FAKEDETECTOR: Effective Fake News Detection with Deep Diffusive Neural Network

Jiawei Zhang¹, Bowen Dong², Philip S. Yu² ¹IFM Lab, Department of Computer Science, Florida State University, FL, USA ²BDSC Lab, Department of Computer Science, University of Illinois at Chicago, IL, USA jzhang@ifmlab.org, {bdong5, psyu}@uic.edu

Abstract-In recent years, due to the booming development of online social networks, fake news for various commercial and political purposes has been appearing in large numbers and widespread in the online world. With deceptive words, online social network users can get infected by these online fake news easily, which has brought about tremendous effects on the offline society already. An important goal in improving the trustworthiness of information in online social networks is to identify the fake news timely. This paper aims at investigating the principles, methodologies and algorithms for detecting fake news articles, creators and subjects from online social networks and evaluating the corresponding performance. This paper addresses the challenges introduced by the unknown characteristics of fake news and diverse connections among news articles, creators and subjects. This paper introduces a novel gated graph neural network, namely FAKEDETECTOR. Based on a set of explicit and latent features extracted from the textual information, FAKEDETECTOR builds a deep diffusive network model to learn the representations of news articles, creators and subjects simultaneously. Extensive experiments have been done on a real-world fake news dataset to compare FAKEDETECTOR with several state-of-the-art models, and the experimental results are provided in the full-version of this paper at [13].

Index Terms—Fake News Detection; Diffusive Network; Graph Neural Network; Text Mining; Data Mining

I. Introduction

Fake news denotes a type of yellow press which intentionally presents misinformation or hoaxes spreading through both traditional print news media and recent online social media [11]. Fake news has been existing for a long time, since the "Great moon hoax" published in 1835 [1]. In recent years, due to the booming developments of online social networks, fake news for various commercial and political purposes has been appearing in large numbers and widespread in the online world. With deceptive words, online social network users can get infected by these online fake news easily, which has brought about tremendous effects on the offline society already. During the 2016 US president election, various kinds of fake news about the candidates widely spread in the online social networks, which may have a significant effect on the election results. According to a post-election statistical report [3], online social networks account for more than 41.8% of the fake news data traffic in the election, which is much greater than the data traffic shares of both traditional TV/radio/print medium and online search engines respectively. An important goal in improving the trustworthiness of information in online

social networks is to identify the fake news timely, which will be the main task studied in this paper.

Fake news has significant differences compared with traditional suspicious information, like spams [9], [10], [5], [2], in various aspects: (1) impact on society: spams usually exist in personal emails or specific review websites and merely have a local impact on a small number of audiences, while the impact fake news in online social networks can be tremendous due to the massive user numbers globally, which is further boosted by the extensive information sharing and propagation among these users [7], [8], [12]; (2) audiences' initiative: instead of receiving spam emails passively, users in online social networks may seek for, receive and share news information actively with no sense about its correctness; and (3) identification difficulty: via comparisons with abundant regular messages (in emails or review websites), spams are usually easier to be distinguished, whereas identifying fake news with erroneous information is incredibly challenging, since it requires both tedious evidence-collecting and careful fact-checking due to the lack of other comparative news articles available.

These characteristics aforementioned of fake news pose new challenges on the detection task. Besides detecting fake news articles, identifying the fake news creators and subjects will actually be more important, which will help completely eradicate a large number of fake news from the origins in online social networks. Generally, for the news creators, besides the articles written by them, we are also able to retrieve his/her profile information from either the social network website or external knowledge libraries, e.g., Wikipedia or government-internal database, which will provide fundamental complementary information for his/her background check. Meanwhile, for the news subjects, we can also obtain its textual descriptions or other related information, which can be used as the foundations for news subject credibility inference. From a higher-level perspective, the tasks of fake news article, creator and subject detection are highly correlated, since the articles written from a trustworthy person should have a higher credibility, while the person who frequently posting unauthentic information will have a lower credibility on the other hand. Similar correlations can also be observed between news articles and news subjects. In the following part of this paper, without clear specifications, we will use the general fake news term to denote the fake news articles, creators and subjects by default.

Problem Studied: In this paper, we will study the fake news detection (including articles, creators and subjects) problem in online social networks. Based on various types of heterogeneous information sources, including both textual contents/profile/descriptions and the authorship and article-subject relationships among them, we aim at identifying fake news from the online social networks simultaneously. We formulate the fake news detection problem as a credibility inference problem, where the real ones will have a higher credibility while unauthentic ones will have a lower one instead.

To solve the problem, in this paper, we will introduce a new graph neural network model, namely FAKEDETECTOR. In FAKEDETECTOR, the fake news detection problem is formulated as a credibility label inference problem, and FAKEDETECTOR aims at learning a prediction model to infer the credibility labels of news articles, creators and subjects simultaneously. FAKEDETECTOR deploys a new hybrid feature learning unit (HFLU) for learning the explicit and latent feature representations of news articles, creators and subjects respectively, and introduce a novel deep diffusive network model with the gated diffusive unit for the heterogeneous information fusion within the social networks.

In the following sections of this paper, we will first introduce several important concepts and the problem formulation in Section II, and then talk about the FAKEDETECTOR model in Section III. For detailed information about the data analysis and the experimental studies of the model, the readers are suggested to refer to our full-version paper [13].

II. PROBLEM FORMULATION

A. Terminology Definition

In this paper, we will use the "news article" concept in referring to the posts either written or shared by users in online social media, "news subject" to represent the topics of these news articles, and "news creator" concept to denote the set of users writing the news articles.

DEFINITION 1: (News Article): News articles published in online social networks can be represented as set $\mathcal{N} = \{n_1, n_2, \cdots, n_m\}$. For each news article $n_i \in \mathcal{N}$, it can be represented as a tuple $n_i = (n_i^t, n_i^c)$, where the entries denote its *textual content* and *credibility label*, respectively.

DEFINITION 2: (News Subject): Formally, we can represent the set of news subjects involved in the social network as $S = \{s_1, s_2, \cdots, s_k\}$. For each subject $s_i \in S$, it can be represented as a tuple $s_i = (s_i^t, s_i^c)$ containing its *textual description* and *credibility label*, respectively.

DEFINITION 3: (News Creator): We can represent the set of news creators in the social network as $\mathcal{U} = \{u_1, u_2, \cdots, u_n\}$. To be consistent with the definition of news articles, we can also represent news creator $u_i \in \mathcal{U}$ as a tuple $u_i = (u_i^p, u_i^s)$, where the entries denote the profile information and credibility label of the creator, respectively.

DEFINITION 4: (News Augmented Heterogeneous Social Networks): The online social network together with the news articles published in it can be represented as a news augmented heterogeneous social network (News-HSN) $G = (\mathcal{V}, \mathcal{E})$, where

 $\mathcal{V} = \mathcal{U} \cup \mathcal{N} \cup \mathcal{S}$ covers the sets of news articles, creators and subjects, and the edge set $\mathcal{E} = \mathcal{E}_{u,n} \cup \mathcal{E}_{n,s}$ involves the authorship links between articles and creators, and the topic indication links between articles and subjects.

B. Problem Formulation

Based on the definitions of terminologies introduced above, the fake news detection problem studied in this paper can be formally defined as follows.

Problem Formulation: Given a News-HSN $G=(\mathcal{V},\mathcal{E})$, the fake news detection problem aims at learning an inference function $f:\mathcal{U}\cup\mathcal{N}\cup\mathcal{S}\to\mathcal{Y}$ to predict the *credibility labels* of news articles in set \mathcal{N} , news creators in set \mathcal{U} and news subjects in set \mathcal{S} . In learning function f, various kinds of heterogeneous information in network G should be effectively incorporated, including both the textual content/profile/description information as well as the connections among them.

III. PROPOSED METHODS

In this section, we will provide the detailed information about the FAKEDETECTOR model in this section. FAKEDETECTOR covers two main components: *representation feature learning*, and *credibility label inference*, which together will compose the deep diffusive network model FAKEDETECTOR.

A. Representation Feature Learning

As illustrated in the analysis provided in [13], in the news augmented heterogeneous social network, both the textual contents and the diverse relationships among news articles, creators and subjects can provide important information for inferring the credibility labels of fake news. In this part, we will focus on feature learning from the textual content information based on the *hybrid feature extraction unit* as shown in Figure 1, while the relationships will be used for building the deep diffusive model in the following subsection.

1) Explicit Feature Extraction: The textual information of fake news can reveal important signals for their credibility inference. Besides some shared words used in both true and false articles (or creators/subjects), a set of frequently used words can also be extracted from the article contents, creator profiles and subject descriptions of each category respectively. Let \mathcal{W} denotes the complete vocabulary set used in the PolitiFact dataset, and from \mathcal{W} a set of unique words can also be extracted from articles, creator profile and subject textual information, which can be denoted as sets $\mathcal{W}_n \subset \mathcal{W}$, $\mathcal{W}_u \subset \mathcal{W}$ and $\mathcal{W}_s \subset \mathcal{W}$ respectively (of size d).

These extracted words have shown their stronger correlations with their fake/true labels. As shown in the left component of Figure 1, based on the pre-extracted word sets \mathbf{W}_n , given a news article $n_i \in \mathcal{N}$, we can represent the extracted explicit feature vector for n_i as vector $\mathbf{x}_{n,i}^e \in \mathbb{R}^d$, where entry $x_{n,i}^e(k)$ denotes the number of appearance times of word $w_k \in \mathbf{W}_n$ in news article n_i . In a similar way, based on the extracted word set \mathcal{W}_u (and \mathcal{W}_s), we can also represent the extracted explicit feature vectors for creator u_j as $\mathbf{x}_{u,j}^e \in \mathbb{R}^d$ (and for subject s_l as $\mathbf{x}_{s,l}^e \in \mathbb{R}^d$).

2) Latent Feature Extraction: Besides those explicitly visible words about the news article content, creator profile and subject description, there also exist some hidden signals about articles, creators and subjects, e.g., news article content information inconsistency and profile/description latent patterns, which can be effectively detected from the latent features as introduced in [6]. Based on such an intuition, in this paper, we propose to further extract a set of latent features for news articles, creators and subjects based on the deep recurrent neural network model.

Formally, given a news article $n_i \in \mathcal{N}$, based on its original textual contents, we can represents its content as a sequence of words represented as vectors $(\mathbf{x}_{i,1}, \mathbf{x}_{i,2}, \cdots, \mathbf{x}_{i,q})$, where q denotes the maximum length of articles (and for those with less than q words, zero-padding will be adopted). Each feature vector $\mathbf{x}_{i,k}$ corresponds to one word in the article. Based on the vocabulary set \mathcal{W} , it can be represented in different ways, e.g., the one-hot code representation or the binary code vector of a unique index assigned for the word. The latter representation will save the computational space cost greatly.

As shown in the right component of Figure 1, the latent feature extraction is based on RNN model (with the basic neuron cells), which has 3 layers (1 input layer, 1 hidden layer, and 1 fusion layer). Based on the input vectors $(\mathbf{x}_{i,1}, \mathbf{x}_{i,2}, \cdots, \mathbf{x}_{i,q})$ of the textual input string, we can represent the feature vectors at the hidden layer and the output layer as follows respectively:

$$\left\{ \begin{array}{l} \text{\# Fusion Layer: } \mathbf{x}_{n,i}^l = \sigma(\sum_{t=1}^q \mathbf{W}_i \mathbf{h}_{i,t}), \\ \text{\# Hidden Layer: } \mathbf{h}_{i,t} = GRU(\mathbf{h}_{i,t-1}, \mathbf{x}_{i,t}; \mathbf{W}) \end{array} \right.$$

where GRU (Gated Recurrent Unit) [4] is used as the unit model in the hidden layer and the W matrices denote the variables of the model to be learned.

Based on a component with a similar architecture, we can extract the latent feature vector for news creator $u_j \in \mathcal{U}$ (and subject $s_l \in \mathcal{S}$) as well, which can be denoted as vector $\mathbf{x}_{u,j}^l$ (and $\mathbf{x}_{s,l}^l$). By appending the explicit and latent feature vectors together, we can formally represent the extracted feature representations of news articles, creators and subjects as $\mathbf{x}_{n,i} = \left[(\mathbf{x}_{n,i}^e)^\top, (\mathbf{x}_{n,i}^l)^\top \right]^\top$, $\mathbf{x}_{u,j} = \left[(\mathbf{x}_{u,j}^e)^\top, (\mathbf{x}_{u,j}^l)^\top \right]^\top$ and $\mathbf{x}_{s,l} = \left[(\mathbf{x}_{s,l}^e)^\top, (\mathbf{x}_{s,l}^l)^\top \right]^\top$ respectively, which will be fed as the inputs for the deep diffusive unit model to be introduced in the next subsection.

B. Deep Diffusive Unit Model

Actually, the credibility of news articles are highly correlated with their subjects and creators. The relationships among news articles, creators and subjects are illustrated with an example in Figure 2. For each creator, they can write multiple news articles, and each news article has only one creator. Each news article can belong to multiple subjects, and each subject can also have multiple news articles taking it as the main topics. To model the correlation among news articles, creators and subjects, we will introduce the deep diffusive graph neural network model as follow.

The overall architecture of FAKEDETECTOR corresponding to the case study shown in Figure 2 is provided in Figure 4. Besides the HFLU feature learning unit model, FAKEDETECTOR also uses a *gated diffusive unit* (GDU) model for effective relationship modeling among news articles, creators and subjects, whose structure is illustrated in Figure 3. Formally, the GDU model accepts multiple inputs from different sources simultaneously, i.e., \mathbf{x}_i , \mathbf{z}_i and \mathbf{t}_i , and outputs its learned hidden state \mathbf{h}_i to the output layer and other unit models in the diffusive network architecture.

Here, let's take news articles as an example. Formally, among all the inputs of the GDU model, x_i denotes the extracted feature vector from HFLU for news articles, \mathbf{z}_i represents the input from other GDUs corresponding to subjects, and t_i represents the input from other GDUs about creators. Considering that the GDU for each news article may be connected to multiple GDUs of subjects and creators, the $mean(\cdot)$ of the outputs from the GDUs corresponding to these subjects and creators will be computed as the inputs z_i and \mathbf{t}_i instead respectively, which is also indicated by the GDU architecture illustrated in Figure 3. For the inputs from the subjects, GDU has a gate called the "forget gate", which may update some content of z_i to forget. The forget gate is important, since in the real world, different news articles may focus on different aspects about the subjects and "forgetting" part of the input from the subjects is necessary in modeling. Formally, we can represent the "forget gate" together with the updated input as

$$ilde{\mathbf{z}}_i = \mathbf{f}_i \otimes \mathbf{z}_i, ext{ where } \mathbf{f}_i = \sigma \left(\mathbf{W}_f \left[\mathbf{x}_i^ op, \mathbf{z}_i^ op, \mathbf{t}_i^ op
ight]^ op
ight).$$

Here, operator \otimes denotes the entry-wise product of vectors and \mathbf{W}_f represents the variable of the forget gate in GDU.

Meanwhile, for the input from the creator nodes, a new node-type "adjust gate" is introduced in GDU. Here, the term "adjust" models the necessary changes of information between different node categories (e.g., from creators to articles). Formally, we can represent the "adjust gate" as well as the updated input as

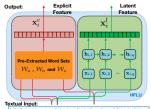
$$\tilde{\mathbf{t}}_i = \mathbf{e}_i \otimes \mathbf{t}_i, \text{ where } \mathbf{e}_i = \sigma \left(\mathbf{W}_e \left[\mathbf{x}_i^\top, \mathbf{z}_i^\top, \mathbf{t}_i^\top \right]^\top \right),$$

where W_e denotes the variable matrix in the adjust gate.

GDU allows different combinations of these input/state vectors, which are controlled by the selection gates \mathbf{g}_i and \mathbf{r}_i respectively. Formally, we can represent the final output of GDU as

$$\begin{aligned} \mathbf{h}_{i} &= \mathbf{g}_{i} \otimes \mathbf{r}_{i} \otimes \tanh \left(\mathbf{W}_{u} [\mathbf{x}_{i}^{\top}, \tilde{\mathbf{z}}_{i}^{\top}, \tilde{\mathbf{t}}_{i}^{\top}]^{\top} \right) \\ &\oplus \left(\mathbf{1} \ominus \mathbf{g}_{i} \right) \otimes \mathbf{r}_{i} \otimes \tanh \left(\mathbf{W}_{u} [\mathbf{x}_{i}^{\top}, \mathbf{z}_{i}^{\top}, \tilde{\mathbf{t}}_{i}^{\top}]^{\top} \right) \\ &\oplus \mathbf{g}_{i} \otimes \left(\mathbf{1} \ominus \mathbf{r}_{i} \right) \otimes \tanh \left(\mathbf{W}_{u} [\mathbf{x}_{i}^{\top}, \tilde{\mathbf{z}}_{i}^{\top}, \mathbf{t}_{i}^{\top}]^{\top} \right) \\ &\oplus \left(\mathbf{1} \ominus \mathbf{g}_{i} \right) \otimes \left(\mathbf{1} \ominus \mathbf{r}_{i} \right) \otimes \tanh \left(\mathbf{W}_{u} [\mathbf{x}_{i}^{\top}, \mathbf{z}_{i}^{\top}, \mathbf{t}_{i}^{\top}]^{\top} \right), \end{aligned}$$

where $\mathbf{g}_i = \sigma(\mathbf{W}_g \left[\mathbf{x}_i^\top, \mathbf{z}_i^\top, \mathbf{t}_i^\top \right]^\top)$, and $\mathbf{r}_i = \sigma(\mathbf{W}_r \left[\mathbf{x}_i^\top, \mathbf{z}_i^\top, \mathbf{t}_i^\top \right]^\top)$, and term 1 denotes a vector filled with value 1. Operators \oplus and \ominus denote the entry-wise addition and minus operation of vectors. Matrices \mathbf{W}_u , \mathbf{W}_g ,





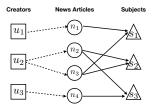


Fig. 2. Relationships of Articles, Creators and Subjects.

 \mathbf{W}_r represent the variables involved in the components. Vector \mathbf{h}_i will be the output of the GDU model.

The introduced GDU model also works for both the news subjects and creator nodes in the network. When applying the GDU to model the states of the subject/creator nodes with two input only, the remaining input port can be assigned with a default value (usually vector 0). Based on the GDU, we can denote the overall architecture of the FAKEDETECTOR as shown in Figure 4, where the lines connecting the GDUs denote the data flow among the unit models. In the following section, we will introduce how to learn the parameters involved in the FAKEDETECTOR model for concurrent credibility inference of multiple nodes.

C. Deep Diffusive Network Model Learning

In the FAKEDETECTOR model as shown in Figure 4, based on the output state vectors of news articles, news creators and news subjects, the framework will project the feature vectors to their credibility labels. Formally, given the state vectors $\mathbf{h}_{n,i}$ of news article n_i , $\mathbf{h}_{u,j}$ of news creator u_j , and $\mathbf{h}_{s,l}$ of news subject s_l , we can represent their inferred credibility labels as vectors $\mathbf{y}_{n,i}$, $\mathbf{y}_{u,j}$, $\mathbf{y}_{s,l} \in \mathcal{R}^{|\mathcal{Y}|}$ respectively (\mathcal{Y} is the objective label set), which can be represented as

$$\begin{cases} \mathbf{y}_{n,i} &= softmax\left(\mathbf{W}_{n}\mathbf{h}_{n,i}\right), \\ \mathbf{y}_{u,j} &= softmax\left(\mathbf{W}_{u}\mathbf{h}_{u,j}\right), \\ \mathbf{y}_{s,l} &= softmax\left(\mathbf{W}_{s}\mathbf{h}_{s,l}\right). \end{cases}$$

where \mathbf{W}_u , \mathbf{W}_n and \mathbf{W}_s define the weight variables projecting state vectors to the output vectors, and function $softmax(\cdot)$ represents the softmax function.

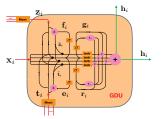
Meanwhile, based on the news articles in the training set $\mathcal{T}_n \subset \mathcal{N}$ with the ground-truth credibility label vectors $\{\hat{\mathbf{y}}_{n,i}\}_{n_i \in \mathcal{T}_n}$, we can define the loss function of the framework for news article credibility label learning as the cross-entropy between the prediction results and the ground truth:

$$\mathcal{L}(\mathcal{T}_n) = -\sum_{n_i \in \mathcal{T}_n} \sum_{k=1}^{|\mathcal{Y}|} \hat{\mathbf{y}}_{n,i}[k] \log \mathbf{y}_{n,i}[k].$$

Similarly, we can define the loss terms introduced by news creators and subjects based on training sets $\mathcal{T}_u \subset \mathcal{U}$ and $\mathcal{T}_s \subset \mathcal{S}$ as

$$\mathcal{L}(\mathcal{T}_u) = -\sum_{u_j \in \mathcal{T}_u} \sum_{k=1}^{|\mathcal{Y}|} \hat{\mathbf{y}}_{u,j}[k] \log \mathbf{y}_{u,j}[k],$$

$$\mathcal{L}(\mathcal{T}_s) = -\sum_{s_l \in \mathcal{T}_s} \sum_{k=1}^{|\mathcal{Y}|} \hat{\mathbf{y}}_{s,l}[k] \log \mathbf{y}_{s,l}[k],$$



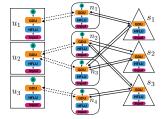


Fig. 3. Gated Diffusive Unit (GDU).

Fig. 4. The Architecture of Framework FAKEDETECTOR.

where $\mathbf{y}_{u,j}$ and $\hat{\mathbf{y}}_{u,j}$ (and $\mathbf{y}_{s,l}$ and $\hat{\mathbf{y}}_{s,l}$) denote the prediction result vector and ground-truth vector of creator (and subject) respectively.

Formally, the main objective function of the FAKEDETECTOR model can be represented as follows:

$$\min_{\mathbf{W}} \mathcal{L}(\mathcal{T}_n) + \mathcal{L}(\mathcal{T}_u) + \mathcal{L}(\mathcal{T}_s) + \alpha \cdot \mathcal{L}_{reg}(\mathbf{W}),$$

where **W** denotes all the involved variables to be learned, term $\mathcal{L}_{reg}(\mathbf{W})$ represents the regularization term (i.e., the sum of L_2 norm on the variable vectors and matrices), and α denotes the regularization term weight. By resolving the optimization functions, we will be able to learn the variables involved in the framework. In this paper, we propose to train the framework with the *back-propagation* algorithm. For the news articles, creators and subjects in the testing set, their predicted credibility labels will be outputted as the final result. More information about the experimental studies of FAKEDETECTOR on real-world datasets is available in our full-version of this paper at [13].

IV. ACKNOWLEDGEMENT

This work is supported in part by NSF through grant III-1763365 and by Florida State University. This work is supported in part by NSF under grants III-1526499, III-1763325, III-1909323, CNS-1930941, and CNS-1626432.

REFERENCES

- [1] Great moon hoax. https://en.wikipedia.org/wiki/Great_Moon_Hoax. [Online; accessed 25-September-2017].
- [2] L. Akoglu, R. Chandy, and C. Faloutsos. Opinion fraud detection in online reviews by network effects. In *ICWSM*, 2013.
- [3] H. Allcott and M. Gentzkow. Social media and fake news in the 2016 election. *Journal of Economic Perspectives*, 2017.
- [4] J. Chung, Ç. Gülçehre, K. Cho, and Y. Bengio. Empirical evaluation of gated recurrent neural networks on sequence modeling. CoRR, abs/1412.3555, 2014.
- [5] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Zhao. Detecting and characterizing social spam campaigns. In *IMC*, 2010.
- [6] Y. Kim. Convolutional neural networks for sentence classification. In EMNLP, 2014.
- [7] S. Lin, Q. Hu, J. Zhang, and P. Yu. Discovering Audience Groups and Group-Specific Influencers. 2015.
- [8] Y. Teng, C. Tai, P. Yu, and M. Chen. Modeling and utilizing dynamic influence strength for personalized promotion. In ASONAM, 2015.
- [9] S. Xie, G. Wang, S. Lin, and P. Yu. Review spam detection via temporal pattern discovery. In KDD, 2012.
- [10] S. Xie, G. Wang, S. Lin, and P. Yu. Review spam detection via time series pattern discovery. In WWW, 2012.
- [11] Y. Yang, L. Zheng, J. Zhang, Q. Cui, Z. Li, and P. Yu. TI-CNN: convolutional neural networks for fake news detection. *CoRR*, abs/1806.00749, 2018
- [12] Q. Zhan, J. Zhang, S. Wang, P. Yu, and J. Xie. Influence maximization across partially aligned heterogenous social networks. In *PAKDD*. 2015.
- [13] J. Zhang, B. Dong, and P. Yu. Fakedetector: Effective fake news detection with deep diffusive neural network. *CoRR*, abs/1805.08751, 2018.