RoSeq: Robust Sequence Labeling
Joey Tianyi Zhou, Hao Zhang, Di Jin, Xi Peng, Yang Xiao, and Zhiguo Cao

Abstract—In this paper, we mainly investigate two issues for sequence labeling, namely, label imbalance and noisy data that are commonly seen in the scenario of named entity recognition (NER) and are largely ignored in the existing works. To address these two issues, a new method termed robust sequence labeling (RoSeq) is proposed. Specifically, to handle the label imbalance issue, we first incorporate label statistics in a novel conditional random field (CRF) loss. In addition, we design an additional loss to reduce the weights of overwhelming easy tokens for augmenting the CRF loss. To address the noisy training data, we adopt an adversarial training strategy to improve model generalization. In experiments, the proposed RoSeq achieves the state-of-the-art performances on CoNLL and English Twitter NER—88.07% on CoNLL-2002 Dutch, 87.33% on CoNLL-2002 Spanish, 52.94% on WNUT-2016 Twitter, and 43.03% on WNUT-2017 Twitter without using the additional data.

Index Terms—Label imbalance, named entity recognition (NER), sequence labeling.

I. INTRODUCTION

EXISTING multioutput learning mainly aims at determining multiple outputs for a given input. In many cases, the output often involves a structure that is helpful to the training models, e.g., sequences, strings, trees, lattices, or graphs. In order to infer the structured outputs from an observation sequence rather than a data point, label sequence learning or sequence labeling has been widely studied, where the output sequence has inherent interconnections rather than a simple concatenation of individual units. It is also an important step in the most natural language processing (NLP) applications and has been applied to numerous real-world tasks including but not limited to part-of-speech (POS) tagging [1], named entity recognition (NER) [2], [3], and speech recognition [4].

In these tasks, NER has attracted increasing interests, which detects not only the type of named entity but also the entity boundaries. To disambiguate different entity types of same tokens, NER needs a deep understanding of the contextual semantics. As shown in Fig. 1, for example, the token “California” in the first sentence is labeled as Location (LOC), whereas it is labeled as Miscellaneous (MISC) and organization (ORG) in the second and third sentences, respectively. To tackle this challenging problem, a variety of methods have been proposed, which are usually based on hand-crafted rules and have suffered from limited performance in practice [5]–[7]. Recent works have devoted to developing learning-based algorithms, especially neural network-based methods, which have remarkably advanced the state of the arts [1], [2], [8]–[11]. Furthermore, these end-to-end models generalize well on new entities based on features automatically learned from data.

Although deep learning-based methods have achieved significant progress, they ignore two important and commonly seen properties of existing NER data sets as follows.

1) The label distribution is extremely imbalanced. Take the CoNLL-2002 Dutch NER data set as a showcase [Fig. 2(a)], 90.48% data are with unmeaning entity “O.” Similarly, for the WNUT-2017 English Twitter NER data set, the label of “O” even occupies 94.62% of the entire data. [see Fig. 2(b)].

2) The data set is noisy. Like the WNUT data set collected from user-generated tweets, the NER data set is collected
from the social media and thus contains lots of noise, such as emojis, punctuation, incomplete or misspelled words, urls, unknown tokens, and so on. For example, here is a sentence from tweets in WNUT data set, “Soooo Glad its Finally Friday !!!! :P Thissss week went to slow fo’me :/.” Here, “Soooo” is misspelled and should be “So.” “fo’me” should be “for me.”

The first label imbalance issue severely affects the convergence performance of the NER models. In practice, the performance of these neural-based methods degrades significantly since the learned models favor the overwhelming label types. Here, we train one state-of-the-art (SOTA) neural network-based NER model (i.e., bidirectional long short term memory (LSTM) (BiLSTM)-convolutional neural networks (CNNs)-conditional random field (CRF) [10]) on WNUT-2017 data set and report its F1 scores of different entity types on the development set given in Table I. Note that for the NER task, the F1 score of unmeaning entity “O” does not be considered in the final result. However, we only compute F1 score of “O” for comparing with the rest meaningful entity types.

We observe that the dominant “O” label achieves more than 97% F1 score, whereas the other meaningful entity types such as “Group” and “Product” only achieve around 10% F1 score. In the experiment, we also find that those data with “O” label can be correctly classified with very high confidence. Unfortunately, in the NER task, we only care about the performance of those meaningful token types rather than the nonmeaningful “O” entity.

Most existing works ignore the noisy data issue and usually assume that the NER data are clean. In consequence, the noisy and untrimmed data affects performance significantly. For example, the F1 score on the clean NER data set such as CoNLL data set collected from news could easily reach over than 80%. In contrast, the noisy data sets such as WNUT are collected from Twitter, which is able to reach around 50% only. To the best of our knowledge, there are only few works that explicitly discuss and give an in-depth analysis of how to handle these noisy data in NER.

Based on the above-mentioned observations, we propose a novel learning algorithm, termed as robust sequence labeling (RoSeq), which focuses on how to handle label imbalance and noisy data issues in a single framework. Specifically, to handle the label imbalance issue, we propose a new label-aware CRFs (LACRF) algorithm which assigns different labels with different weights. Furthermore, inspired by the success of the focal loss (FL) [12] in solving object detection problem, we assign confidence-dependent weights to different samples so that the model will not be overwhelmed by such as the samples with “O” entity type in NER data sets. In other words, we add the FL to the aforementioned LACRF loss as the overall loss. On the other hand, to address the noisy data issue, we adopt the adversarial training (AT) to virtually create adversarial examples to improve the robustness of model training. The contributions of this paper could be summarized as follows.

1) To the best of our knowledge, this could be the first work to explicitly discuss the label imbalance and noisy data issues for sequence labeling. We find that the application of NER generally encounters these two issues.

2) We propose RoSeq to alleviate the overfitting and non-robust training problem caused by the label imbalance and noisy data. Specifically, RoSeq employs a word-level BiLSTM on the top of character-level and word embedding features to learn relevant high-level features in an end-to-end manner. Furthermore, a new objective function is proposed for RoSeq.

3) Extensive experimental results show the remarkable improvements over the SOTA NER models, especially in the case of imbalanced label. In brief, our method achieves SOTA performance on a series of NER benchmark data sets, namely, 87.33% F1 for CoNLL-2002 Spanish, 88.07% F1 for CoNLL-2002 Dutch, 52.94% F1 for WNUT-2016, and 43.03% F1 for WNUT-2017.

II. RELATED WORK

Our work is related to the following topics, i.e., NER and robust learning that are briefly introduced in this section.

A. Named Entity Recognition

NER is typically framed as a sequence labeling task that aims at automatic detection of named entities (e.g., person, organization, and location) from free text [13]. The early works are usually based on the hidden Markov model (HMM) [14], support vector machine (SVM) [15], CRF [16], or perception models with the hand-crafted features [5]–[7]. More specifically, they employed a system to read a large-scale annotated training data, memorize a list of entities, and create disambiguation rules based on discriminative features. Among them, CRFs and HMMs are very effective and have achieved SOTA performance in handling sequential data [1], [16]. Comparing with generative models (e.g., HMMs), discriminative models (e.g., CRFs) are usually more powerful, which aims at maximizing the conditional probability of the true label rather

![Fig. 2. Label statistics on CoNLL-2002 Dutch NER and WNUT-2017 English Twitter NER train set. The label type “O” is dominant in different data sets. (a) CoNLL-2002 Dutch Twitter NER train set. The label type “O” is dominant in different data sets. (b) WNUT-2017 English Twitter NER train set. The label type “O” is dominant in different data sets.](image-url)
than modeling the joint distribution. Thanks to impressive results achieved by CRFs, it has been widely used for handling sequential data in the scenario of NLP and biological sequence analysis.

Recent researches have shifted towards deep neural networks (DNNs) [2], [17]–[19]. Collobert et al. [8] proposed a feed-forward neural network with a fixed sized window for each word, but it failed in considering useful relations between long-distance words. To overcome this limitation, Chiu and Nichols [9] designed a BiLSTM-CNNs architecture that automatically detects word- and character-level features. Ma and Hovy [10] further extended [9] into BiLSTM-CNNs-CRF architecture wherein the CRF module is added to optimize the output label sequence. Liu et al. [20] proposed a task-aware neural language model (LM) termed as LM-LSTM-CRF which incorporates character-aware neural LMs to extract character-level embedding under a multitask framework. Yang et al. [21] proposed a transfer learning approach based on a deep hierarchical recurrent neural network (RNN) that utilizes the information from different lingual/domain data sets by fully or partially sharing the model parameters among different tasks. Ni and Florian [22] and Ni et al. [23] utilizes the Wikipedia entity-type mappings to improve low-resource NER. In addition, some recent works [24]–[29] show that multitask learning with joint training on multiple tasks/languages could improve its performance. Most recently, the pretrained LMs have also shown effectiveness in improving the performance of many NLP tasks [30], [31]. In this paper, we focus on solving the label imbalance and noisy data issues, thus we will not use any external resources nor knowledge transfer and will not investigate the performance with resource boosting methods.

B. Robust Learning

Imbalanced distribution is commonly seen in many nonNLP applications, especially in computer vision tasks such as object detection [12], segmentation [32], clustering [33], [34], and dimension reduction [35]. The fundamental issue with the imbalanced learning problem is the ability of the imbalanced data to significantly compromise the performance of most standard learning algorithms. There are many solutions [36] proposed to address this issue. Sampling methods [37] for imbalanced learning is one direction. Typically, the use of sampling methods in imbalanced learning applications consists of the modification of an imbalanced data set by some mechanisms in order to provide a balanced distribution. Sampling methods attempt to balance distributions by considering the representative proportions of class examples in the distribution. Studies [37] have shown that a balanced data set could improve the overall classification performance compared to an imbalanced data set for several base classifiers. Cost-sensitive methods [38] for imbalanced learning is another branch, which consider the costs associated with misclassifying or overwhelming easy samples [36]. Although the class imbalance problem has been discussed for years, the investigation of it on the task of NER is still limited.

To achieve robustness from noisy data, early works eliminate the effectiveness of noise using feature selection [39] and stochastic optimization [40]. In recent, AT [41], [42] is proposed to improve the robustness of image classification model by injecting malicious perturbations into input images. In the NLP community, Miyato et al. [43] proposed a semi-supervised text classification method by applying AT, where for the first time adversarial perturbations were added onto word embeddings. Yasunaga et al. [44] applied AT to POS tagging. Although these methods achieve some improvements by deploying AT, their analysis is insufficient for noisy data. In this paper, we provide a more in-depth analysis why AT is workable on the noisy NLP data.

III. ROBUST SEQUENCE LABELING

A. Character-Level Feature Representation

Previous works have shown that character features can improve the NER performance by capturing morphological and semantic information [29]. In practice, character-level representation learning method could be roughly classified into two subjects: one is character-level BiLSTM (Char-BiLSTM) [2] and the other is character-level CNN (Char-CNN) [9], [10]. Reimers and Gurevych [45] have observed that the performance difference between the Char-BiLSTM and Char-CNN approaches is statistically insignificant on sequence labeling tasks, but Char-CNN approach has less parameters and is more competitive in running time and computation resources. Thus, our method adopts the Char-CNN approach as the character-level encoder to learn character representation for each word.

To build the character-level feature representation encoder, let C and dc denote the character vocabulary and the dimension of character embeddings, respectively. Let the word w consist a sequence of characters [c1, c2, ..., cn], its character-level representation is denoted by the matrix Cw ∈ Rdc×n, where n is the length of word w. Then, the Char-CNN is designed using multiple filters with different widths to learn the character-level feature for word w. Typically, let F ∈ Rdc×k be a convolutional filter with width k and bF be the bias term, the feature map Fw ∈ Rn−k+1 is obtained by applying a convolution between Cw and F as follows:

\[
\text{F}_w[i] = \text{tanh}((C_w[:, i : i + k - 1], F) + b_F)
\]

(1)

where (·, ·)F denotes the Frobenius inner product and Fw[i] represents the i-th element of Fw. With the following formula, we use the max-pooling to capture the most important feature as the representation of w corresponding to the kernel F.

\[
\text{e}_w = \max_i F_w[i].
\]

(2)

Since our Char-CNN contains multiple filters, suppose we have m filters F1, F2, ..., Fm, thus, the final character-level feature representation of word w is e_w = [e_{F1}, e_{F2}, ..., e_{Fm}]. In other words, the concatenation of features is obtained by different filters.

Instead of using the obtained character-level feature representation e_w of word w for the further process directly, Kim et al. [46] indicate that running e_w through the highway networks is able to obtain the improvements on LMs. The highway network [47] optimizes the neural networks and increases their depth by using the learned gating mechanisms...
to regulate information flow. In other words, similar to the memory cell in LSTM, highway networks allow for training of deep networks by adaptively carrying some dimensions of the input directly to the output [46].

Formally, highway network consists of a feed-forward layer and two nonlinear transformations (i.e., transform gate and carry gate), where the former applies an affine transform followed by a nonlinear activation function to learn new features and the transformations express how much of the output is produced by transforming the input and carrying it. By applying highway network on the character-level feature representation, we have

$$z = t \odot g(W_{e}e^{o} + b_{e}) + (1 - t) \odot e^{o}$$  \hspace{1cm} (3)$$

where $g$ is a nonlinear activation function. In our implementation, we use the tanh function. $t = \sigma(W_{T}e^{o} + b_{T})$ is the transform gate, $1 - t$ denotes the carry gate, $\sigma$ denotes the Sigmoid activation function, and $z$ is the output of highway network. As the dimensions of $e^{o}$ and $z$ are required be consistent, $W_{e}$ and $W_{T}$ are two square matrices. Generally, we adopt two layers of highway network at the top of Char-CNN and denote $e^{\text{char}}$ as the final character-level feature representation of a word. The structure of the character-level encoder is shown in Fig. 4.

In this section, we introduce the proposed RoSeq model in details. Fig. 3 shows the architecture of the RoSeq model, which consists of character-level encoder, word-level encoder, label decoder, and adversarial training module.

B. Word-Level Feature Representation

To learn a better word-level representation, we concatenate character-level features of each word with a latent word embedding as $e_{j} = [e^{\text{char}}_{j}, e^{\text{word}}_{j}]$, where the latent word embedding $e^{\text{word}}$ is initialized with pretrained embeddings and fixed during training. One unique characteristic of NER is that the historical and future input for a given time step could be useful for label inference. To exploit such a characteristic, we use a BiLSTM [48] to extract contextualized word-level features. LSTM is a variant of RNN, which is capable of learning long-term dependencies and coping with the gradient vanishing and exploding problems. Basically, the LSTM unit is similar to the RNN unit, except that the hidden layer updates are replaced by purpose-built memory cells to control the proportions of information to forget and to pass to the next time step.

Formally, the formulas to update a LSTM unit at time $t$ are

$$i_{t} = \sigma(W_{i}h_{t-1} + U_{i}e_{t} + b_{i})$$

$$f_{t} = \sigma(W_{f}h_{t-1} + U_{f}e_{t} + b_{f})$$

$$c_{t} = \tanh(W_{c}h_{t-1} + U_{c}e_{t} + b_{c})$$

$$o_{t} = \sigma(W_{o}h_{t-1} + U_{o}e_{t} + b_{o})$$

$$h_{t} = o_{t} \odot \tanh(c_{t})$$

where $\sigma$ is the Sigmoid activation function and $\odot$ represents the elementwise product. $i_{t}$, $f_{t}$, and $o_{t}$ are the input gate, forget gate, and output gate, respectively. $e_{t}$ represents the input instance at the time stamp $t$ and $h_{t}$ is the corresponding hidden state (also called output) at time $t$. $W_{e}$ denotes the weight for hidden state $h_{t}$, $U_{i}$ represents the weight of different gates for input $e_{t}$, and $b_{i}$ denotes the bias.

The hidden state $h_{t}$ of LSTM is capable of taking information from left (past) contexts but cannot take information from right (future) contexts. However, it is beneficial to have access to both past and future contexts for sequence labeling tasks. Therefore, we introduce BiLSTM that represents the input sequence forwards and backwards as two separate hidden states so that the past and future information are learned. Specifically, let $h_{t} = \text{lstm}(h_{t-1}, e_{t})$ denote the hidden state update process of unidirectional LSTM for a particular time frame. In this way, for the BiLSTM, we have

$$\overrightarrow{h}_{t} = \text{lstm}(\overrightarrow{h}_{t-1}, e_{t})$$

$$\overleftarrow{h}_{t} = \text{lstm}(\overleftarrow{h}_{t+1}, e_{t})$$

where $\overrightarrow{h}_{t}$ and $\overleftarrow{h}_{t}$ are the learned left context (forward) and right context (backward) representations, respectively. After the BiLSTM layer, the final representation of a word is obtained by fusing its left and right context representations, we apply a nonlinear layer for this process as

$$h_{t} = \tanh(W_{l}\overrightarrow{h}_{t} + W_{r}\overleftarrow{h}_{t} + b)$$  \hspace{1cm} (6)$$

Note that, the representation integrates both local and global information, which could capture contextually sensitive signals across sequences.

C. Label Decoder

For the sequence labeling tasks, dependencies or correlations between labels in neighborhoods are crucial to disambiguate different entity types of each word. Therefore, it is promising and helpful to utilize the correlations and decode the best chain of labels for a given input sequence so that the resulting label sequence could be meaningful. For instance, in the NER task with standard BIO2 annotation scheme [49], I-LOC is illegal to follow B-ORG (mixing different annotation types), B-PER cannot follow another B-PER (wrong annotation dependence), and so on. CRF is a widely used method to make joint labeling of the tokens in a sequence [16], hence, we use a linear-chain CRF as label decoder to capture the relationships of labels and model the label sequence jointly, instead of predicting each label independently.

In the CRF decoder, there are two kinds of cliques, namely, local cliques and transition cliques, where local cliques correspond to the individual elements in the sequence, whose representation is $h_{t}$, as defined in (6), and transition cliques, on the other hand, reflect the evolution of states between the neighboring elements. Formally, let $h = \{h_{1}, h_{2}, \ldots, h_{T}\}$ represents a generic representation sequence where $h_{t}$ is the representation vector of the $t$th word and $y = \{y_{1}, y_{2}, \ldots, y_{T}\}$ denotes a generic sequence of labels for $h$, hence the probabilistic model for linear-chain CRF defines a family of conditional probability $p(y|h)$ over all possible label sequences $y$ given $h$ can be written as

$$p(y|h) = \frac{\exp \left\{ \sum_{t=2}^{T} \theta_{y_{t-1}, y_{t}} + \sum_{t=1}^{T}(W_{y}h_{t} + b_{y}) \right\}}{Z(h)}$$  \hspace{1cm} (7)$$
where \( Z(\mathbf{h}) \) is an instance-specific normalization function and \( \theta \) indicates a transition matrix that contains transition probabilities, i.e., \( \theta_{i,j} \) is the probability of transition \( (y_i, y_j) \).

Despite that linear-chain CRF takes the correlations between subsequent labels into consideration, however, it does not solve the problem of label imbalance in the sequence. In order to address this issue, we introduce a label-aware weight \( \xi \in \mathbb{R}^{[L]} \), where \([L]\) is the number of unique labels. The label-aware weight is a resource specific weight vector, which is derived from the statistical distribution of various label types in the resource data set, where a label with higher frequency tends to have lower weight. The idea of introducing this label-aware weight is to suppress the effect of massive but unmeaning label, i.e., "O" label, by reducing its contribution.

The idea of introducing this label-aware weight vector \( \xi \) is also equivalent to minimize the negative log-likelihood, and increasing the importance of other meaningful labels. Formally, we first calculate the label proportion for each label. Let \( \vartheta \in \mathbb{R}^{[L]} \) denote the label proportion of label \( Y_i \) (e.g., \( Y_i \in \{O, PER, LOC, ORG, MISC\} \)), the label-aware weight vector \( \xi \) is computed as

\[
\xi = \left( \frac{\max_{\vartheta \in [L]} \vartheta}{\vartheta} \right)^\tau
\]

(8)

where \( \vartheta = [\vartheta_1, \vartheta_2, \ldots, \vartheta_L]^{\top} \) and \( \tau \) is a scalar to adjust the magnitude of weight values. In this way, if the label proportion is higher, then the weight contribution is smaller. Hence, by employing the label-aware weight into the CRF, termed as LACRF, the (7) can be rewritten as

\[
\hat{p}(y|h) = \frac{\exp \{ \sum_{t=2}^{T} \vartheta_{y_{t-1}, y_t} + \sum_{t=1}^{T} \xi \cdot (W_y h_t + b_y) \}}{Z(\mathbf{h})}
\]

(9)

while \( Z(\mathbf{h}) \) is the corresponding normalization term after introducing the label-aware weight vector \( \xi \). Our objective is to maximize the conditional log-likelihood estimation, which is also equivalent to minimize the negative log-likelihood, and the negative logarithm of the likelihood is defined as

\[
\ell_{LACRF} = -\sum_i \log \hat{p}(y|h).
\]

(10)

The LACRF can alleviate the label-imbalance; however, it does not differentiate between easy and hard samples, which is still remained to be addressed. Despite the correlations between labels in NER task and by treating NER as a traditional classification task where each input token has the corresponding class, it is obvious that "O" class is dominant and other classes only occupy extremely small part in the NER data set. According to Table I, the dominating data with "O" class, termed easy samples, achieves notably higher confidence compared with other rare classes. This may be caused by the fact that the training procedure is still dominated by the easily classified examples without sufficient valuable learning signal, which leads to degenerated models.

This issue is also commonly seen in the object detection task and Lin et al. [12] proposed a simple but effective approach, namely, FL to address it. The main idea is to reshape the loss function to down-weight overwhelming easy samples (i.e., background objects) and thus focus training on hard samples (i.e., foreground objects). Similar to background objects in object detection, in NER, the data with "O" label: 1) occupies the overwhelming portion in the training phrase; 2) are classified with very high accuracy (around 97% F1 score); and 3) are not considered in the evaluation. Motivated by the effectiveness of FL for handling the object detection, we apply it to address the easy/hard sample issue in NER task. For the convenience of presentation, we here only present the binary case, and it is easy to be applied to the multiclass scenario. Formally, we first define

\[
q_t = \begin{cases} 
q & \text{if } y = 1 \\
1 - q & \text{if otherwise}
\end{cases}
\]

where \( y \in [1, -1] \) specifies the ground-truth class and \( q \in [0, 1] \) is the model’s estimated probability for the class with label \( y = 1 \) based on the softmax of the word-level fusion features (Fig. 3). The FL is to add a modulating factor \( (1 - q_t)^\gamma \) to the cross-entropy loss of the classification task, with tunable focusing parameter \( \gamma \geq 0 \). The definition of FL is given as

\[
\ell_{FL} = \sum_i -\left(1 - q_t\right)^\gamma \log(q_t).
\]

(11)

In this way, when the input data are misclassified and \( q_t \) is small, the modulating factor is near 1 and the loss is unaffected. As \( q_t \to 1 \), the factor goes to 0 and the loss for well-classified examples is down-weighted.

So far we combine the LACRF loss and label-balanced cross entropy loss as

\[
\ell = \ell_{LACRF} + \ell_{FL}
\]

(12)

where \( \ell_{LACRF} \) and \( \ell_{FL} \) play regularization roles on the label level and the instance level, respectively. The model can be trained end-to-end with standard back-propagation by minimizing the \( \ell \).

D. Adversarial Training

In the computer vision community, a lot of experiments [50] have demonstrated the fragility of deep learning models to adversarial examples [42], which are created by changing a very small proportion of pixels. Those adversarial examples and original examples are virtually indistinguishable to human perception [51]. Recently, adversarial samples are wisely incorporated into training to improve the generalization and robustness of the model, which is so-called AT [43]. It emerges as a powerful regularization tool to stabilize training and prevent the model from being stuck in a local minimum.

As the discussion in the introduction, the noisy data contain a lot of abbreviations, emojis, and so on, which harm the NER performance significantly. The main reason is that the pretrained features such as word2vec are trained from clean data and they are not helpful to represent those noisy data such as emojis and misspelled words. To handle this challenge, in this paper, we explore AT. Specifically, we construct an adversarial sample by compounding the original sample with a perturbation bounded by a small norm \( \epsilon \) to maximize the loss function as follows:

\[
\hat{\eta} = \arg \max_{\eta: \|\eta\|_2 \leq \epsilon} \ell(\Theta; x + \eta)
\]

(13)
Fig. 3. Architecture of RoSeq.

Fig. 4. Character-level feature representation with convolutional and highway networks.

where $\Theta$ denotes the current model parameters set. By adding loss-aware perturbation during training, the model becomes more resistant to noisy data.

Unfortunately, we are unable to compute $\eta$ in (13) exactly since the exact optimization with respect to $\eta$ is unfeasible. Following the strategy in [42], this value can be approximated by linearizing it as follows:

$$\hat{\eta} = \epsilon \frac{g}{\|g\|_2}, \quad \text{where } g = \nabla \ell(\Theta; x)$$

(14)

where $\epsilon$ can be determined on the validation set. In this way, adversarial examples are generated by adding small perturbations to the inputs in the direction that most significantly increases the loss function of the model. We find such $\eta$ against the current model parameterized by $\Theta$, at each training step, and construct an adversarial example by

$$x_{\text{adv}} = x + \hat{\eta}.$$  

(15)

Noted that we generate this adversarial example on both the word and character embedding layer, respectively, as shown in Fig. 3.

Then, the classifier is trained on the mixture of original and adversarial examples to improve the generalization. To this end, we augment the loss in (12) and define the loss function for AT as

$$\ell_{\text{AT}} = \ell(\Theta; x) + \ell(\Theta; x_{\text{adv}})$$

(16)

where $\ell(\Theta; x)$ and $\ell(\Theta; x_{\text{adv}})$ represent the loss from an original example and its adversarial counterpart, respectively. Note that we present the AT in a general form for the convenience of presentation. For different samples, the loss and parameters should correspond to their counterparts. For example, we can compute the perturbations $\eta_c$ for char-embedding and $\eta_w$ for the word embedding.

IV. EXPERIMENTS

A. Data Sets

To verify the effectiveness of our method, we conduct the experiments on the following widely used NER data sets: CoNLL-2002 Dutch & Spanish NER [52], CoNLL-2003 English NER [53], and WNUT-2016/17 English Twitter NER [54], and we use begin, inside, outside, end, single tagging scheme [2], [5], [10], [55] in our experiments. For CoNLL data sets, there are four different types of named entities: Location (LOC), Person (PER), Organization (ORG), and Miscellaneous (MISC). The WNUT-2016 data set contains ten types of named entities, whereas WNUT-2017 data set has six types, and $O$ is used as unmeaning label for all of those data sets. The statistics of the data sets are described in Table II. Note that different from CoNLL data sets, WNUT is the annotated NER data sets on the noisy user-generated text, e.g., tweets.
B. Experimental Setup

We use publicly available pretrained word embeddings for English, Spanish, and Dutch languages in our experiments. For English, we choose the 100-dimensional GloVe [56] word embeddings, which is trained on Wikipedia-2014 and Gigaword-5,1 whereas for Spanish and Dutch, we use the pretrained 50-dimensional word embeddings are trained using the word2vec package2 on the corresponding Wikipedia articles (2017-12-20 dumps) [29].

Specifically, we also use the orthographic encoder [27], [57], [58] for characters and words while training on the WNUT-2016/17 data sets for fair comparison. The orthographic encoder is used to encapsulate capitalization, punctuation, word shape, and other orthographic features. Let “n” denotes number, “c” is a letter (“C” if capitalized), punctuation is marked as “p.” Then, for example, given a sentence “I don’t like 13!,” its corresponding orthographic representation is “C cccpc cccc nnp.” In the experiment, we represent each orthographic character and orthographic word with 30-dimensional and 50-dimensional randomly initialized vectors, respectively. Then those features are concatenated to their corresponding words or characters.

For model hyperparameters, we use three filters with widths [2, 3, 4] for Char-CNN encoder and set each filter number as 20, the dimension of hidden states of word-level BiLSTM is 100, τ in the label-aware weight is set to 0.25, γ in the FL is fixed to 2.0, and the ϵ of AT is fixed to 5.0 in our experiment. Batch size is set as 16 for all experiments. The parameters optimization is performed by Adam optimizer [59] with gradient clipping of 5.0 to avoid gradient exploding problem and learning rate decay strategy. We choose the initial learning rate of β0 = 0.001 for all experiments. At each epoch τ, learning rate βt is updated using βt = β0/(1 + ρ × t), where ρ is the decay rate with value 0.05, we also set a minimal learning rate βmin = 1e-4 and let βt = βmin if βt < βmin. To reduce the overfitting issue, we also apply dropout mechanism [60] to the word and character embedding layers with drop rate 0.2 and the output of the BiLSTM layer with drop rate 0.5, respectively.

For the base model, we create a standard BiLSTM-CNNs-CRF model that simply removes the FL, AT, and LACRF components, and train this model on each data set. All the hyperparameter settings and parameters optimization strategies of this base model are the same as the aforementioned setup, except that we only use the basic linear-chain CRF for the base model and no AT, as well as FL, are adopted.

C. Comparison With State-of-the-Art Methods

In this section, we compare our approach, i.e., RoSeq model, with the SOTA methods on the five benchmark data sets. In the experiment, we run both the base model and our RoSeq model to show the improvements on the benchmark data sets and then compare with SOTA methods. The results on the test set of each benchmark data set are reported in Table III. The proposed RoSeq is able to achieve a new SOTA performance on different data sets, i.e., 88.07% on CoNLL-2002 Dutch, 87.33% on CoNLL-2002 Spanish, 91.42% on CoNLL-2003 English, 52.94% on WNUT-2016 Twitter, and 43.03% on WNUT-2017 Twitter. Note that we do not include the performance of some of the most recent works [9], [20], [30], [31], and [61], for a fair comparison. Although those works achieve slightly higher results on some of the benchmark data sets, they either incorporate external resources, transfer knowledge from other lingual/domain data sets, augment POS tags or lexicons as additional inputs, or jointly training with cross-lingual/domain data sets by sharing model parameters, and so on. In contrast, our model does not use any additional resources and only focus on the task data set itself during the training phase. How to incorporate additional information to further boost performance is not the focus of this paper.

D. Ablation Study of RoSeq Model

In the proposed RoSeq model, we introduce the LACRF, FL, and AT for addressing the label imbalance, easy/hard samples, and noisy data issues. In this section, we investigate the effects of those introduced components and study how they help to improve the model. We conduct the experiments on the CoNLL-2002 Dutch NER and WNUT-2016 English Twitter NER data sets and the results are summarized in Table IV.

From the table, we observe that all the proposed components have contributions to improve the base model, while the AT contributes the most. It is also interesting to note that the performance improvement on WNUT-2016 English Twitter NER data set is higher than that on CoNLL-2002 Dutch NER data set, and we have the similar observation on rest two CoNLL and WNUT-2017 data sets. Since the CoNLL data sets are collected from news wire articles, which are clean and can be easily understood by the learning model. In contrast, the WNUT data sets, which were obtained from user-generated tweets, contain a lot of noises, such as emojis, punctuation, incomplete or misspelled words, and so on. Those noises affect the model’s performance largely due to a large amount of

1https://nlp.stanford.edu/projects/glove/
2https://github.com/tmikolov/word2vec
TABLE III
COMPARISON WITH THE SOTA METHODS (F1 SCORE (%))

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Copal et al. [62]</td>
<td>-</td>
<td>82.44</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Huang et al. [1]</td>
<td>-</td>
<td>-</td>
<td>90.10</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Gillick et al. [63]</td>
<td>82.84</td>
<td>82.59</td>
<td>86.50</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Luo et al. [7]</td>
<td>-</td>
<td>-</td>
<td>91.20</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Lampel et al. [2]</td>
<td>81.74</td>
<td>85.75</td>
<td>90.94</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Ma et al. [10]</td>
<td>-</td>
<td>-</td>
<td>91.21</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Yang et al. [21]</td>
<td>85.19</td>
<td>85.77</td>
<td>91.26</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Lin et al. [29]</td>
<td>86.55</td>
<td>85.88</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Sikdar et al. [64]</td>
<td>-</td>
<td>-</td>
<td>40.06</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Espinosa et al. [65]</td>
<td>-</td>
<td>-</td>
<td>44.77</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Partolas et al. [57]</td>
<td>-</td>
<td>-</td>
<td>46.16</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Limosphamath &amp; Collier [58]</td>
<td>-</td>
<td>-</td>
<td>52.41</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Patrick et al. [66]</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>39.98</td>
<td>-</td>
</tr>
<tr>
<td>Lin et al. [67]</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>40.42</td>
<td>-</td>
</tr>
<tr>
<td>Von &amp; Cieliebak [68]</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>40.78</td>
<td>-</td>
</tr>
<tr>
<td>Agulaa et al. [27]</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>41.86</td>
<td>-</td>
</tr>
<tr>
<td>Base Model</td>
<td>85.23</td>
<td>85.37</td>
<td>90.33</td>
<td>46.13</td>
<td>39.12</td>
</tr>
<tr>
<td>RoSeq Model</td>
<td>88.07</td>
<td>87.33</td>
<td>91.42</td>
<td>52.94</td>
<td>43.03</td>
</tr>
</tbody>
</table>

TABLE IV
PERFORMANCE COMPARISON BETWEEN MODELS WITH DIFFERENT COMPONENTS

<table>
<thead>
<tr>
<th>Method</th>
<th>NER Datasets</th>
<th>CoNLL-2002 Dutch</th>
<th>WNUT-2016 English</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Model</td>
<td>85.23</td>
<td>46.13</td>
<td></td>
</tr>
<tr>
<td>+LACRF</td>
<td>85.61</td>
<td>46.99</td>
<td></td>
</tr>
<tr>
<td>+FL</td>
<td>86.08</td>
<td>47.86</td>
<td></td>
</tr>
<tr>
<td>+AT</td>
<td>86.99</td>
<td>50.85</td>
<td></td>
</tr>
<tr>
<td>+LACRF +FL</td>
<td>86.52</td>
<td>48.20</td>
<td></td>
</tr>
<tr>
<td>+LACRF +AT</td>
<td>87.32</td>
<td>51.11</td>
<td></td>
</tr>
<tr>
<td>+FL +AT</td>
<td>87.67</td>
<td>52.09</td>
<td></td>
</tr>
<tr>
<td>RoSeq Model</td>
<td>88.07</td>
<td>52.94</td>
<td></td>
</tr>
</tbody>
</table>

out-of-vocabulary tokens, wrong semantic/syntactic relations between words, and so on.

For the CoNLL-2002 Dutch data set, the base model achieves 85.23% F1 score. The LACRF component slightly improves the performance by 0.38%. The FL component improves the performance with around 0.85%. The AT improves the model most significantly with pushing the F1 score to 86.95%. Therefore, AT not only helps to generalize the model and suppress the noise but also create new training samples by injecting the perturbation into the input token embeddings. Finally, the RoSeq model, which merges those three components, achieves 88.07% on the CoNLL-2002 Dutch NER data set.

For the WNUT-2016 English Twitter data set, the performance increasing trends are similar to that on Dutch data set. Although the absolute F1 scores obtained by the model are relatively lower than that of the CoNLL-2002 Dutch data set, the performance improvement is much larger. Similarly, the AT contributes the most, since WNUT-2016 data set is the noisy user-generated data and AT component is good at suppressing the noises in the data set. Different from CoNLL-2002 Dutch data set, the RoSeq model achieves more than 6.8% improvements on WNUT-2016 data set.

E. Labelwise Performance Analysis

In the proposed RoSeq model, the introduced components, i.e., LACRF, FL, and AT, show improvements for NER task on different data sets. In this experiment, we further conduct the labelwise performance analysis of the RoSeq model and the base model. Here, we also take CoNLL-2002 Dutch NER and WNUT-2016 English Twitter NER as a showcase and results are illustrated in Fig. 5. Note that the result of “O” label in the figure is only visualized for comparison, which is not considered as the contribution in the final result. Labels in the figure are sorted by frequency in descending order.

In Fig. 5(a), the RoSeq model outperforms the base model on all the five labels. Although it only shows a slight improvement on the unmeaning and dominating “O” label compared to the base model, the RoSeq gives more significant improvements for the rest meaningful labels. For example, for “PER,” “LOC,” and “ORG” labels, our method obtains around 1.7%, 0.9%, and 3.01% absolute improvement in F1 score, respectively. For the label “MISC” with the lowest F1 score in the base model, our method improves the F1 score by 5.19% and it is the largest improvement among all the labels, which indicates that our method is more effective for the sparse labels and hard samples.

For WNUT-2016 English Twitter data set, as shown in Fig. 5(b), the results are similar to that on CoNLL-2002 Dutch NER, while the improvements of RoSeq model are more significant. The performance of the base model and our method is comparable in nonmeaningful “O” label. In the remaining meaningful labels, our method increases 5.46%, 4.51%, 13.0%, 4.0%, and 0.15% absolute improvement in F1 score, respectively. For the label “MISC” with the lowest F1 score in the base model, our method improves the F1 score by 5.19% and it is the largest improvement among all the labels, which indicates that our method is more effective for the sparse labels and hard samples.
Fig. 5. Comparison of the results between Base and RoSeq models at the label level on CoNLL-2002 Dutch NER and WNUT-2016 English Twitter NER test sets. Red bar: base model. Blue bar: results of RoSeq model. The number below each label denotes the label proportion in the training data set.
(a) CoNLL-2002 Dutch. (b) WNUT-2016 English Twitter.

### TABLE V
**COMPARISON OF PREDICTED EXAMPLES BETWEEN THE BASE MODEL AND ROSEQ**

<table>
<thead>
<tr>
<th>Base Model</th>
<th>RoSeq Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dole (B-PER) also said he opposed California (B-LOC) Proposition 215 which ...</td>
<td>Dole (B-PER) also said he opposed California (B-LOC) Proposition 215 which ...</td>
</tr>
<tr>
<td>California (B-LOC) at New (B-LOC) York (B-LOC)</td>
<td>California (B-LOC) at New (B-LOC) York (B-LOC)</td>
</tr>
<tr>
<td>... who appeared in his major-league record 2,282nd straight game today, a 13-0 loss to the California (B-LOC) Angle (B-ORG).</td>
<td>... who appeared in his major-league record 2,282nd straight game today, a 13-0 loss to the California (B-LOC) Angle (B-ORG).</td>
</tr>
<tr>
<td>... (a Newmont-Santa (B-MISC) Fe (B-ORG) deal) is positive, it does all the right things.</td>
<td>... (a Newmont-Santa (B-MISC) Fe (B-MISC) deal) is positive, it does all the right things.</td>
</tr>
<tr>
<td>Newmont (B-ORG) proposed to Santa (B-LOC) Fe (B-LOC) a stock-swap merger at a ratio of 0.33 ...</td>
<td>Newmont (B-LOC) proposed to Santa (B-LOC) Fe (B-LOC) a stock-swap merger at a ratio of 0.33 ...</td>
</tr>
</tbody>
</table>

* Green color indicates correctly predicted while red color represents falsely predicted.

34.59% and 45.68%, whose F1 scores absolutely increase by 18.21% and 21.08%, respectively. For the “product” label, our method increases the F1 score from 10.8% of the base model to 27.59%, which is more than 2.5 times improvement. For those failed labels in the base model, our method achieves 14.14% F1 score on “musicartist” label. Furthermore, our method also fails to recognize any “tvshow” label from the data set.

Overall, by comparing the labelwise performance of the base model and our RoSeq model on CoNLL-2002 Dutch and WNUT-2016 English Twitter data sets, we demonstrate that the RoSeq model is able to address the label imbalance issue and also shows its effectiveness to improve the performance, especially on the noisy user-generated data sets (e.g., WNUT data sets) and limited training size of some classes.

Moreover, we also show some predicted examples for both of the base model and our proposed RoSeq algorithm to verify the effectiveness of RoSeq, as justified in Table V. In particular, we choose several testing samples from CoNLL-2003 data sets where the base model fails to assign correct labels for the specific phrases, whereas RoSeq still works well. Those samples also verify the capacity of RoSeq for handling the ambiguous labels, compared with the base method. For example, the ground truth label for “California” in the first sample is “MISCELLANEOUS,” but it is “ORGANIZATION” in the second and third samples. Although RoSeq yields the correct predictions, the base model predicts the “California” in all the three samples as “LOCATION” label type (which is the most frequent label for this word. In the fourth sample, “Newmont-Santa” and “Fe” are combined to be labeled as “MISCELLANEOUS.” However, the base model assigns two different label types for “Newmont-Santa” and “Fe” as “MISCELLANEOUS” and “ORGANIZATION,” respectively. In the last testing sample, “Santa” and “Fe” are merged to represent a “LOCATION.” Nevertheless, the base model mistakenly predicts “Santa Fe” as “ORGANIZATION.” In contrast, RoSeq makes the correct predictions for the last two testing samples. We have similar observations in other testing samples. Generally, we can conclude that RoSeq is more effective than the base method to reduce the wrong predictions.

## V. Conclusion

To address the, namely, label imbalance and noisy data problems, we develop a RoSeq model for NER. To the end, we introduce three components, LACRF, FL, and AT, to handle the proposed issues. Extensive experiments show the superiority of RoSeq over existing models on CoNLL-NER and WNUT-NER benchmark data sets without external resources.


Joey Tianyi Zhou received the Ph.D. degree in computer science from Nanyang Technological University, Singapore, in 2015. He is currently a Scientist with the Research Agency for Science, Technology, and Research, Institute of High Performance Computing, Singapore. Dr. Zhou was a recipient of the Best Poster Honorable Mention at ACML 2012, the Best Paper Award from the BeyondLabeler Workshop on IJCAI 2016, the Best Paper Nomination at ECCV 2016, and the NIPS 2017 Best Reviewer Award. He has served as an Associate Editor for the IEEE ACCESS and a Guest Editor for IET Image Processing.

Hao Zhang received the B.S. degree in communications engineering from the Dalian University of Technology, Dalian, China, in 2015, and the M.S. degree in communications engineering from Nanyang Technological University, Singapore, in 2016. He is currently a Research Engineer with the Agency of Science, Technology, and Research, Artificial Intelligence Initiative, Singapore.

Di Jin received the B.S. degree in precision instruments from Tsinghua University, Beijing, China, in 2015. He is currently pursuing the Ph.D. degree with the Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, Cambridge, MA, USA.

Xi Peng received the Ph.D. degree in computer science from Sichuan University, Chengdu, China, in 2013. He is currently a Research Professor with the College of Computer Science, Sichuan University. His current research interests include unsupervised representation learning and differentiable programming, and their applications in computer vision and image processing. In these areas, he has authored more than 40 papers.

Yang Xiao received the B.S., M.S., and Ph.D. degrees from the Huazhong University of Science and Technology, Wuhan, China, in 2004, 2007, and 2011, respectively. He was a Research Fellow with the School of Computer Engineering, Institute of Media Innovation, Nanyang Technological University, Singapore. He is currently an Associate Professor with the School of Artificial Intelligence and Automation, Huazhong University of Science and Technology. His current research interests include computer vision, image processing, and machine learning.

Zhiguo Cao received the B.S. and M.S. degrees in communication and information system from the University of Electronic Science and Technology of China, Chengdu, China, in 1985 and 1990, respectively, and the Ph.D. degree in pattern recognition and intelligent system from the Huazhong University of Science and Technology, Wuhan, China, in 2001. He is currently a Professor with the School of Artificial Intelligence and Automation, Huazhong University of Science and Technology. His current research interests include spread across image understanding and analysis, depth information extraction, 3-D video processing, motion detection and human action analysis. His current research results, which have published dozens of papers at International Journals and Prominent Conferences, have been applied to automatic observation system for crop growth in agricultural, for weather phenomenon in meteorology and for object recognition in video surveillance system based on computer vision.