sum_{i=1}^{|u|}\left[\lambda\left\|\mathcal{F}_i - \hat{\mathcal{F}}_i\right\|^2 + (1-\lambda)\|\Theta\|^2\right] \tag{27}$$

where $|u|$ is the number of users, $\hat{\mathcal{F}}_i$ is the nature of the observed user, and Θ is the set of parameters that can be searched through the following iterative procedure:

$$\Theta^{(l+1)} = \Theta^{(l)} - 2\lambda\left(\mathcal{F}_i - \hat{\mathcal{F}}_i\right)\frac{\partial \mathcal{F}_i}{\partial \Theta^{(l)}} - 2(1-\lambda)\Theta^{(l)} \tag{28}$$

IV. EXPERIMENTS AND ANALYSIS

A. Datasets

TABLE III
LISTS OF BEHAVIOR PATTERNS

Behavior Types	Behavior Pattern Names
Personal Behaviors	Authentication Status
	Personal Profile
	Registration Time
	User Level
	Personal Tags
Interactive Behaviors	Vector of Social Relations
	Number of Speeches
	Originality of Speeches
	Sequential Relevance of Speeches
	Frequency of Comments
	Frequency of Obtained Comments
	Forwarding Frequency
	Forwarded Frequency

TABLE II
EVALUATION METRICS

Metrics	Expressions
Precision	$\dfrac{\psi(TP)}{\psi(TP) + \psi(FP)}$
Recall	$\dfrac{\psi(TP)}{\psi(TP) + \psi(FN)}$
Accuracy	$\dfrac{\psi(TP) + \psi(TN)}{\psi(TP) + \psi(FP) + \psi(TN) + \psi(FN)}$
F-Score	$\dfrac{2 \cdot Precision \cdot Recall}{Precision + Recall}$
AUC	$\dfrac{\sum_{i \in posi} K(i) - \psi(POS)[\psi(POS) + 1]/2}{\psi(POS)\psi(NEG)}$

Twitter and Sina Weibo, two universally acknowledged social network data sources, are utilized in this research for experimental evaluation, given that there are no datasets of IoT-based social media that are publicly available and related data are still hard to acquire due to the imperfect functions of applications. Two datasets with respect to these two platforms are briefly described as follows:

Twitter[1]—This dataset was collected by Yang *et al.* [35] and crawled from the Twitter website with the aid of the official API. The dataset contains 11000 labeled users as well as their records of tweets and behaviors, with 1000 being marked as spammers. In addition, the dataset includes metadata such as personal profiles, authentication statuses, social relationships, identity information and locations.

Weibo[2]—We utilized the Weibo API to collect the metadata and activity records of 6072 relatively active users in June 2019. Five graduate students were assigned to label all of these Weibo users according to artificial experience. For inconsistent labeling, the label endorsed by the majority was selected as the final label. In total, 1158 users were marked as spammers. In addition, this dataset involves metadata such as social relationships, blog contents, personal profiles and identity

TABLE IV
BASELINES

Metrics	Expressions
LDA+K-means	Topic model LDA is used to extract the semantic features of users. In addition, spammers can be detected through a K-means clustering algorithm. [26]
Bi-AE+LR	The semantic features of users are represented by Bi-AE, as described in Section III.A. In addition, spammers are detected by logistic regression (LR).
SVM	Behavior pattern features are extracted and encoded as Co-Spam. In addition, spammers are detected by a support vector machine (SVM).
CNN	Behavior pattern features are encoded as Co-Spam. In addition, spammers are detected by a convolutional neural network (CNN).
NMF	The features of semantic behavior patterns and semantics are encoded. Spammers are detected by nonnegative matrix factorization (NMF). [15]

[1] http://faculty.cse.tamu.edu/guofei/research_release.html
[2] This dataset will be released publicly after related programs are completed.

TABLE V
PRECISION AND RECALL RESULTS UNDER DIFFERENT PROPORTIONS OF TRAINING DATA

| Metrics	Algorithms	Twitter Dataset			Weibo Dataset		
		50% Training	60% Training	70% Training	50% Training	60% Training	70% Training
Precision	LDA+ K-means	0.8610	0.8736	0.8948	0.8420	0.8299	0.8742
	Bi-AE+LR	0.8805	0.8860	0.9059	0.8485	0.8444	0.8945
	SVM	0.8988	0.8932	0.9186	0.8763	0.8580	0.8856
	CNN	**0.9306**	0.9033	0.9315	0.8676	0.8676	0.8838
	NMF	0.9165	0.9249	0.9235	0.8759	0.8714	0.9048
	Co-Spam	0.9248	**0.9348**	**0.9432**	**0.8871**	**0.8830**	**0.9210**
Recall	LDA+ K-means	0.8340	0.8650	0.8800	0.8345	0.8899	0.8802
	Bi-AE+LR	0.8580	0.8767	0.9100	0.8500	0.8826	0.8877
	SVM	0.8600	0.8850	0.9042	0.8724	0.9072	0.8815
	CNN	0.8820	0.9167	0.9143	0.8655	0.9058	0.8975
	NMF	0.8960	0.9117	0.9242	0.8810	0.9130	0.9086
	Co-Spam	**0.9120**	**0.9367**	**0.9443**	**0.8913**	**0.9406**	**0.9443**
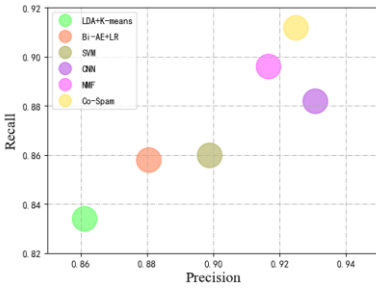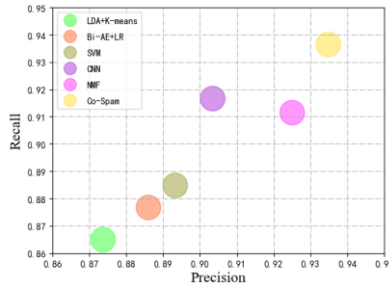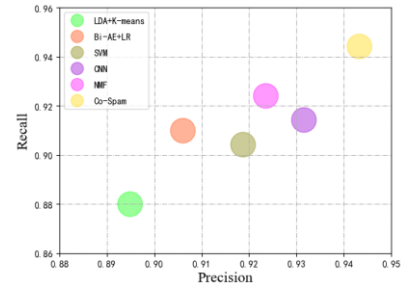
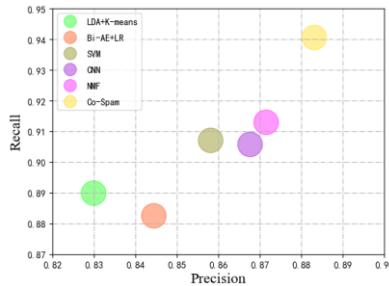(a) 50% for training   (b) 60% for training   (c) 70% for training
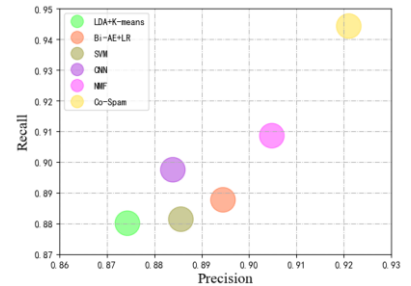
Fig. 5. Joint relations between precision and recall based on the Twitter dataset with respect to three sizes of training data.
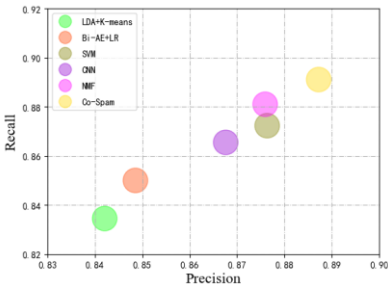
(a) 50% for training   (b) 60% for training   (c) 70% for training

Fig. 6. Joint relations between precision and recall based on the Weibo dataset with respect to three sizes of training data.

information.

Every tweet or blog of each user, as well as the behaviors occurring close to it, is viewed as a record of his or her activity associated with one timestamp. To virtualize the scenarios of this research, the behavior attributes are expanded and listed in TABLE III.

B. Experimental Settings

Spammer detection is a binary classification process in which spammers and normal users are labeled 1 and 0, respectively. To measure the classification performance of detection methods, four conceptions are introduced. True positive (TP) and false positive (FP) are defined as samples that are correctly and incorrectly predicted to be positive, respectively. Similarly, true negative (TN) and false negative (FN) are defined as samples that are correctly and incorrectly predicted to be negative, respectively. Thus, the expressions of the five evaluation metrics utilized in our experiments are mathematically defined in TABLE II. Among them, POS and NEG denote positive and negative samples, $\psi(\cdot)$ denotes the counting operation, and $K(\cdot)$ denotes the returning index number.

Five typical classification methods, which are described in TABLE IV, are selected as baselines to be compared with the proposed Co-Spam. To assess effect of collaborative awareness of semantic pattern and behavioral pattern, the two factors are
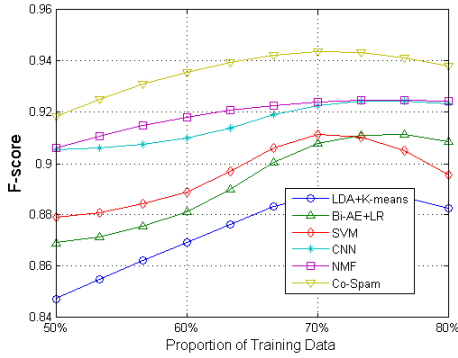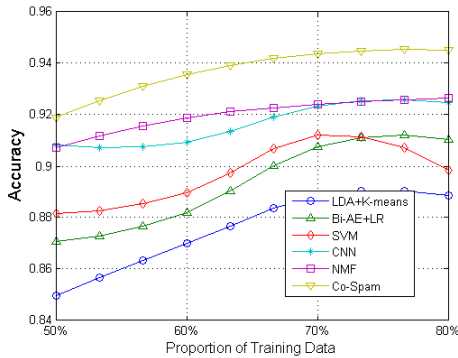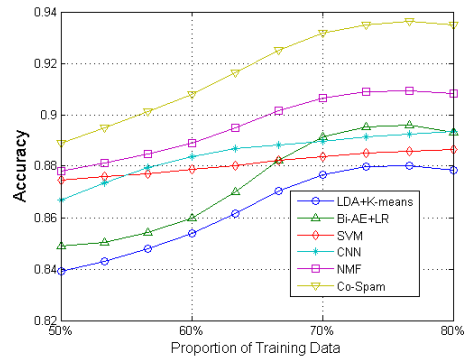
(a) Results based on the Twitter dataset
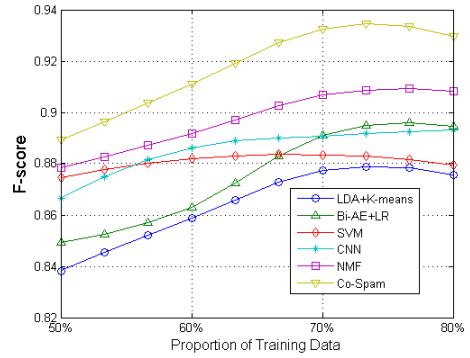
(b) Results based on the Weibo dataset

Fig. 7. F-score results based on two datasets with respect to four sizes of training data.
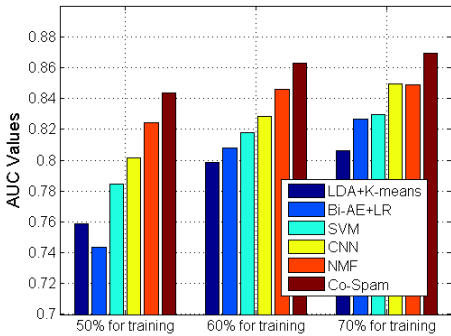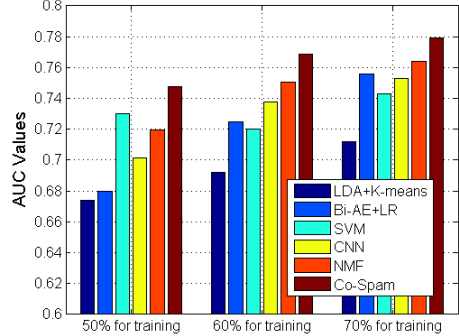

(a) Results based on the Twitter dataset

(b) Results based on the Weibo dataset

Fig. 8. Accuracy results based on two datasets with respect to four sizes of training data.

(a) Results based on the Twitter dataset

(b) Results based on the Weibo dataset

Fig. 9. AUC results on two datasets with respect to four training sizes.

fully considered while selecting baselines. The first two methods are semantic pattern-based detection approaches, while the intermediate two methods are behavioral pattern-based detection approaches. The last one took both of two factors into consideration, but neglected long-term characteristics.

The development environment of the experiments involves a deep learning workstation with a 28-core CPU and 256 GB of memory. The proposed Co-Spam is implemented with the aid of TensorFlow. In one sentence, topic words and background words are sampled through the proportion of 60% and 40%, respectively. Initially, the batch size of Co-Spam was set to 200, and the SGD learning rate was set to 0.01, where the trade-off parameters τ of Eq. (10) and λ of Eq. (27) were set to 0.5. The ratio of training data was initially set to 70% and was changed

multiple times during the experiments.

C. Results and Analysis

TABLE V lists the experimental results based on two datasets under different proportions of training data with respect to two metrics: precision and recall. It can be intuitively observed that the proposed Co-Spam always performs better than the baselines with different proportions of training data, 50%, 60% and 70%. Fig. 5 and Fig. 6 demonstrate the joint relations between precision and recall based on two datasets through six scatter diagrams, in which a larger distance between a scatter and the origin indicates better performance of such a method. This group of experiments is able to effectively reflect the advantages of collaborative awareness between semantic and behavior patterns because the relatively global

view certainly provides a considerable improvement of detection precision. It is also noticed that Co-Spam failed to obtain the best performance on Twitter when training size is 50%. As the training size is small, the Co-Spam may not be well trained yet. This fact is likely to bring some uncertainty.

Fig. 7 and Fig. 8 illustrate the F-score results and accuracy results, respectively, based on two datasets with respect to four proportions of training data, in which the proportion of 80% is further taken into consideration. Two aspects of this phenomenon can be deduced from these figures. First, most methods obtain relatively ideal results when the proportion of training data is set to 70%, and they perform better than when the proportion of training data is set to 80%. Second, the proposed Co-Spam always performs dramatically better than the baselines, regardless of the proportion of training data. The above results can be attributed to the fact that the Co-Spam method collaboratively exploits the characteristics of semantic and behavior patterns. Such a comprehensive insight promotes the depth of the feature space and will certainly improve the results compared with general spammer detection methods. The two subfigures in Fig. 9 show the AUC results of the Co-Spam and baselines obtained based on two datasets with respect to three sizes of training data: 50%, 60% and 70%. This group of experimental results reflects the relatively stable performance with the changing tendency of the Co-Spam and baselines. Overall, behavior-based methods perform better than semantic-based methods but worse than methods jointly driven by both semantic and behavior patterns. Compared with the NMF method based on both types of factors, the proposed Co-Spam still shows better performance. This group of experimental results evaluated the excellent performance of the proposed Co-Spam again. In addition to the collaborative awareness of semantic and behavior patterns, it also takes the evolving nature of social activities into account, which is the main reason the results above were obtained.

In summary, the proposed Co-Spam is able to obtain an improvement of approximately 5% compared with existing mainstream spammer detection approaches. It is undeniable that time complexity of Co-Spam is quite large, because its model has a large number of parameters. Therefore, price of good detection precision is the time complexity.

V. CONCLUSIONS

The past decade has witnessed great progress in the IoT, which has become an essential component in future smart cities. However, the emergence of spamming problems in IoT-based social media applications is posing increasingly serious security threats to IoT cyberspace. To that end, effective spammer detection methods have been a major concern in academia. Existing research can be divided into two types: semantic pattern-based approaches and behavior pattern-based approaches. However, all such approaches suffer from some drawbacks or limitations to some extent. To tackle this challenge, this paper leverages the collaborative awareness of these two factors and proposes a novel spammer detection mechanism named Co-Spam for future IoT applications. First, the speech contents and behavior records of a user at different

timestamps are viewed as feature sequences. Then, a collaborative neural network architecture composed of three neural network models, a Bi-AE, a GCN and the LSTM, is developed to identify the nature of the user. Finally, a series of experiments are conducted to verify the efficiency of the proposed Co-Spam. At the same time, running time of the Co-Spam is longer than general baselines. This is because a huge amount of parameters are introduced to construct more fine-grained feature space. The obtainment of relative ideal detection precision is taken high computational complexity as price. This is one major direction in the future researches.

REFERENCES

[1]   X. Zhang, L. Yang, Z. Ding, J. Song, Y. Zhai, and D. Zhang, "Sparse Vector Coding-based Multi-Carrier NOMA for In-Home Health Networks," *IEEE J. Sel. Areas Commun.* (accept on 15 March, 2020).

[2]   F. Ahmad *et al.*, "Blockchain in Internet-of-Things: Architecture, Applications and Research Directions," in *Proc. of 2019 International Conference on Computer and Information Sciences,* Sakaka, Saudi Arabia, 2019, pp. 1-6.

[3]   Z. Wu *et al.*, "hPSD: A hybrid PU-learning-based spammer detection model for product reviews," *IEEE Trans. Cybern.,* 2018. vol. 50, no.4, pp. 1595-1606, 2020.

[4]   M. Fazil, M. Abulaish, "A hybrid approach for detecting automated spammers in twitter," *IEEE Trans. Inf. Forensics and Security,* vol. 13, no.11, pp. 2707-2719, 2018.

[5]   S. Rathore, V. Loia, J. H. Park, "SpamSpotter: an efficient spammer detection framework based on intelligent decision support system on facebook," *Appl. Soft Comput.,* vol. 67, pp. 920-932, 2018.

[6]   J. Cao *et al.*, "Collusion-aware detection of review spammers in location based social networks," *World Wide Web,* vol. 22, no.6, pp. 2921-2951, 2019.

[7]   H. Chen *et al.*, "Semi-supervised clue fusion for spammer detection in Sina Weibo," *Inf. Fusion,* vol. 44, pp. 22-32, 2018.

[8]   S. Shehnepoor *et al.*, "NetSpam: A network-based spam detection framework for reviews in online social media," *IEEE Trans. Inf. Forensics and Security,* vol. 12, no.7, pp. 1585-1595, 2017.

[9]   M. Alazab, R. Broadhurst, "Spam and criminal activity". *Trends and Issues in Crime and Criminal Justice (Australian Institute of Criminology),* vol. 52, pp. 1-20, 2016.

[10] A. Li *et al.*, "Spam Review Detection with Graph Convolutional Networks," in *Proc. of the 28th ACM International Conference on Inf. and Knowl. Manag.,* Beijing, China, 2019, pp. 2703-2711.

[11] Z. Wang *et al.*, "Graph-based review spammer group detection," *Knowl. and Inf. Systems,* vol. 55, no.3, pp. 571-597, 2017.

[12] Q. Dang *et al.*, "Detecting cooperative and organized spammer groups in micro-blogging community," *Data Mining and Knowl. Discovery,* vol. 31, no.3, pp. 573-605, 2017.

[13] Y. Liu, B. Pang, "A unified framework for detecting author spamicity by modeling review deviation," *Expert Syst. With Appl.,* vol. 112, pp. 148-155, 2018.

[14] H. Fu *et al.*, "Robust spammer detection in microblogs: Leveraging user carefulness," *ACM Trans. Intell. Syst. and Technol.,* vol. 8, no.6, pp. 1-31, 2017.

[15] D. Yu *et al.*, "Constrained NMF-based semi-supervised learning for social media spammer detection," *Knowledge-Based Syst.,* vol. 125, no.1, pp. 64-73, 2017.

[16] M. Yang, *et al.*, "Detecting review spammer groups," in *Proc. of the Thirty-First AAAI Conference on Artificial Intelligence,* San Francisco, California, USA, 2017, pp. 5011-5012.

[17] R. Vinayakumar *et al.,* "Deep Learning Approach for Intelligent Intrusion Detection System," *IEEE Access,* vol. 7, pp. 41525-41550, 2019.

[18] C. Li *et al.*, "SSDMV: Semi-supervised deep social spammer detection by multi-view data fusion," in *Proc. of the 2018 IEEE International Conference on Data Mining,* Singapore, 2018, pp. 247-256.

[19] F. Wu, C. Wu, J. Liu, "Semi-Supervised Collaborative Learning for Social Spammer and Spam Message Detection in Microblogging," in *Proc. of the 27th ACM International Conference on Inf. and Knowl. Manag.,* Torino, Italy, 2018, pp. 1791-1794.

[20] L. You *et al.*, "Integrating aspect analysis and local outlier factor for intelligent review spam detection," *Future Generation Computer Syst.,* vol. 102, pp. 163-172, 2020.

[21] C. Yuan *et al.*, "Learning review representations from user and product level information for spam detection," in *Proc. of IEEE International Conference on Data Mining,* Beijing, China, 2019, pp. 1444-1449.

[22] J. R. Méndez, T. R. Cotos-Yañez, D. Ruano-Ordás, "A new semantic-based feature selection method for spam filtering," *Appl. Soft Comput.,* vol. 76, pp. 89-104, 2019.

[23] A. C. Pandey, D. S. Rajpoot, "Spam review detection using spiral cuckoo search clustering method," *Evolutionary Intelligence,* vol. 12, no.2, pp. 147-164, 2019.

[24] M. Alazab*,* "Profiling and classifying the behavior of malicious codes," *J. Syst. and Softw.*, vol. 100, pp. 91-102, 2015.

[25] Y. Liu, B. Pang, X. Wang, "Opinion spam detection by incorporating multimodal embedded representation into a probabilistic review graph," *Neurocomputing*, vol. 366, pp. 276-283, 2019.

[26] Z. Wang, S. Gu, X. Xu, "GSLDA: LDA-based group spamming detection in product reviews," *Appl. Intelligence,* vol. 48, no.9, pp. 3094-3107, 2018.

[27] M. Bao *et al.*, "Learning Semantic Coherence for Machine Generated Spam Text Detection," in *Proc. of 2019 International Joint Conference on Neural Netw.,* Budapest, Hungary, 2019, pp. 1-8.

[28] L. Li *et al.*, "Document representation and feature combination for deceptive spam review detection," *Neurocomputing,* vol. 254, pp. 33-41, 2017.

[29] H. He *et al.*, "A new semantic attribute deep learning with a linguistic attribute hierarchy for spam detection," in *Proc. of 2017 International Joint Conference on Neural Netw.,* Anchorage, AK, USA, 2017, pp. 3862-3869.

[30] T. A. Almeida *et al.*, "Text normalization and semantic indexing to enhance instant messaging and SMS spam filtering," *Knowledge-Based Syst.,* vol. 108, pp. 25-32, 2016.

[31] C. Yuan *et al.*, "Jointly embedding the local and global relations of heterogeneous graph for rumor detection," in *Proc. of 2019 IEEE International Conference on Data Mining,* Beijing, China, 2019, pp. 796-805.

[32] X. Wang, K. Liu, J. Zhao, "Handling cold-start problem in review spam detection by jointly embedding texts and behaviors," in *Proc. of the 55th Annual Meeting of the Association for Computational Linguistics,* Vancouver, Canada, 2017, pp. 366-376.

[33] Z. Cui *et al.*, "Dressing as a whole: Outfit compatibility learning based on node-wise graph neural networks," in *Proc. of the 28th World Wide Web Conference,* San Francisco, CA, USA, 2019, pp. 307-317.

[34] Ayrat Khalimov *et al.*, "Container-based Sandboxes for Malware Analysis: A Compromise Worth Considering," in *Proc. of the 12th IEEE/ACM International Conference on Utility and Cloud Computing,* Auckland, New Zealand, 2019, pp. 219-227.

[35] C. Yang, R. Harkreader, G. Gu, "Empirical evaluation and new design for fighting evolving twitter spammers," *IEEE Trans. Inf. Forensics and Security,* vol. 8, no.8, pp. 1280-1293, 2013.

Zhiwei Guo received the B.E. degree from Zhengzhou University, Zhengzhou, China, in 2013, and the Ph.D. degree from Chongqing University, Chongqing, China, in 2018. He is currently an Assistant Professor with Chongqing Technology and Business University, Chongqing, China. In 2017, he gave an oral presentation in the International Joint Conference on Artificial Intelligence (IJCAI 2017). His research interests focus on applications of data mining and pattern recognition in the Internet of Things.

Yu Shen received the B.E. degree from Huazhong Agricultural University, Wuhan, China, in 2004, and Ph.D. degree from Dalian University of Technology, Dalian, China, in 2009. He is currently a Researcher with Chongqing Technology and Business University, and has led or is leading three national projects of China. His research interests include intelligent control and Internet of Things.

Ali Kashif Bashir (Senior Member, IEEE) is a Senior Lecturer at the Department of Computing and Mathematics, Manchester Metropolitan University, United Kingdom. He is also holding Adjunct Professor Position at National University of Science and Technology, Pakistan. He is a senior member of IEEE, invited member of IEEE Industrial Electronic Society, member of ACM, and Distinguished Speaker of ACM. His past assignments include Associate Professor of ICT, University of the Faroe Islands, Denmark; Osaka University, Japan; Nara National College of Technology, Japan; the National Fusion Research Institute, South Korea; Southern Power Company Ltd., South Korea, and the Seoul Metropolitan Government, South Korea. He has worked on several research and industrial projects of South Korean, Japanese and European agencies and Government Ministries.

He received his Ph.D. in computer science and engineering from Korea University South Korea. He has authored over 140 research articles and is supervising/co-supervising several graduate (MS and PhD) students. His research interests include internet of things, wireless networks, distributed systems, network/cyber security, cloud/network function virtualization, machine learning, etc. He is serving as the Editor-in-chief of the IEEE FUTURE DIRECTIONS NEWSLETTER. He is also serving as area editor of KSII Transactions on Internet and Information Systems; associate editor of IEEE Access, IET Quantum Computing. He is leading many conferences as a chair (program, publicity, and track) and had organized workshops in flagship conferences like IEEE Infocom, IEEE Globecom, IEEE Mobicom, etc.

Muhammad Imran is an Associate Professor in the College of Applied Computer Science at King Saud University, Saudi Arabia. He received a Ph. D in Information Technology from the University Teknologi PETRONAS, Malaysia in 2011. His research interest includes Mobile and Wireless Networks, Internet of Things, Big Data Analytics, Cloud computing, and Information Security. His research is financially supported by several national and international grants. He has completed a number of international collaborative research projects with reputable universities.

He has published more than 250 research articles in peer-reviewed, well-recognized international conferences and journals. Many of his research articles are among the highly cited and most downloaded. He served as an Editor in Chief for European Alliance for Innovation (EAI) Transactions on Pervasive Health and Technology. He is serving as an associate editor for top ranked international journals such as IEEE Communications Magazine, IEEE Network, Future Generation Computer Systems, and IEEE Access. He served/serving as a guest editor for about two dozen special issues in journals such as IEEE Communications Magazine, IEEE Wireless Communications Magazine, Future Generation Computer Systems, IEEE Access, and Computer Networks. He has been involved in about one hundred peer-reviewed international conferences and workshops in various capacities such as a chair, co-chair and technical program committee member. He has been consecutively awarded with **Outstanding Associate Editor of IEEE Access** in 2018 and 2019 besides many others.

journals, he has also published papers in some of the core conferences of his area of specialization such as-IEEE Globecom, IEEE ICC, IEEE Greencom, IEEE CSCWD. He has guided many research scholars leading to Ph.D. and M.E./M.Tech. His research is supported by funding from TCS, CSIT, UGC and UGC in the area of Smart grid, energy management, VANETs, and Cloud computing. He is member of the Cyber-Physical Systems and Security (CPSS) research group. He has research funding from DST, CSIR, UGC, and TCS. He has total research funding from these agencies of more than 2 Crores under different schemes from the GOI. Recently, he has also got International research projects under DST-research initiative. He has hindex of 53 (according to Google scholar, March 2020) with 9300 citations to his credit. He is editorial board members of ACM Computing Survey, IEEE Transactions on Sustainable Computing, Computer Communications, IEEE Network, IEEE Communication Magazine, International Journal of Communication Systems, Wiley, Security and Communication, John Wiley, and Journal of Networks and Computer Applications, Elsevier. He has visited many countries mainly for the academic purposes. He is a visiting research fellow at Coventry University, Coventry, UK, Charles Darwin University, Australia. He has many research collaborations with premier institutions in India and different universities across the globe. He has been engaged in different academic activities inside and outside the Institute. He has supervised 12 Ph.D. students and 5 are currently pursuing their thesis. He has also supervised more than 25 M.E./M.Tech. thesis. He is a Senior Member of the IEEE.

Neeraj Kumar received his Ph.D. in CSE from SMVD University, Katra (J & K), India, and was a postdoctoral research fellow in Coventry University, Coventry, UK. He is working as a Full Professor in the Department of Computer Science and Engineering, Thapar Institute of Engineering & Technology, Patiala (Pb.), India since 2014. Dr. Neeraj is an internationally renowned researcher in the areas of VANET & CPS Smart Grid & IoT Mobile Cloud computing & Big Data and Cryptography. He has published more than 400 technical research papers in leading journals and conferences from IEEE, Elsevier, Springer, John Wiley, and Taylor and Francis. His paper has been published in some of the high impact factors journals such as-IEEE Transactions on Industrial Informatics, IEEE Transactions on Industrial Electronics, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Power Systems, IEEE Transactions on Vehicular Technology, IEEE Transactions on Smart Grid, IEEE Journal of Biomedical and Health Informatics, IEEE Access, IEEE Transactions on Consumer Electronics, IEEE Systems Journal, IEEE IoT Journal, IEEE Wireless Communication Magazine, IEEE Vehicular Technology Magazine, IEEE Communication Magazine, IEEE Networks Magazine etc. Apart from the

Di Zhang received the M.Sc. (Hons.) degree from Central China Normal University, Wuhan, China, in 2013, and the Ph.D. (Hons.) degree from Waseda University, Tokyo, Japan, in 2017.

He is currently a Senior Researcher with the Information System Laboratory, Department of Electrical and Computer Engineering, Seoul National University, Seoul, South Korea. He is also an Assistant Professor with Zhengzhou University, Zhengzhou, China. He visited the National Key Laboratory of Alternate Electrical Power System with Renewable Energy Sources, North China Electric Power University, in 2015–2017, and the Advanced Communication Technology Laboratory, National Chung Hsing University, in 2012. His research interests include 5G, Internet of Things, vehicle communications, green communications, and signal processing.

Dr. Zhang served as a Technical Program Committee member of several IEEE conferences such as the IEEE International Conference on Communications, the IEEE Wireless Communications and Networking Conference, the IEEE Vehicular Technology Conference, the IEEE Consumer Communications and Networking Conference, and the IEEE International Conference on e-Health Networking, Applications and Services.

Keping Yu received the M.E. and Ph.D. degrees from the Graduate School of Global Information and Telecommunication Studies, Waseda University, Tokyo, Japan, in 2012, and 2016, respectively.

He was a Research Associate and a Junior Researcher with the Global Information and Telecommunication Institute, Waseda University, from 2015 to 2019 and from 2019 to 2020, respectively, where he is currently a Researcher. He has hosted and participated in more than ten projects, is involved in many standardization activities organized by ITU-T and ICNRG of IRTF, and has contributed to ITU-T Standards Y.3071 and Supplement 35. His research interests include smart grids, information-centric networking, the Internet of Things, blockchain, and information security. He was the Chair of the IEEE/CIC ICCC 2nd EBTSRA workshop, the General Co-Chair and the Publicity Co-Chair of the IEEE VTC2020-Spring EBTSRA workshop, the TPC Co-Chair of the SCML2020, the Local Chair of the MONAMI 2020, the Session Co-Chair of the CcS2020, and the Session Chair of the ITU Kaleidoscope 2016. He has served as a TPC Member for more than ten international conferences, including ITU Kaleidoscope, the IEEE Vehicular Technology Conference (VTC), the IEEE Consumer Communications and Networking Conference (CCNC), and the IEEE Wireless Communications and Networking Conference (WCNC). He has been a Lead Guest Editor for Sensors, Peer-to-Peer Networking and Applications, and Energies. He is an Editorial Board Member of the IEEE OPEN JOURNAL OF VEHICULAR TECHNOLOGY (OJVT).