European Journal of Operational Research xxx (xxxx) xxx

Contents lists available at ScienceDirect

European Journal of Operational Research

journal homepage: www.elsevier.com/locate/ejor

Interfaces with Other Disciplines

Detecting fake news for reducing misinformation risks using analytics approaches

Chaowei Zhang[a], Ashish Gupta[a,*], Christian Kauten[a], Amit V. Deokar[b], Xiao Qin[a]

[a] Auburn University, Auburn, AL 36849 USA
[b] University of Massachusetts Lowell, Lowell, MA 01854 USA

ARTICLE INFO

Article history:
Received 19 April 2018
Accepted 10 June 2019
Available online xxx

Keywords:
Analytics
Fake news
Classification
Topic modeling
Text analytics

ABSTRACT

Fake news is playing an increasingly dominant role in spreading misinformation by influencing people's perceptions or knowledge to distort their awareness and decision-making. The growth of social media and online forums has spurred the spread of fake news causing it to easily blend with truthful information. This study provides a novel text analytics–driven approach to fake news detection for reducing the risks posed by fake news consumption. We first describe the framework for the proposed approach and the underlying analytical model including the implementation details and validation based on a corpus of news data. We collect legitimate and fake news, which is transformed from a document based corpus into a topic and event–based representation. Fake news detection is performed using a two-layered approach, which is comprised of detecting fake topics and fake events. The efficacy of the proposed approach is demonstrated through the implementation and validation of a novel *FakE News Detection* (*FEND*) system. The proposed approach achieves 92.49% classification accuracy and 94.16% recall based on the specified threshold value of 0.6.

1. Introduction

Fake news can be defined "as the online publication of intentionally or knowingly false statements of fact (Klein & Wueller, 2017)." In essence, the focus is on articles or messages posted online with the anticipation of the message going "viral". Fake news thrives on the false rumors, hoaxes, sensationalism, and scandal resulting from the dissemination of news articles through social media (Fisher, 2014). While intentional harm is debated, various incentives, – such as monetary, social, and political benefits – often drive the fake news spread.

Recent proliferation in the use of social media as a vehicle for spreading fake news has significantly raised the risks imposed on individuals as well as organizations by the spread of misinformation (false information). For example, social platforms are frequently used to spread fake news via modifying authentic news or making fabricated news. Very recently, Berners-Lee, the inventor of the World Wide Web, claimed that fake news has been one of the most disturbing Internet trends that have to be resolved (Swartz, 2017). It is challenging, if not futile, to detect deceptive news due to the diversity and disguise of deceptions. Fake news may cause adverse influence coupled with damages. It influences an individual's decision-making and distorts one's perceptions about the real events by altering the information feeds that are utilized for news consumption. At the organizational level, the impact is more adverse as it poses risk to their brand names and can potentially affect on the consumption of their product or services (Gross, 2017). News articles shared using social media further exacerbate this problem due to increased online media consumption and use of bots (e.g., twitter bots) that automate the spread of false information. A recent survey indicates that, of the known false news stories that appeared in the three months before the 2016 election, those favoring either one of the presidential candidates were shared approximately 38 million times on Facebook (Allcott & Gentzkow, 2017).

Contemporary developments in methods of news verification address the growing demand for automated means of discriminating real news from fake news among the immense volume of data (Rubin, Chen, & Conroy, 2015a). In general, existing fake news detection approaches are categorized into two groups based on the underlying approaches, namely, linguistic, or network techniques. Linguistic approaches (e.g., natural language processing or NLP) are focused on news content, and aim to investigate fake news patterns by analyzing underlying semantics. In contrast, network approaches leverage existing knowledge networks to check facts

* Corresponding author.
E-mail addresses: czz0032@auburn.edu (C. Zhang), azg0074@auburn.edu (A. Gupta), jck0022@tigermail.auburn.edu (C. Kauten), amit_deokar@uml.edu (A.V. Deokar), xqin@auburn.edu (X. Qin).

https://doi.org/10.1016/j.ejor.2019.06.022
0377-2217/

of news (e.g., Jang et al., 2018). Recent operations research studies have started to utilize the capabilities of such text analytics and modeling approaches in various application domains. For example, text analytics approaches have been used for suggesting improved design features for augmented reality health apps (Li, Gupta, Zhang, & Flor, 2018). A few studies have applied such techniques in finance. For example, Tsai and Wang (2017) predicts financial risks by using a finance-specific sentiment lexicon and regression and ranking techniques to explore the relations between sentiment words and financial risks based on a bag-of-words model. A few studies have applied text analytics approaches for detecting product defects (Abrahams, Fan, Wang, Zhang, & Jiao, 2015), sales forecasting (Lau, Zhang, & Xu, 2018), etc. Use of these techniques in operations research is increasing as researchers start to investigate the value of unstructured data for knowledge discovery with different industry sectors.

A growing number of techniques have been devised to verify news credibility (Conroy, Rubin, & Chen, 2015; Jin, Cao, Jiang, & Zhang, 2014). Existing fake news detection methods aim to detect intentionally deceptive news. Unfortunately, these approaches are inadequate to automatically and accurately pinpoint fake news from a massive amount of new data that is continuously generated by social media and web services. To address this gap, we propose a novel two-phase approach to detecting fake news. In phase one, we extract events from legitimate news, which are then categorized into an array of topic clusters. Each cluster is centered around a news topic. In phase two, a news item to be verified is classified into a topic cluster, where we validate the events reported in the news by comparing to those in the topic cluster. This approach is inspired by fake news detection demands (Rubin, Conroy, Chen, & Cornwell, 2016) and is reliant on text clustering and classification approaches (Lin, Jiang, & Lee, 2014; Wang et al., 2016), as well as lexical databases (Miller, 1995; Wei, Lu, Chang, Zhou, & Bao, 2015).

Recently developed fact checking tools are adept at comparing news against a collection of knowledge represented as a network. However, such comparisons are very time consuming due to the volume and constant growth of the knowledge base. To speed up the detection performance, we propose to partition a large number of genuine and authenticate news (a.k.a., factual statements) into clusters, each of which is comprised of news sharing similar topics. To judge the credibility of a news, we classify the news into a topic cluster in which events are compared against those of the news. In case the news does not fall into any existing cluster, we mark the news as a deceptive one.

We demonstrate the implementation of the proposed approach for detecting fake news by carrying out two distinctive phases to discover deceptive news. First, trustworthy news are categorized into clusters according to topics. Each cluster is centered around common news topics. Second, we detect fake news by verifying events extracted from the news in a specific cluster.

The approach proposed in this study treats news as a fake one if (1) it is a news outlier (i.e., not classified in any topic cluster) or (2) the similarity between the news events and those of the cluster is below a specified threshold. A large number of authenticated news articles classified into news clusters based on topics and stored in a news database that periodically receives news updates by accumulating latest news stories from legitimate news sources such as CNN and Fox News that have been verified as legitimate by the research community. If an incoming news to be detected cannot be classified into any existing news cluster, it is marked as a candidate fake news. Otherwise, the incoming news is placed into the corresponding cluster for further analysis. The credibility of the incoming news is measured by comparing the events extracted from the news with those in the news cluster. When the news article's credibility is below a specified threshold, the news are classified as fake.

This study makes several contributions. First, a novel analytics-based approach for fake news detection that applies topic based classifying mechanism to group legitimate news into multiple topic clusters is presented. News in each cluster share common topics. An event-extraction mechanism is designed for extracting events from these news articles. Second, we propose and implement a credibility measure for evaluating the authenticity of any news by comparing events extracted from the news to those of the legitimate news. Third, based on the proposed approach, we present a framework for the development and validation of a novel system, *FEND*, to detect fake news by leveraging a large legitimate news database that we built. Finally, we illustrate how to evaluate the performance of *FEND* using a real-world news dataset. The experimental results indicate that *FEND* achieves a high fake news detection accuracy.

2. Literature review

2.1. Fake news risks

The initiation and spread of fake news presents significant risks from many different perspectives, including from a national security standpoint. A good example of this is deliberately misleading news that attempt to influence an individual's perception about another individual or election results. In politically divided environments, such as those being witnessed in the US and Europe, people tend to gravitate towards news from sources that are congenial to their belief or political taste. This may be attributed to confirmation bias or "tunnel vision" which involves one-sided case building based on preconceived notions or ideologies (Nickerson, 1998). Pennycook and Rand (2017) report on three studies aimed at testing the propensity to think analytically and susceptibility to fake news. These studies find that, contrary to the confirmation bias theory, people are deceived by fake news as they fail to think analytically while consuming media, not because they think in a motivated manner. Silverman (2015) discusses various cognitive biases that act as barriers in evaluating and correcting misinformation when humans process fake news, i.e., misinformation. The spread of fake news presents the risk of duping readers that takes disadvantage of the readers' preference for congenial news and the lack of analytical thinking while consuming news media.

The preference for agreeable news bits is further exacerbated with the "echo chamber" or the "filter bubble" phenomenon occurring with social media. On social media platforms, people tend to selectively associate with individuals of similar viewpoints and consume information appealing to their perspectives. The personalization features of social media amplifies the effect (Pariser, 2012). Fake news functions as a catalyst to further intensify readers' point of views and runs the risk of information polarization. Guess, Nyhan, and Reifler (2018) demonstrate the information polarization effect due to differential consumption of fake news occurring through selective exposure to misinformation.

Often, instances of fake news are subsequently followed by fact-checks published on different media outlets. However, as shown by a study conducted by Shin and Thorson (2017), partisan news consumers selectively evaluate and share fact-checking articles, again due to the "echo chamber" effect. Studies on political behavior have shown different results with respect to fact-correction phenomenon. Nyhan and Reifler (2010) found that a "backfire effect" occurs when humans are presented with fact-checks of misinformation, in that they psychologically counter-argue and strengthen their initial false perceptions. However, a recent study by Wood and Porter (2018) has shown no evidence of factual backfiring. From a risk analysis perspective, although fact-checks may be effective in correcting the news for the record, they are practically ineffective in mitigating the risk of false information consumption

Please cite this article as: C. Zhang, A. Gupta and C. Kauten et al., Detecting fake news for reducing misinformation risks using analytics approaches, European Journal of Operational Research, https://doi.org/10.1016/j.ejor.2019.06.022

and information polarization that occurs in the first place. This emphasizes a clear need for more objective fake news detection mechanisms that can serve to prevent the consumption of false or misinformation.

Clearly, fake news presents a keen risk of damaging the foundations of journalism ideals of veracity, objectivity and accountability. Fake news publishers risk accusations of crimes and violations of governmental regulations. Klein and Wueller (2017) present a detailed survey of many legal and regulatory issues that fake news publishers may face. These may range from civil legal claims concerned with defamation, intellectual property law, or intentional infliction of emotional distress (IIED) to government violations and crimes such as cyberbullying. Also, such publishers may be in violation of social media platform account policies and search advertising restrictions. Savvy publishers act to proactively minimize the legal exposure and risks through mechanisms such as disclaimers and notices, website terms and conditions, and media liability insurance policies. In response, social media platforms have become cautious and have started incorporating detection mechanisms for fake news. However, cross-platform mechanisms have received limited attention. Detecting fake news by originating from sources across multiple websites and platforms can serve as a useful tool for regulators.

To mitigate these risks, various detection approaches are discussed in the following subsection.

2.2. Fake news detection

Fake news are created by fabricating nonexistent news or modifying legitimate news. The credibility of fake news are boosted by (1) imitating well-known authors' writing styles or (2) expressing opinions with a tone frequently used in real news. Very recently, an increasing number of fake news detection methods have been developed. All existing detection schemes may be grouped into two distinct classes, namely, linguistic-based methods and network-based methods (Conroy et al., 2015). Network-based approaches for fake news detection apply network properties as a supporting component for various linguistic-based approaches. Commonly used network properties include, but not limited to, website information, authors/subscribers information, time stamps, and the like.For example, Venkatesan, Han, Sharman (2014) performs user behavior analysis to reduce the misinformation in online social networking forum related to Parkinson's disease. This study reports that misinformation embedded within the discussion thread depends on its content and users characteristics of the author. Another study proposes a model that focuses on investigating the quality of responses in an online crowd-sourced health, clarity of the thread questions, and the users' potential for making useful contributions (Venkatesan, Han, Kisekk, Sharman, Kudumula, Jaswal, 2013). The existing sentiment and syntax analysis schemes are customized for special data types, thereby being inadequate for fake news detection systems.

A rumor detection model or CNT proposed by Qazvinian et al. adopts a variety of features such as content-based features (e.g., words and segments appearance, part of speech), network-based features (i.e., re-tweets or tweets propagation) and twitter-specific Memes (i.e., Hashtag or shared URLs). CNT orchestrates an array of strategies to select features to detect misinformation in microblogs (Qazvinian, Rosengren, Radev, & Mei, 2011). Rubin et al. devised an SVM-based algorithm, AHGNA, that embraces five predictive features (i.e., Absurdity, Humor, Grammar, Negative Affect, and Punctuation) (Rubin et al., 2016). After an assortment of feature combinations were evaluated using a total of 360 news articles, Rubin et al. illustrated that the best combination can detect satirical news with a 90% precision and 84% recall. Common fake news features discovered by these approaches may govern unethical writers to write fake news without exhibiting the detectable features. To address this weakness, Hua, Wang, Wang, Zheng, and Zhou (2017) advocate a way of exploiting semantic knowledge from short texts. Hua et al. (2017) scheme incorporates text segmentation, part-of-speech tagging, concept labeling, as well as a vocabulary database to harvest a collection of attributes, concepts and instances from a well-known knowledge base. This knowledge-intensive approach offers insights on short texts such a twitter. While a majority of fake news originates from websites, social media facilitates their spread. Larger text originating from news outlets and opinion threads offer deeper insights into the topic and provide richer contexts. Open information extraction (OIE) is a task of extracting factual information from textual data such as Twitter posts, spams, and articles in social media. More recently, OIE tools have been used for producing grammatical clauses, which can be used for topic extraction purposes. For example, Ghosh and Ghosh (2016) demonstrated their approach by extracting topics from a collection of 50,000 microblogs during a disaster event.

Similar to the above semantic knowledge based approach, our proposed approach aims to grasp an understanding of news through complete comparisons of news content. This approach no longer relies solely on statistical, sentiment, or syntax analysis to detect fake news but uses topic and event level analysis to understand patterns that are deeply embedded within the news for improved detection accuracy. Also, traditional fake news detection approaches pay more attention to reducing content leakage, which may provide misleading information when original articles are imitated or modified. As such, our proposed approach takes full advantage of in-depth semantic analysis of the sentences by incorporating OIE coupled with the other techniques to extract knowledge from news articles.

2.2.1. Sentiment and syntax analysis

Linguistic-based methods such as statistical analysis (Deoras et al., 2013; Xu & Taft, 2015), sentiment analysis (Socher et al., 2013), linguistic cues analysis (Siering, Koch, & Deokar, 2016) and deep syntax analysis (Cinque, 2014; Michalon, Ribeyre, Candito, & Nasr, 2016) have been deployed to detect abnormal information within the text data with high accuracy.

Statistical analysis. Hancock, Woodworth, and Porter (2013) proposed an approach to examining the features of crime narratives. Their results show that psychopaths' speech contain a high frequency of disfluencies; psychopaths often use past tense and less present tense verbs in narratives. Rubin and Lukoianova (2015) proposed the rhetorical structure theory or *RST* to identify the discrepancy between real and fake textual data by applying the Vector Space Model (i.e., VSM) to assess the confidence level for each datum.

Sentiment analysis is a widely adopted strategy for detecting general deception, particularly deceptive Spams. Fusilier, Montes-y Gómez, Rosso, and Cabrera (2015) proposed PU-learning to detect deceptive spams by analyzing positive and negative opinions. PU-learning is a semi-supervised technique for building a binary classifier on the basis of positive (i.e., deceptive opinions) and unlabeled examples.

Linguistic cues analysis. Siering et al. (2016) demonstrate that linguistic cues derived from deception theories, in conjunction with content cues based on message content, can be quite effective in distinguishing between fraudulent and non-fraudulent projects on crowd funding platforms. Deception detection is shown to be particularly effective when both static communication (e.g., project description) is analyzed along with dynamic communication (e.g., forum messages). This study uses a similar approach of analyzing entire communication content, i.e., news, but differs from Siering et al. (2016) study by focusing on the content similarity.

Please cite this article as: C. Zhang, A. Gupta and C. Kauten et al., Detecting fake news for reducing misinformation risks using analytics approaches, European Journal of Operational Research, https://doi.org/10.1016/j.ejor.2019.06.022

Deep syntax analysis. Probability context free grammars or *PCFG* is a practical method that applies deep syntax analysis to separate sentences into rewrite trees representing syntax structures. For example, Feng, Banerjee, and Choi (2012) investigated syntactic stylometry for deception detection, where features are derived from context free grammar (i.e., CFG) parse trees on hotel review data. Unfortunately, these existing detection schemes are tailored for special data types or specific contexts such as spam reviews detection Chen et al. (2017) and spam mail detection (e.g., Iyengar, Kalpana, Kalyankumar, & GunaNandhini, 2017); therefore, are inadequate for a general-purpose fake news detection that could apply to wide ranging topics or issues.

2.2.2. Topic extraction

TextRunner is one of the early, but highly scalable, OIE systems proposed by Banko, Cafarella, Soderland, Broadhead, and Etzioni (2007). Since the inception of TextRunner, a few popular OIE approaches have been developed: *ReVerb* (Etzioni, Fader, Christensen, Soderland, & Mausam, 2011), *OLLIE* (Fader, Soderland, & Etzioni, 2011), and *Stanford OpenIE* (Angeli, Premkumar, & Manning, 2015). In 2013, Del Corro and Gemulla (2013) proposed another OIE approach (ClausIE) that maintains information integrity of original textual data by decomposing sentences into a list of 'clauses'. Another study by Bast and Haussmann (2013) embraces similar extraction phases, but supplements the capabilities of the approach proposed in Del Corro and Gemulla (2013) by implementing contextual sentence decomposition to facilitate semantic searching. Xavier and de Lima (2014) presented a way to extract text relationships without verb expressions. Extraction results were validated by OLLIE and ClausIE. Their findings confirm that more extra relations are discovered by ClausIE than OLLIE, meaning that ClausIE has better performance than OLLIE.

2.3. Fake news detection applications

Recent efforts on fake news detection have focused on varied approaches. For example:

B.S. Detector – alerts users of unreliable news sources (Ravenscraft, 2016) by searching all links of a given webpage for sources that have been collected in a unreliable-news database, which includes samples of fake news, satire, extreme bias, conspiracy theory, rumor mill, state news, junk science, and the like. Although the database manages vital and rich information to facilitate fake-news detection, this approach only utilizes a knowledge base of untrustworthy links. Unlike the browser extension, our approach takes the news content and performs an ingrained analysis to quantify credibility scores.

PolitiFact – is a six-dimensional rating system developed to check facts. It is frequently used to rate the accuracy and credibility of claims made by US officials and others (Roy, 2013). The PolitiFact system largely depends on human intervention, during which, journalists assess information via watching TV, scanning social media, and evaluating reader comments. In contrast to PolitiFact, our system applies artificial intelligence models that utilize text analysis of news sources rather than interventions offered by a body of journalists.

Fake News Detector AI – identifies fake-news websites by measuring similarity to existing fake-news websites using artificial intelligence techniques as a blackbox (Dormehl, 2017). This system uses a neural network–based feature analysis (e.g., headline, code structures, site popularity) approach on known websites, thereby yielding the credibility of the tested websites. Our system differs from this detection tool in the types of features. More specifically, Fake News Detector AI relies on network-based features, whereas our system employs semantic-based features.

3. The analytics model

This section describes the conceptual and mathematical underpinnings of the proposed analytical model developed for establishing the credibility of news articles. We start this section by describing the composition of complete and incomplete sentences. Next, we formally define events and topics extracted from complete sentences. Boolean-value functions that distinguish fake events and topics from legitimate ones are subsequently described. Finally, we describe the mathematical formulation used for quantifying credibility of news articles.

3.1. Topics and events

Fake news could be detected through either topics or events. A news article α consists of a large number of sentences. We model article α as a set of n sentences. Thus, we have

$$\alpha = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}. \tag{1}$$

where each sentence (e.g., σ_i) is expressed as the following triple

$$\sigma_i = (U_i, V_i, O_i), 1 \le i \le n. \tag{2}$$

For the ith sentence σ_i in (2), U_i is a subject set; V_i is a predicate set; and O_i is an object set. Thus, we write these three sets as

$$U_i = \{u_i^1, u_i^2, \ldots u_i^{p_i}\}, 1 \le i \le n. \tag{3}$$

where p_i is the number of subjects in subject set U_i.

$$V_i = \{v_i^1, v_i^2, \ldots v_i^{q_i}\}, 1 \le i \le n. \tag{4}$$

where q_i is the number of predicates in predicate set V_i.

$$O_i = \{o_i^1, o_i^2, \ldots o_i^{r_i}\}, 1 \le i \le n. \tag{5}$$

where r_i is the number of objects in object set O_i.

We categorize sentences in article α into complete sentences and incomplete sentences, depending on the existence of object set O_i in the triple of the ith sentence. We refer to sentence σ_i as a complete sentence if its object set O_i does exist in the sentence triple; otherwise, sentence σ_i is referred to as incomplete sentence (i.e., $O_i = \varnothing$). Hence, the set of sentences for article α can be rewritten as a combination of two disjoint sentence sets S_{ic} and S_{cp}. Note that S_{ic} is a set of incomplete sentences, whereas S_{cp} is a set of complete sentences. Thus, we rewrite (1) as

$$\alpha = S_{ic} \cup S_{cp}, \; S_{ic} \cap S_{cp} = \varnothing, \tag{6}$$

where incomplete sentence set S_{ic} is expressed as

$$S_{ic} = \{\sigma_1', \sigma_2', \ldots, \sigma_m'\}, \tag{7}$$

where incomplete sentence $\sigma_i' = (U_i', V_i', O_i')$ has an empty object set. Thus, we have $O_i' = \varnothing$, and $1 \le i \le m$.

The model proposed in this study detects fake news from complete sentence set S_{cp} rather than from incomplete sentence set S_{ic}; the reason is two-fold. First, incomplete sentences only bear information fragments due to the lack of objects. Second, among the four types of sentences from the language's perspective (i.e., *declarative sentences*, *interrogative sentences*, *imperative sentences* and *exclamatory sentences* (McMenamin, 1993)), declarative sentences – expressing statements – are incomplete sentence.

Let us consider three examples of incomplete sentences.

- *Incomplete Sentence 1:* Lucy is *lying*.
- *Incomplete Sentence 2:* It's *raining* outside.
- *Incomplete Sentence 3:* Water *evaporates* when it's hot.

These sentences have no objects because of the usage of intransitive verbs. The three incomplete sentences provide no details (e.g., Why Lucy lies? or what Lucy said?). In our proposed model,

Please cite this article as: C. Zhang, A. Gupta and C. Kauten et al., Detecting fake news for reducing misinformation risks using analytics approaches, European Journal of Operational Research, https://doi.org/10.1016/j.ejor.2019.06.022

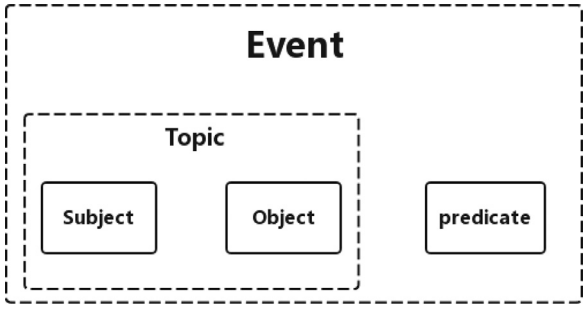


Fig. 1. Relationship between event and topic.

incomplete sentences S_{ic} from article α are pruned during the preprocessing procedure.

Some sentences may contain fake information whereas others might have legitimate information. In what follows, we elaborate on the discrepancy between fake events and fake topics from the perspective of sentences. We start such a comparison by introducing events and topics in a formal way (Fig. 1).

As described above, each event consists of subject, predicate, and object sets. Given sentence $\sigma_i = (U_i, V_i, O_i)$, an event set E_i can be derived from subject set U_i, predicate set V_i, and object set O_i. Let us model such an extraction procedure as an event mapping function x, where E is the Cartesian product of sets U, V, and O. Thus, we have

$$x : U \times V \times O \rightarrow E. \tag{8}$$

Suppose the sizes of sets U_i, V_i, and O_i in sentence σ_i are p_i, q_i, and r_i, respectively. The total number of events extracted from sentence σ_i is a product of p_i, q_i, and r_i (i.e., $p_i \times q_i \times r_i$). Hence, event set E_i of the ith sentence σ_i can be expressed as

$$E_i = \{e_i^1, e_i^2, \ldots, e_i^{w_i}\},\ \ w_i = \ p_i \times q_i \times r_i, \tag{9}$$

where t_i is the total number of events extracted from sentence σ_i.

Let us make use of the following complete sentence (see also (2)) as an example to elaborate the definition of events extracted from sentences in the proposed model.

Complete-Sentence Example 1: A *computer* and a *car* require an *operator* and *power*.

The above complete sentence is expressed as triple $\sigma = (U, V, O)$, where subject set U, predicate set V, and object set O are specified as $U = \{'computer', 'car'\}$, $V = \{'require'\}$ and $O = \{'operator', 'power'\}$. The set sizes p (i.e., $|U|$), q (i.e., $|V|$), and r (i.e., $|O|$) are 2, 1, and 2. 2

In this example, sets U and O consist of multiple elements and set V is a single-element set. We extract one element from each set to form an event. The total number w of events extracted from σ is four, because the product of p, q, and r is 4 (i.e., $w = 2 \times 1 \times 2$).

The *event-set* E of sentence σ is expressed as $E = \{e^1, e^2, \ldots, e^4\}$, which is the Cartesian product of sets U, V, and O. Therefore, the events in set E are written as

- $e^1 = \{'computer', 'require', 'operator'\}$,
- $e^2 = \{'computer', 'require', 'power'\}$,
- $e^3 = \{'car', 'require', 'operator'\}$, and
- $e^4 = \{'car', 'require', 'power'\}$,

The events modeled from a complete sentence (see also (2)) above articulate vital news information on what is happening. After events are extracted from complete sentences in a news article, *FEND* is positioned to compare the article's events against all the events from the legitimate news database. Some extracted events may identical to those in the database, whereas the others may be similar to the events in news database.

We now introduce the concept of *topics* to facilitate news article classification. Since topic-based clustering is more likely to group articles into a small number of clusters compared to event-based counterparts, topic-based clustering is more suitable than event-based news clustering. In our dataset, for example, multiple events are prone to sharing the same topic. This evidence implies that the number of events is larger than the number of topics in a given dataset. More specifically, the number of topics ranges from 4987 to 29,877 in the top 20 clusters; the number of events in these clusters skyrockets to the range anywhere between 52,874 and 210,182.

Given a set A of articles, we aim to classify all the news articles in A into multiple news clusters in accordance to topics, which are defined as subject-object pairs. Let topic t_i^j be the jth topic in sentence σ_i. Topic t_i^j is created in the format of subject-object pair as

$$t_i^j = (u_i^j, o_i^j),\ \ u_i^j \in U_i \ \wedge \ o_i^j \in O_i \tag{10}$$

where u_i^j is a subject in set U_i and o_i^j is an object in set O_i. Topics from sentence σ_i form topic set T_i. Thus, we have

$$T_i = \{t_i^1, t_i^2, \ldots, t_i^w\},\ \ w_i = \ p_i \times q_i \times r_i, \tag{11}$$

Each topic of sentence σ_i (e.g., $t_i^j \in T_i$) can be directly derived from σ_i's event set E_i (see also (9)) by pruning the predicate of each event.

The relationship between event and topic is formally expressed below:

$$e_i^j = (t_i^j,\ v_i^{j_a}),\ \ 1 \le j \le w_i, \tag{12}$$

where $v_i^{j_a}$ is one component of **predicate-set** v_i^j.

Again, let us consider *complete-sentence example 1* (i.e., "A computer and a car require an operator and power"). Four topics extracted from this complete sentence include t_i^1, t_i^2, t_i^3, and t_i^4. The corresponding topics are listed below:

- $t_i^1 = \{'computer', 'operator'\}$,
- $t_i^2 = \{'computer', 'power'\}$,
- $t_i^3 = \{'car', 'operator'\}$,
- $t_i^4 = \{'car', 'power'\}$,

To articulate scenarios where multiple events may share the same topics, we consider another example.

Complete-Sentence Example 2: A *computer* and a *carrequire* and *consume power*.

In the above example, sets U and V consist of two elements; set O is a single-element set. We obtain set $E = \{e^1, e^2, \ldots, e^4\}$, where we have

- $e^1 = \{'computer', 'require', 'power'\}$,
- $e^2 = \{'car', 'require', 'power'\}$,
- $e^3 = \{'computer', 'consume', 'power'\}$, and
- $e^4 = \{'car', 'consume', 'power'\}$,

The topic set in this example is $T = \{t^1, t^2, \ldots, t^4\}$; thus, we have

- $t_i^1 = \{'computer', 'power'\}$,
- $t_i^2 = \{'computer', 'power'\}$,
- $t_i^3 = \{'car', 'power'\}$,
- $t_i^4 = \{'car', 'power'\}$,

We show that topics t_i^1 and t_i^2 identical; similarly, t_i^3 and t_i^4 refer to the same topic. We conclude that in this example, there are two topics – i.e., *('computer', 'power')* and *('car', 'power')* – where each topic appears twice.

Please cite this article as: C. Zhang, A. Gupta and C. Kauten et al., Detecting fake news for reducing misinformation risks using analytics approaches, European Journal of Operational Research, https://doi.org/10.1016/j.ejor.2019.06.022

3.2. Fake events and fake topics

Recall that an event is a triple containing a subject, a predicate, and an object (see (9)). The proposed model acquires a large number of legitimate news articles to build a knowledge base, which in turn assists in detecting untrustworthy articles in terms of credibility. In this study, we treat these legitimate articles as training data fed into the analytics model to build the knowledge base of legitimate news.

We introduce a boolean-valued function f_E to detect if a given event is fake or legitimate. Thus, we have

$$f_E \ : \ U \ \times \ V \ \times \ O \ \rightarrow B_E, \tag{13}$$

where $B_E = \{0, 1\}$ is a boolean domain (i.e., 0 = fake event, 1 = legitimate event).

Similarly, we define a boolean-valued function f_T to determine whether a topic is fake or not. Thus, we have

$$f_T \ : \ U \ \times \ O \ \rightarrow B_T, \tag{14}$$

where $B_T = \{0, 1\}$ is a boolean domain (i.e., 0 = fake topic, 1 = legitimate topic).

Let f_V be a boolean-valued function to signify if a predicate is true or false. Hence, we have

$$f_V \ : \ V \ \rightarrow B_T, \tag{15}$$

where $B_V = \{0, 1\}$ is a boolean domain (i.e., 0 = false predicate, 1 = true predicate).

Given the jth event (i.e., e_i^j) of article α, the value $f_E(e_i^j)$ is derived from the boolean-valued functions $f_T(t_i^j)$ and $f_V(v_i^j)$ as follows:

$$f_E(e_i^j) = f_T(t_i^j) \ \wedge \ f_V(v_i^j). \tag{16}$$

where event e_i^j is comprised of topic t_i^j and v_i^j.

3.3. Metric for credibility and performance evaluation

The credibility of article α is computed through a function $g(\alpha)$, which is derived from boolean-value function f_E (see (13)). The credibility of article α is measured as the percentage of legitimate events in the article. Thus, we have

$$g(\alpha) \ = \ \frac{\sum_{j=1}^{w_i}(f_E(e_i^j))}{w_i}. \tag{17}$$

where α is the test article, w_i is the total number of events in article α, $f_E(e_i^j)$ is the boolean-valued function defined in (13).

Given a news article α, we apply Eq. (17) to quantify the article's credibility. If its credibility drops below a specified threshold (e.g., 0.6), article α will be classified as fake news. For simplicity, we treat all events in articles equally during the credibility calculation stage. In a real-world scenario, an article may tend to be a fake one if a key event is not legitimate. The importance of each event might be represented by its frequency during the classification stage. Unfortunately, millions of events are generated during the fake-news detection phase. It may be assumed that events typically tend to be independent of one another. For example, when we test a dataset of 14,221 articles, we extracted approximately 200,000 topics; the number of events is in the order of magnitude larger that of topics. Consequently, it is impractical to rely on the weights of events to distinguish important events from unimportant ones. Alternatively, event importance could be specified by users, who can manually assign a large weight to an event that is more personally vital than others and vice versa.

Next, we introduce notation $d_{r\rightarrow r}$, $d_{r\rightarrow f}$, $d_{f\rightarrow r}$, and $d_{f\rightarrow f}$ to derive important performance metrics. Let $d_{r\rightarrow r}$ be the number of legitimate news articles truly verified as legitimate ones; $d_{r\rightarrow f}$ is the number of legitimate news falsely detected as fake news; $d_{f\rightarrow r}$ is the number of fake news treated as legitimate news; and $d_{f\rightarrow f}$ is the number of fake news correctly detected as fake ones. We summarize the notation in Table 1.

Table 1
Legitimate and fake news count notation for performance metrics.

Label	Pred	
	real	fake
real	$d_{r\rightarrow r}$	$d_{r\rightarrow f}$
fake	$d_{f\rightarrow r}$	$d_{f\rightarrow f}$

To measure the performance of the fake news detection system, we define four performance metrics using the notation listed in Table 1. These four measures, namely *accuracy*, *precision*, *recall*, and *F-score* are widely adopted in prior studies (Tang et al., 2018; Yang & Siu, 2017).

Let A be an *accuracy* rate, which is the percentage of news that are correctly identified as fake or real news among all news. Thus, A is expressed as (18).

$$A = \frac{d_{r\rightarrow r} \ + \ d_{f\rightarrow f}}{d_{r\rightarrow r} \ + \ d_{r\rightarrow f} \ + \ d_{f\rightarrow r} \ + \ d_{f\rightarrow f}}, \tag{18}$$

P denotes a precision rate, which is the fraction of accurately detected fake news among all the detected fake news. We express precision P as (19).

$$P = \frac{d_{f\rightarrow f}}{d_{r\rightarrow f} \ + \ d_{f\rightarrow f}}, \tag{19}$$

R represents a *recall* rate, which is the fraction of detected fake news among all the ground truth fake news. Hence, recall R can be written as (20).

$$R = \frac{d_{f\rightarrow f}}{d_{f\rightarrow r} \ + \ d_{f\rightarrow f}}, \tag{20}$$

F, or *F-score*, is the harmonic mean of precision P and recall R. Thus, we derive F from P and R as (21).

$$F = \frac{2 \times P \times R}{P + R}. \tag{21}$$

4. Research framework and methodology

In this section, we first introduce the framework describing the proposed methodological approach used for fake news detection. Next we describe the web crawler design with corresponding pseudocode. Third, we illustrate the pipeline of data processing. Finally, we describe the analytics approaches used for clustering and classification of fake news. The entire framework and various components are integrated together to develop a novel fake news detection system, referred to as *FEND* (Fak*E* N*e*ws *D*etection).

4.1. Research framework

Fig. 2 presents the framework that guides the design and development of *FEND*. *FEND* is driven by a ground-truth knowledge base comprised of legitimate-news clusters and corresponding verb lists. The model-training framework that drives the functioning of *FEND* creates clusters based on topics such that news articles in the same cluster share a set of topics. Articles classified in separate clusters have distinctive topic sets.

Fake news is detected through two subsequent phases (see Fig. 10), namely, (1) fake-topics detection using news clusters and (2) the fake-predicate detection through verb comparisons. News clusters are assembled according to news topics; a news article is believed to be fake when (1) the news cannot be classified into any

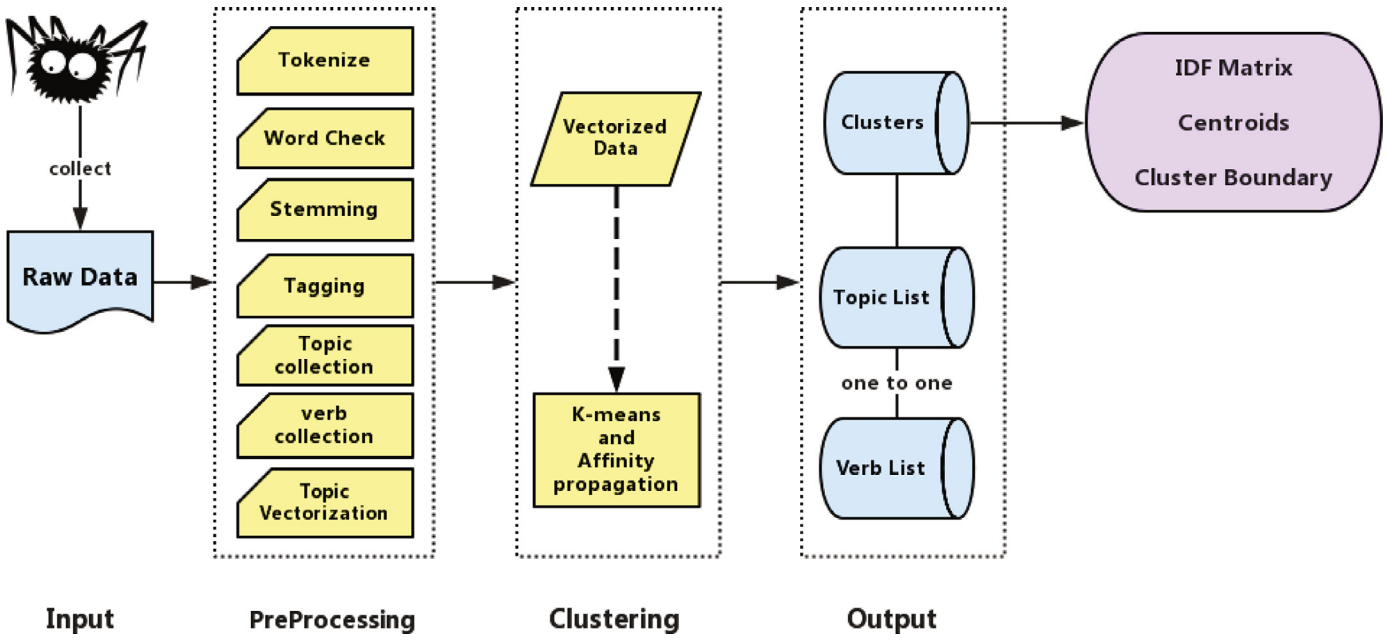


Fig. 2. Model-training framework builds ground-truth knowledge bases by classifying legitimate news articles into news clusters.

cluster or (2) its verbs have a low similarity level with the corresponding verbs in its news cluster.

Handling the synonyms of words is a critical issue to be addressed. Our proposed models address this issue in several ways by incorporating approaches such as lemmatization, stemming, and parts-of-speech tagging to ensure redundant or noisy data is removed during the pre-processing phase. In particular, we employ a list of functions available from the WordNet library (Fellbaum, 2010; Miller, 1995) to detect synonyms of the predicate of an event in a verb list. Such a detection procedure is outlined as follows:

- the first step is to exploit all synonym arguments of predicate and each word in the verb list.
- the second step is to traverse and compare the current tested predicate with each verb in the contrasted verb list with respect to synonym arguments, thereby obtaining the largest similarity between argument pairs.
- the last step is to collect a specified number (e.g., 100) of synonym pairs to approximate a low similarity boundary (e.g., 86.6%), which is compared against the largest similarity obtained in step 2 to determine the synonyms.

To illustrate the above three steps, let us consider the following example. The word *'consume'* has six synonym arguments, namely, (1) *'devour.v.03'*, (2) *'consume.v.02'*, (3) *'consume.v.03'*, (4) *'consume.v.04'*, (5) *'consume.v.05'*, and (6) *'consume.v.06'*. The argument format is *'Word.POS.Sense'*, where *POS* is word type and *Sense* is the word's frequency count for a particular meaning of that word. The word 'expend' only contains two synonym arguments, including *'use.v.03'* and *'spend.v.02'*. Next, we compare and calculate the similarity of each argument pair, where one argument is from word *'consume'* and another one is from word *'expend'*. The last step is to greedily pick the largest value among all similarities as a reference to determine if these two words are synonyms. The framework presented in Figs. 2 and 3 present seamless integration of the training and the testing procedure.

The framework presents seamless integration of the training procedure and the testing procedure, and comprises three modules: the training data collection module, the data pre-processing module, and the news clustering module. The training data collection module acquires raw data from legitimate news websites and removes noise such as advertisements; we implement this module using a custom web crawler designed specifically for building the repository and performing in a data streaming fashion. The data pre-processing module integrates an array of text processing techniques to extract topics and events from the newly collected news data. The clustering module classifies the news articles into separate groups according to the extracted events. The output database maintains news clusters, each of which is coupled with a corresponding verb list. This output database serves as ground truth to validate the credibility of other incoming news articles.

Fig. 3 outlines the framework that applies the trained model built from the existing legitimate news data to detect fake news. The fake news detection framework consists of a data pre-processing module, a filtering module, and a verification module. The input of the data pre-processing module is the same as that of the first module in the aforementioned model training framework. The input data (i.e., raw data) is either extracted from training data or collected from fake news websites using a web crawler. The pre-processing module not only deploys all the components of the training data pre-processing module, but also vectorizes topics of testing data using the *IDF weights matrix* (Inverse document frequency), which is extracted from the training procedure to ensure the consistency of vectorization. Similarly, the pre-processing module exploits topics and events of each testing data to produce vectorized data as well as the corresponding *verb list*. The second module (i.e., the filtering module) employs a two-layer filtering procedure. The first layer filtrates testing data that fail in falling into any news cluster; these type of news are detected by the filter as fake news. The second layer of the filtering module is in charge of comparing the verb list of each remaining testing data with the verb list of the corresponding cluster to quantify the credibility of each of remaining testing data. The last module (i.e., the verification module) identifies fake news and real news using a threshold, which is specified in accordance to the credibility of all the testing data. The fake news detection framework discovers fake news and outlier news that falls outside of extracted news clusters.

We make use of the following example to shed light on how our algorithm can be executed from the training phase to the testing phase.

Please cite this article as: C. Zhang, A. Gupta and C. Kauten et al., Detecting fake news for reducing misinformation risks using analytics approaches, European Journal of Operational Research, https://doi.org/10.1016/j.ejor.2019.06.022

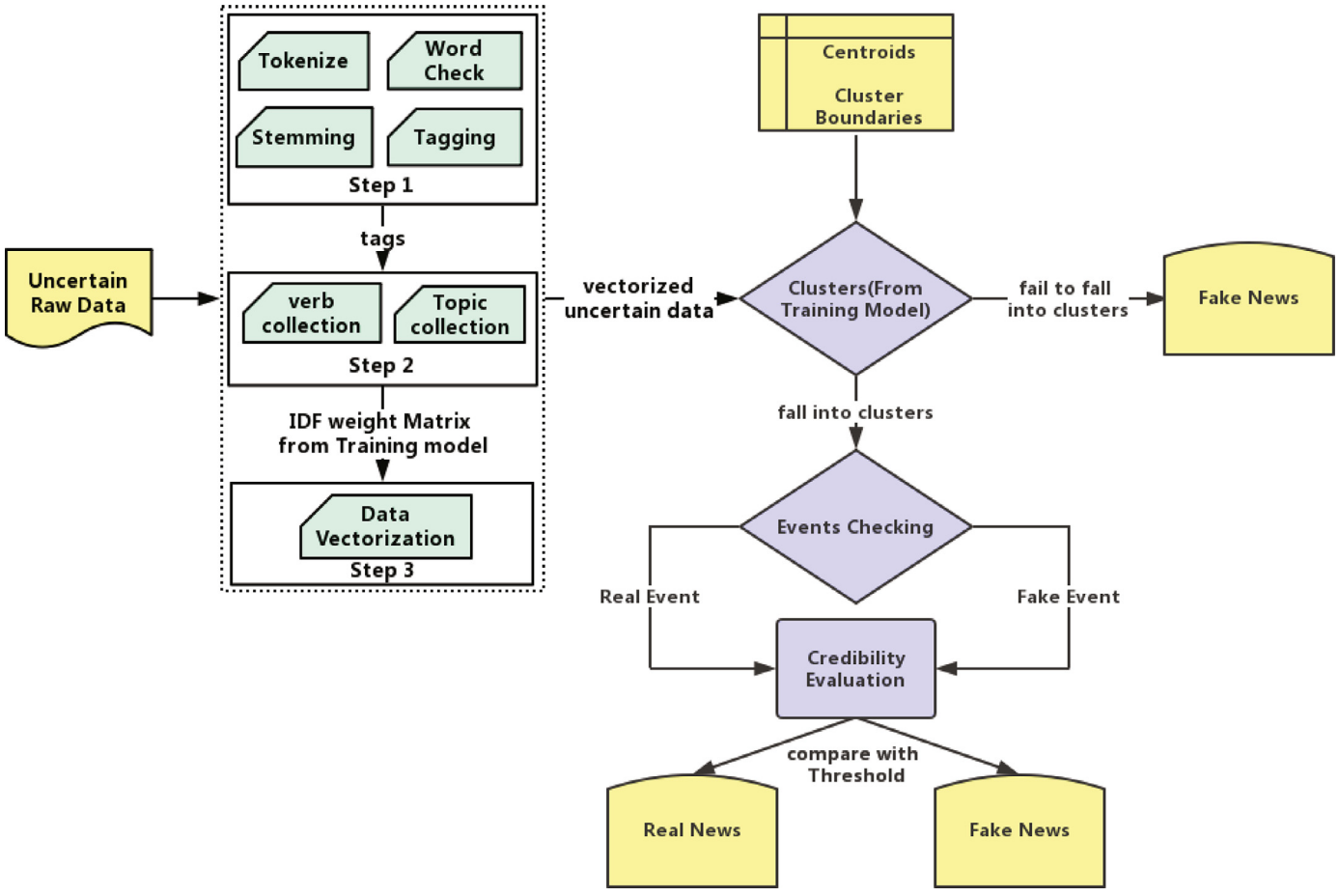


Fig. 3. Fake news detection framework includes two filters: (1) the news that cannot be classified into any cluster or (2) its verbs have a low similarity level with the corresponding verbs in its news cluster.

Table 2
Two clusters are obtained in the training phase. Topics and verbs are extracted for the two clusters (i.e., clusters 1 and 2) and the test data (i.e., article 7).

Cluster	Articles	Topics	Verbs(In format: topic corresponding verb list)
Cluster 1	1, 3, 4	'abc', 'abd', 'acd'	a{a'}, b{b', b"}, c{c', c", c""}, d{d', d", d"', d""}
Cluster 2	2, 5, 6	'aef', 'bef', 'cef'	a{a'}, b{b', b"}, c{c', c", c""}, e{e', e"}, f{f', f", f"'}
	7 (tested article)	'defg'	d{d', d""}, e{e"'}, f{f', f"', f""}, g{g', g"}

Example 3: Let us consider two clusters obtained in the training phase. We list the two clusters in which cluster 1 contains three articles (i.e., articles 1, 3, and 4) whereas cluster 2 is comprised of the other three articles (i.e., article 2, 5, and 6); article 7 is a testing sample. We summarize the two clusters and the tested news along with their topics and verbs in Table 2.

Now we evaluate the credibility of the tested data in the above example. The tested data (i.e., article 7) belongs to cluster 2, in which article 7's credibility can be quantified as follows. In topic list 'defg', element topic d includes one legitimate and one fake verb. Similarly, we determine the number of legitimate and fake verbs for the other topics (i.e., e, f, and g) in the list. Thus, we have e (0 legitimate and 1 fake), f (2 legitimate and 1 fake). In this example, topic g turns out to be an emergent topic in which all the verbs (i.e., g' and g") are treated as fake. Hence, we have g (0 legitimate and 2 fake). For tested article 7, its total number of verbs (a.k.a., events) is eight (8), among which three (3) are legitimate verbs. Consequently, the credibility of the tested data (i.e., article 7) is 3/8 or 47.5%.

The fake news detection framework discovers fake news including outlier news by identifying news items that fail to fall into any news clusters. The *FEND* system can be applied in two phases, namely, fake topics detection and fake events detection. We subsequently implement this two phase framework to develop the *FEND* system that can be applied for detecting fake topics and detecting fake events. Subsequent subsections describe various components of the fake news detection framework and *FEND* system.

The three metrics applied to decide if a news is in a cluster include IDF Matrix, coordinates of centroids (a.k.a, vector of centroids), and boundary of centroids (a.k.a, the largest distance between centroids and points in their cluster). IDF matrix is derived from feature weights using the TF-IDF technique explained in Section 4.2. In what follows, we summarize the procedure utilized for deciding if a given tested news is in a cluster.

First step is to extract topics from the given news. This step is also referred to as ' feature extraction. Second step is to vectorize the news using IDF-Matrix and its topics retrieved from Step 1. Third step is to calculate the distance between vectorized news (i.e., the tested one) and the centroid of a current cluster. Finally,

Please cite this article as: C. Zhang, A. Gupta and C. Kauten et al., Detecting fake news for reducing misinformation risks using analytics approaches, European Journal of Operational Research, https://doi.org/10.1016/j.ejor.2019.06.022

the last step is to decide if this news belongs to the compared cluster or not. The news belongs to the cluster if the distance calculated in the previous step is smaller than cluster-1's boundary from centroid. Otherwise, this news is an outlier.

4.2. Method-data processing and clustering

In the fake news detection framework (see also Fig. 2), the raw data aggregated by the web crawler drives the development of the ground-truth and fake news database. To conduct extensive experiments, we develop a universal web crawler to retrieve news from a various websites to be tested by the fake news detection framework. This web crawler – described in detail in Appendix A – facilitates the pre-processing phase of *FEND* with input data as a set of text files, where each file is an individual news accompanied by author information and published data.

We construct a word-processing pipeline (see also Fig. 2) that is capable of extracting events and topics by the virtue of triple extractions using OIEs, word tokenization, word verification, word stemming, word property tagging, event collection, event decomposition (i.e., topic collection), and topic vectorization.

Raw data acquired using the web crawler in the previous steps is subsequently subjected to a series of pre-processing transformations for annotation as well as topic and event extraction. Stanford CoreNLP library (Manning et al., 2014), which provides a pipeline architecture for performing a sequence of linguistic annotation procedures namely, tokenization, tagging, word check, stemming and part-of-speech tagging, was used with Natural Language Toolkit (Bird, Klein, & Loper, 2009), a python based library for natural language processing. Stanford CoreNLP library is among the most popular and advanced open-source libraries available for performing the pre-processing of raw corpus data. Two separate corpus comprises of ground truth and fake news datasets.

The tokenization algorithm segments each document from the ground truth and fake news corpus into a sequence of sentences, each of which is then rendered into a series of 'tokens' – i.e., a single word or a combination of continuous multiple characters. The output of tokenization algorithm is fed to the stemming algorithm, which performs the morphological analysis of each token generated from the tokenization process. This approach removes the redundancy in word frequency counts by truncating the words back to their roots. For example, separate occurrence of words 'know' and 'knowing' within a document is counted as two instances of occurrence of the word 'know' as 'ing' is stripped from the end. The output from stemming is then passed onto part-of-speech (POS) tagging where each tokenized sentences is further annotated with POS tags for entity and relationship detection. These steps help annotate the data into triple representation, which is a combination of subject, predicate and object as defined in Eq. (2).

The process of vectorization converts tokens into numerical vectors for subsequent topic generation. We used Term Frequency-Inverse Document Frequency (TF-IDF) weighted term approach to accomplish this task (Wu, Luk, Wong, & Kwok, 2008). This approach allows weight the term frequency of tokens by the appropriate weight based on their importance for the document. The TF-IDF approach is integrated with document pre-processing pipeline and uses scikit learn library, which is a python based library for machine learning algorithms. TF-IDF approach evaluates the product of term frequency (i.e., TF) measure of each topic occurrence within a document weighted by its importance (i.e., IDF). TF represents the term frequency of each topic while IDF computes the importance of the topic and generates weight matrix for each topic within the dataset. The raw values of TF-IDF are evaluated using below equation

$$tf\text{-}idf(t,d,D) = tf(t,d) \times idf(t,D) \tag{22}$$

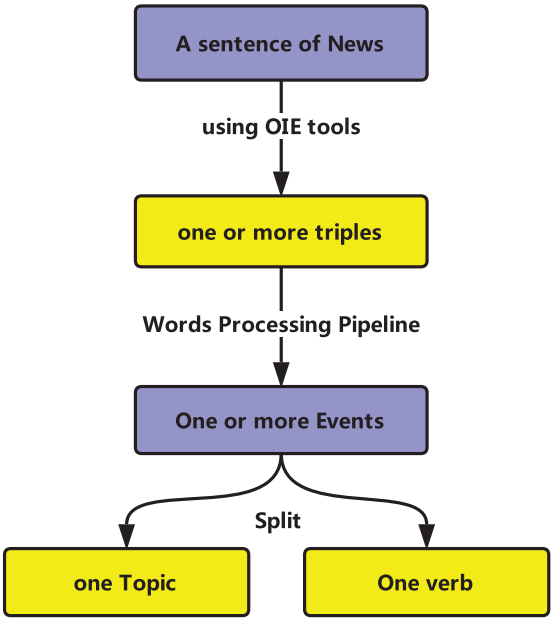


Fig. 4. Process of generating events and topics from news articles: The triple data store connects the OIE tools and the word-processing pipeline. The topic and verb datasets are derived from the event dataset and a verb dataset.

t, d and D denotes a topic, an article and a set of articles in the dataset, respectively. $tf(t, d)$ is used to calculate the frequency of each topic appeared in each article. IDF is evaluated using the below computation

$$idf(d,t) = log\left[\frac{n}{df(d,t)}\right] + 1 \tag{23}$$

Finally, the Euclidian norm is then applied to the raw values of TF-IDF for normalization.

Fig. 4 illustrates the process of generating events and topics from news articles. The triple data store is an internal store connecting the OIE tools and the word-processing pipeline. An event dataset aggregates events extracted by the word-processing pipeline. We implement a module to split the event dataset into a topic dataset and a verb dataset. This enables the classification of news articles in subsequent stages (also see (10) in Section 3.1). In a later phase, the topic dataset drives topic-based news clustering.

We apply two clustering methods, namely k-means and affinity-propagation, to train the models on the three datasets. This strategy allows us to validate our fake news detection theory that treats topics as features of news articles. The rationale behind deploying these two algorithms is two-fold. First, from perspective of implementation, these two clustering algorithms offer ease of implementation in comparison to the other complicated ones. Second, we pick one supervised algorithm (i.e., K-means) and one unsupervised algorithm (i.e., affinity propagation) as an epitome of each algorithm category.

K-means is a classic clustering algorithm in data mining and divides a dataset into k clusters by setting the value of k in advance. K-Means identifies the best centroids by alternating between assigning data points to clusters based on centroids and choosing centroids determined by data points to clusters. The process of the k-means clustering algorithm proceeds as: (1) select k cluster centroids randomly. (2) Calculate the Euclidean Distance between each point and centroids, then save the current clusters. (3) Re-evaluate the distance of data point in each cluster and select the new centroids. (4) Repeat Steps 2 and 3 n times, or until the clusters converge.

Please cite this article as: C. Zhang, A. Gupta and C. Kauten et al., Detecting fake news for reducing misinformation risks using analytics approaches, European Journal of Operational Research, https://doi.org/10.1016/j.ejor.2019.06.022

Table 3
Fake and legitimate news article counts from the website sources.

Type	realNews	fakeNews
CNN	8897	0
New York Times	5334	0
advocate	0	6444
naturalnews	0	2402
politicot	0	3066
greenvillegazette	0	1525

Affinity propagation, proposed by Dueck and Frey (2007), is a popular technique due to its simplicity, ease of applicability, and performance. This scheme relies on the concept of message passing among data points until convergence. Unlike K-means, affinity propagation does not require a-priori specification of the number of clusters. It measures similarity between the pairs of data points while simultaneously considering all the data points as potential exemplars. Real-valued messages are exchanged among data points until a high-quality set of exemplars and corresponding clusters gradually emerges. We articulate the affinity-propagation clustering algorithm by first calculating the responsibilities. Responsibility $r(i, k)$ reflects the accumulated evidence for how well-suited point k is to serve as the exemplar for point i, taking into account other potential exemplars for point i. Responsibility is sent from data point i to candidate exemplar point k. Next, we calculate availability. Availability $a(i, k)$ represents the accumulated evidence for how appropriate it would be for point i to choose point k as its exemplar, taking into account the support from the other points that point k should be an exemplar. Availability is delivered from candidate exemplar point k to point i.

In our experiments, we employ the affinity-propagation (AP) algorithm to perform data clustering. After obtaining the number of news clusters, we apply the number of clusters to the value of k to configure the K-means algorithm. This experimental sequence is important, because K-means algorithm takes the number of clusters as an input parameter. After comparing the clustering results of the K-means and AP algorithms, we discover that the two algorithms yield identical clustering results for input datasets. As such, the credibility of tested news articles remains unchanged regardless of AP or K-means deployed in the training phase. Consequently, the comparisons between these two clustering algorithms are ignored in Section 5.

5. Results and discussion

In this section, we discuss extensive experiments conducted to quantitatively demonstrate the performance strengths of *FEND* using two real-world news datasets. To carry out performance evaluation, we compare our approach with two existing data-mining algorithms with respect to accuracy, precision, recall rate, and *F-score*.

5.1. Datasets

To quantitatively evaluate the effectiveness of our system, we make use of legitimate news available from *CNN* and *New York Times* for model training. Detection accuracy is assessed using various *test datasets*, which are summarized in Table 3. In this study, our news resources such as CNN and New York Times are regarded as legitimate based on the classification done by a large scientist group. They also have wide circulation among larger audience compared with their counterparts (Berkeley, 2018; Mitchell, 2014; OpenSources, 2017). For example, CNN is accessed by approximately 96 million pay-television households, representing 82.8% of households with at least one television set in the U.S. (Staff, 2015).

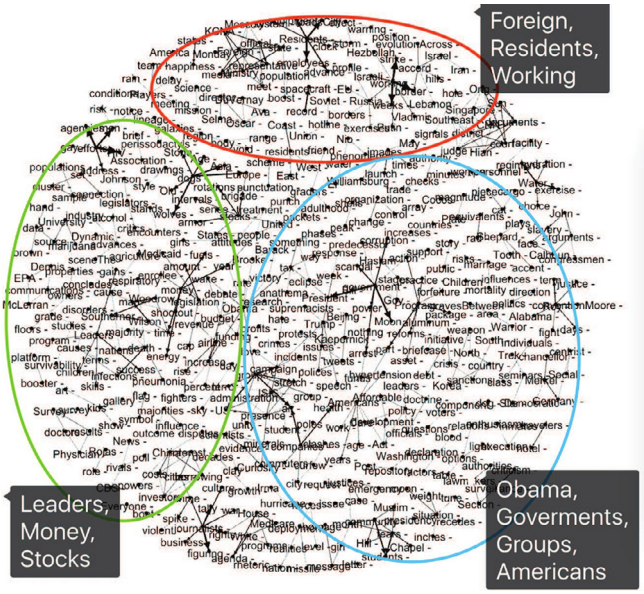


Fig. 5. Network-based topic visualization.

A few viewers may not treat CNN as a legitimate resource because CNN's content is inconsistent with the viewers' opinions. Nonetheless, our system contains a flexible mechanism that allows users to plugin any legitimate news database. Users may choose their trustworthy news outlets for constructing a legitimate news database. Regardless of news database, our system is adept at detecting fake news.

We explore a group of websites classified as fake news domains (Guess et al., 2018) to acquire fake news as ground truth. These websites include, but are not limited to www.greenvillegazette.com,www.politicot.com, www.advocate.com, and www.naturalnews.com. The first three websites publish Pro-Clinton fake news, whereas the last two websites circulates Pro-Trump fake news. News acquired from both Pro-Clinton and Pro-Trump websites drive our unbiased and fair comparison experiments. Note that *Natural News* is a website gaining its popularity from scientific fake news and various conspiracy theories.

5.2. Evaluation

As described earlier, we extract news topics as features using two different clustering techniques, K-means and Affinity Propagation (AP). Both algorithms produced similar number of clusters. However, the composition of the clusters produced using different techniques could have small variation. Both of these approaches apply the euclidean distance as the measure for classifying the data into different clusters. For our dataset, both algorithms produced similar results. We, therefore, focus on clusters produced using AP technique.

Table 4 illustrates selected subjects of 20 clusters that were identified, along with the total number of topics in each cluster. Cluster 1 (see Table 4) is the largest cluster with approx. 29,900 topics and includes subjects such as "foreign", "residents", "workings", "leaders", "stocks", "Obama", "governments", "groups", "Americans", etc. Each of these subjects are associated with various verbs, which make it easier for classifying the articles. On the other end, cluster 20 is the smallest cluster with approx. 5000 topics and includes subjects such as "actress", "theory", "nominations", "film", "tribute", "portrayal", "rewards", "felicity", "spirit", "characters", "actions", etc.

Please cite this article as: C. Zhang, A. Gupta and C. Kauten et al., Detecting fake news for reducing misinformation risks using analytics approaches, European Journal of Operational Research, https://doi.org/10.1016/j.ejor.2019.06.022

Table 4
Article cluster collection for ground truth.

Clusters No.	Subjects (selected)	Number of topics (Repeated topics included)
1	Foreign, residents, workings, leaders, stocks, obama, governments, groups, americans	29,877
2	President, country, policy, children, family, University, government, administration, court, republicans, clinton, immigration	25,318
3	Report, Washington, Facebook, criticism, investigation, department, circumstances, organization	24,476
4	Weapon, chief, authorities, surveillance, peace, contest, Penitentiary, corrections, robbery, violent, surveillance, prisoner, murder	20,386
5	ISIS, adolescent, politico, warning, evil, oceans, deliberation, insult, opponents, correctness, slaughter, panelists, apparatus	19,973
6	Media, trump, campaign, democracy, california, politician, verdict, senate, cnn, nominee, truth, victims	14,323
7	Environment, mediterranean, photographs, hospitals, mountaineers, earthquake, migrant, artists, villages, sight	12,033
8	Devices, databases, company, amazon, business, market, website, engineer, value, worldwide, Google, competitors	10,879
9	Culture, story, police, director, space, blackness, challenge, popularity, experiences, expectations, deficit, motivation, exhibition	9894
10	Ambassador, north, korea, speech, quarantine, surveillance, crisis, policy, conflict, meeting, intelligence, reconnaissance	9435
11	Entrepreneurs, business, startups, guests, experts, incubator, university, recruits, questions, authorities, investigation, photographs, activities	8997
12	Refugees, country, western, violence, police, asylum, extremists, Federal, arrests, Pakistan, psychologist, pursuit	6962
13	Hurricane, Miami, emergency, crosshairs, residents, carolina, economy, Alabama, rumors	6795
14	Gravel, road, accident, license, professor, law, convictions, prosecutors, evidence, instructions, investigators, justice	6580
15	Secretary, military, implementation, tweet, country, defence, fighters, sailors, patriot, freedom, opportunity, democracy, oppression	6439
16	Biases, whites, neighborhoods, relationships, foundation, segregation, marriages, minority, economist, associations, laboratory, interactions	5971
17	Reporters, facebook, survivor, community, firefighter, Twitter, evidence, winners, deputy, photographer, attorney, warrants	5881
18	Olympics, medal, coach, ceremony, champions, reporters, committee, athletes, recognition	5601
19	Sugar, calories, health, vegetables, nutrients, disease, attraction, breaks, textures, deprivation, antioxidants, balance	5033
20	Actress, theory, nominations, film, tribute, portrayal, rewards, felicity, spirit, characters, actions	4987

Table 5
The three topic sub-groups created by the news-topic clustering algorithms.

Topic Zones	Topics
1. Red	Foreign - (representative, KCNA, media, meet, Moscow, Monday, state)...Residents – (area, wave, roadsCity, employees, equipment, advance, storm, clock, system, Coast, East, West, roadsCity).. Workings – (Putin, Vladimir, Russia, Hezbollah, position, border, strike, weeks, Israeli)...
2. Green	Leaders – (gains, policy, children, program, skills, doctrine, grade, success)...Money – (energy, time, legislation, year)...Stocks – (rotations, brigade, armor, intervals, Europe, United, States)... dogs – (Europe, Asia, wolves, Stone, Age, Old)...
3. Blue	Obama – (victory, increase, tax, research, funding, wake, rate, debate, year, Brooke)...Governments – (predecessor, President, Moon, scandal, corruption, arrest, power, nothing)...Groups – (terror, group, Obama, administration, US, air, campaign, stretch)...Americans – (years, age, hypertension, part, work, health)...journalists – (figuring, tally, rights, culture, war, crime, business)

Table 6
The number of fake news detected by the first filter.

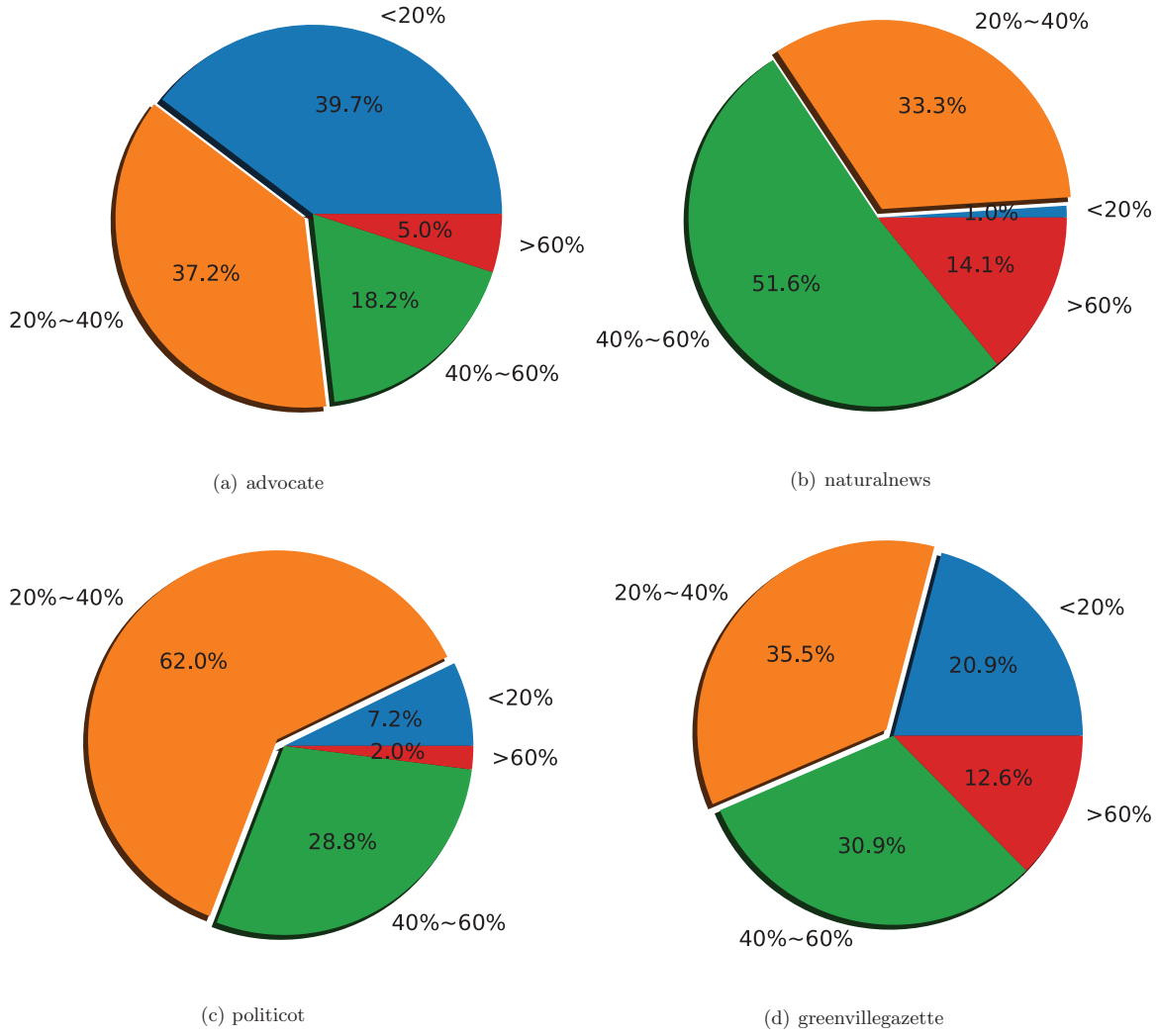
	advocate	naturalnews	politicot	greenvillegazette
Uncertain News	6444	2402	3066	1525
Fake Topics	4312	506	133	478
Remaining Data	2132	1896	2933	1047

Fig. 5 illustrates a network visualization of all the topics belonging to cluster 1, which is the largest cluster. All the topics belonging to the cluster could be grouped into three sub-groups or topic zones. Bolder arrows represent topics occurring with high frequency. In Table 5, we extract almost all of the topics with high frequencies to show the relationship among topics and categorize them based on their sub-groups. For example, “foreign” (representative, KCNA, media, meet, Moscow, Monday, state) identifies one topic (subject-object pair) within the subgroup. Each topic within cluster 1 has relation to the other topics. These results suggest that a particular topic may appear in one article, but may also be identified across multiple similar articles. Our approach performs ingrained fake news classification using two layers of sequential filtering. The first layer of filtering uses the clustering results from the training model to detect the fake news based on any existence of fake topics. The second layer of filtering screens the fake news based on event extraction and credibility evaluation scores. Table 6 summarizes the results after applying the first layer of filtering that is based on topic extraction.

Among all the fake news summarized in Table 6, 66.9% news in advocate.com, 21.1% news in naturalnews.com, 31.4% news in greenvillegazette.com, and 4.4% news in politicot.com are detected as type-1 fake news by the first-level filter. Results suggest that the detection rate of the first-level filter varies significantly across different datasets and shows a wide detection range. For example, the detection rate is the highest for the advocate.com dataset (i.e., 66.9%) and the lowest for the politicot.com dataset (i.e., 4.4%). Over 65% news in advocate.com are correctly detected by the first-level filter, meaning that a large portion of news posted in advocate.com have fake topics (i.e., type-1 fake news). The type-1 fake news detection rates for naturalnews.com and greenvillegazette.com are medium low (i.e., 21.1% and 31.4%), indicating that a majority of news published on naturalnews.com and greenvillegazette.com have legitimate topics. For the news found on politicot.com, only 4.4% are detected as type-1 fake news, suggesting that almost of all the politicot.com news contain trustworthy topics. Results suggest that first filtering layer provides a good mechanism for detecting the reliability of a news source. The output of the first layer feeds to the second layer filter.

The second-level filter detects the credibility of fake news and facilitates the comparison of the individual fake news scores with the threshold ω. Table 7 provides descriptive statistics of remaining

Please cite this article as: C. Zhang, A. Gupta and C. Kauten et al., Detecting fake news for reducing misinformation risks using analytics approaches, European Journal of Operational Research, https://doi.org/10.1016/j.ejor.2019.06.022



(a) advocate (b) naturalnews

(c) politicot (d) greenvillegazette

Fig. 6. the Credibility Distribution of News of all Four Fake News Datasets.

Table 7
Credibility Score Descriptive Statistics for 'Remaining' Fake news.

Fake News	Mean	Range	Std. Deviation
greenvillegazette	0.33	(0.0, 0.88)	0.178
politicot	0.345	(0.1, 0.85)	0.155
naturalnews	0.366	(0.0, 0.67)	0.15
Advocate	0.36	(0.0, 1.0)	0.156

unclassified fake news documents. The average credibility of the fake news is found to have a mean of 0.35, average range of (0.025, 0.85) and average standard deviation of 0.16.

Fig. 6 describes the distribution of credibility scores for each of the four fake news datasets. Each of fake new datasets were found to contain a relatively small proportion of high credibility articles (real news) legitimate articles. For example, advocate dataset contains 5% legitimate news having over 60% credibility, while 77% of news' have credibility lower than 40%. Naturalnews has 14% legitimate news with credibility over 60%, 86% with less than 60% credibility, 34% with less than 40% credibility, and 52% news with credibility between 40% and 60%. Politicot is found to have only 2% news articles with over 60% credibility. Greenvillegazette has more dispersed distribution with 12.4% news articles demonstrating 60% credibility scores. The distribution patterns of fake news suggest that advocate and politicot could be mostly classified as fake news source with fewer than 5% and 2% real news articles respectively. On the other hand, naturalnews and greenvillegazetee has 12–14% real news articles but a more distributed credibility news score. Such websites could be considered as having tendencies for generating fake news content. Fig. 7 shows the performance of two filtering approaches separately as well as collectively. With $\omega = 0.6$, the overall fake news detection performance ranges between 90–97% whereas with $\omega = 0.7$, the overall fake news detection reaches an overall average of 97%.

Next, we carry out four experiments following the three steps. (1) We select 75% news articles (i.e., 10,674 CNN and New York Times news) from the source as training data. (2) We build a model using the training data. (3) The remaining 25% news perform as testing data (i.e., 3,557 news) to validate the model constructed in step 2. The purpose of this cross-validation procedure to evaluate our system's capability of estimating credibility scores of various testing datasets.

Each of the four folds of the testing dataset is populated with the random assignment of news articles drawn from real as well as fake news. Table 8 shows four cross validation data sets.

Table 9 shows the result of cross validation for mixed datasets. The accuracy ranges between 93.77% and 89.55%, pre-

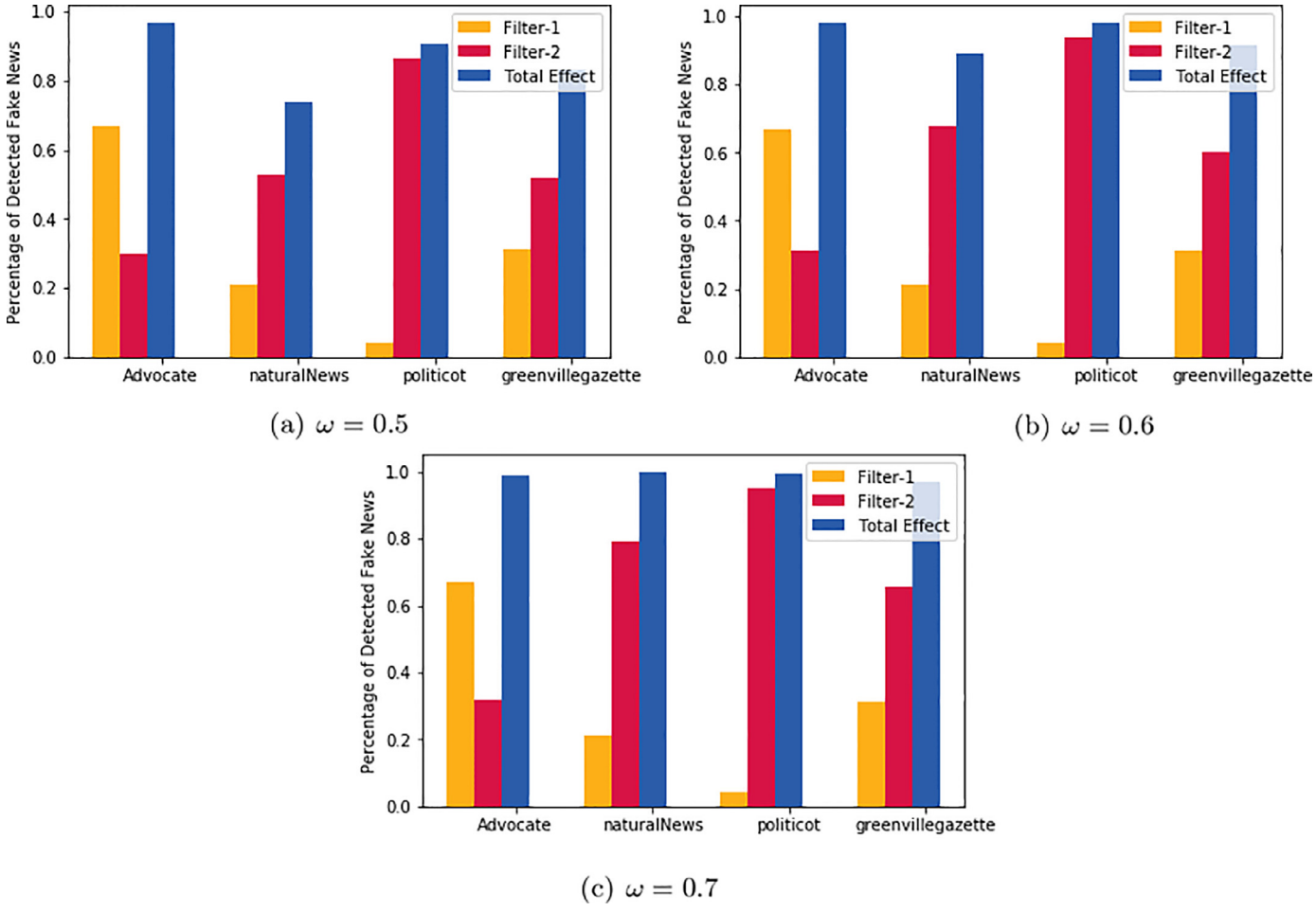


Fig. 7. The performance of two filters in the model.

Table 8
Cross Validation Dataset.

Cross Validation Fold	Corresponding Fake News Dataset	RealNews	FakeNews
1	advocate	3557	6444
2	naturalnews	3557	2402
3	politicot	3558	3066
4	greenvillegazette	3557	1525

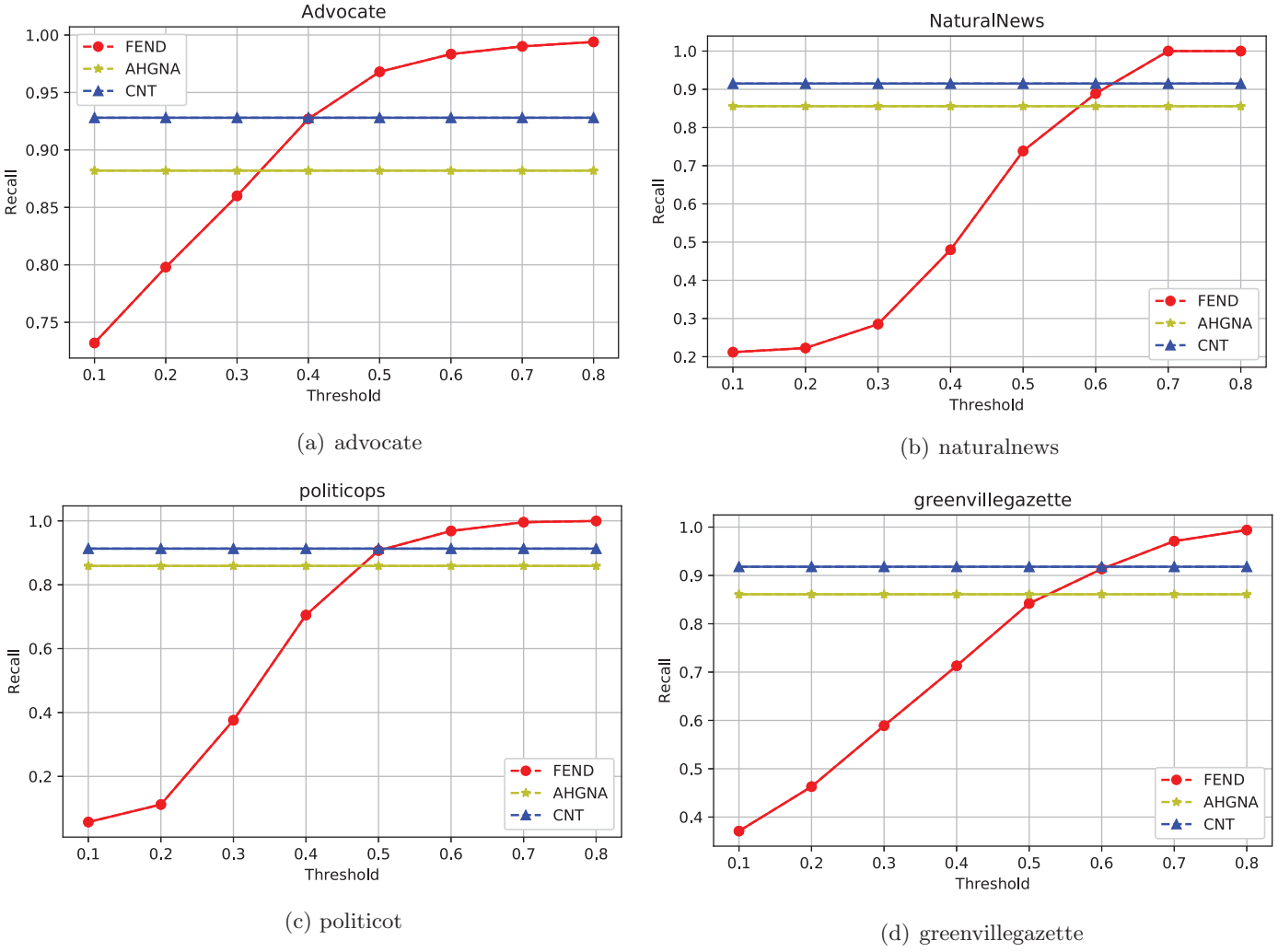
Table 9
Performance Evaluation (use $\omega = 0.6$ as the default threshold for mixed dataset).

Cross Validation Fold	Accuracy	Precision	Recall	F-score
1 (advocate)	93.99%	92.77%	98.34%	95.47%
2 (naturalNews)	91.09%	89.00%	88.88%	88.94%
3 (politicot)	92.27%	86.92%	98.08%	92.16%
4 (greenvillegazette)	92.62%	85.13%	91.34%	88.12%

cision ranges between 92.77% and 83.13%, recall rate ranges between 97.91% and 92.42%, and F-score ranges between 94.91% and 88.31%. Based on the accuracy and recall definitions from Eqs. (18) and (20), recall values for pure fake news and mixed datasets are equal to the the accuracy values of pure fake news datasets.

We further investigate the recall and accuracy of the proposed approach by comparing its efficacy with two other approaches. The first approach is referred to as CNT, a multi-feature detection technique that is based on detecting features: content-based features (such as lexical patterns, part-of-speech pattern), network-based features (e.g. user behavior) and twitter specific memes (e.g., hashtag) (Qazvinian et al., 2011). The second is AHGNA, which uses Absurdity, Humor, Grammar, Negative, and Affect as features for segregating fake or satire from the real (Rubin et al., 2016). Fig. 8 shows the comparison of three approaches based on the recall measure. For higher values of ω, the system built on the proposed approached outperforms CNT and AHGNA approaches. For example, the recall of *FEND* exceeds CNT and AHGNA for ω higher than 0.4 for fake news originating from advocate. Similarly, *FEND* performed better for ω exceeding 0.52 while for politicot news. Finally, for ω greater than 0.6, *FEND* worked better for naturalnews and politicot. Additionally, we found the singled-tailed t-test to be significant at 0.05 as well as 0.01 significance level assuming homoscedasticity. For FEND vs. CNT, p-value is 0.00278 and 0.00015 for FEND vs. AHGNA.

Fig. 9 shows the accuracy comparisons between the proposed method and two baseline methods (i.e., CNT and AHGNA) using the mixed datasets. For a high ω value (e.g., 0.6), our proposed approach outperforms both CNT and AHGNA. For example, Fig. 9(a) reveals that the accuracy of FEND exceeds CNT and AHGNA when the threshold ω is higher than 0.4. More often than not, the



(a) advocate (b) naturalnews

(c) politicot (d) greenvillegazette

Fig. 8. Performance Comparisons among CNT, AHGNA and proposed *FEND* approach based on fake news datasets.

threshold in real-world scenarios is configured in a window between 0.5 and 0.8.

Fig. 10 demonstrates the *F-score* comparisons among FEND, AHGNA, and CNT when threshold ω is configured to 0.6 in the case of four mixed datasets. Fig. 10 illustrates that FEND outperforms AHGNA and CNT in terms of the *F-score* measures. For example, FEND improves AHGNA's *F-score* by up to 4.6% with an average of 2.4%; FEND enhances the CNT's *F-score* by up to 6.2% with an average of 3.3%.

6. Conclusion and future work

Research on fake news is in nascent stages. As fake news becomes more permeated and difficult to detect, increasingly sophisticated approaches are needed to detect fake news. The misinformation spread by fake news poses serious risk for its consumers and target, which could be individuals as well as enterprises. While an individual consuming the fake news develops distorted or misinterpreted perception of reality, which influences their beliefs and decision making, enterprises suffer from fake news due to loss of competitive advantage or damaging impact on their brand. In this study, we propose a novel analytics-driven framework for detecting fake news. We then describe the *FEND* system, which implements the proposed framework for fake news detection and provides its validation. This study also required the development a comprehensive repository of real and fake news which may be utilized for developing future work in this important area of research. This framework utilizes a double-layered approach for classification. The first layer performs fake topic detection and the second layer performs fake event detection, leading to an overall average accuracy of 91.9%. Our approach is novel in the sense that each news article is translated into events, which departs from the traditional approaches of fake news detection that are merely based on syntax rules or sentiments. Our main objective in this study is to develop models that can deal with fake news detection, which is a challenging problem and poses risk for wide sector of population and organizations.

The study has several limitations. There is a focused stream of research on distinguishing fact versus opinion articles (e.g., Mullick, Maheshwari, C., Goyal, & Ganguly, 2017; Rashkin, Choi, Jang, Volkova, & Choi, 2017; Sahu & Majumdar, 2017; Stepinski & Mittal, 2007). We also note that there are other types of news categories, like satire, which are outside the scope of this study, but can be an area of future research based on recent studies (e.g., Golbeck et al., 2018; Rubin, Chen, & Conroy, 2015b). Future studies could specifically focus on models trained on opinions and perspectives. Validation of such a dataset for training purposes may require additional steps to reliably classify

Please cite this article as: C. Zhang, A. Gupta and C. Kauten et al., Detecting fake news for reducing misinformation risks using analytics approaches, European Journal of Operational Research, https://doi.org/10.1016/j.ejor.2019.06.022

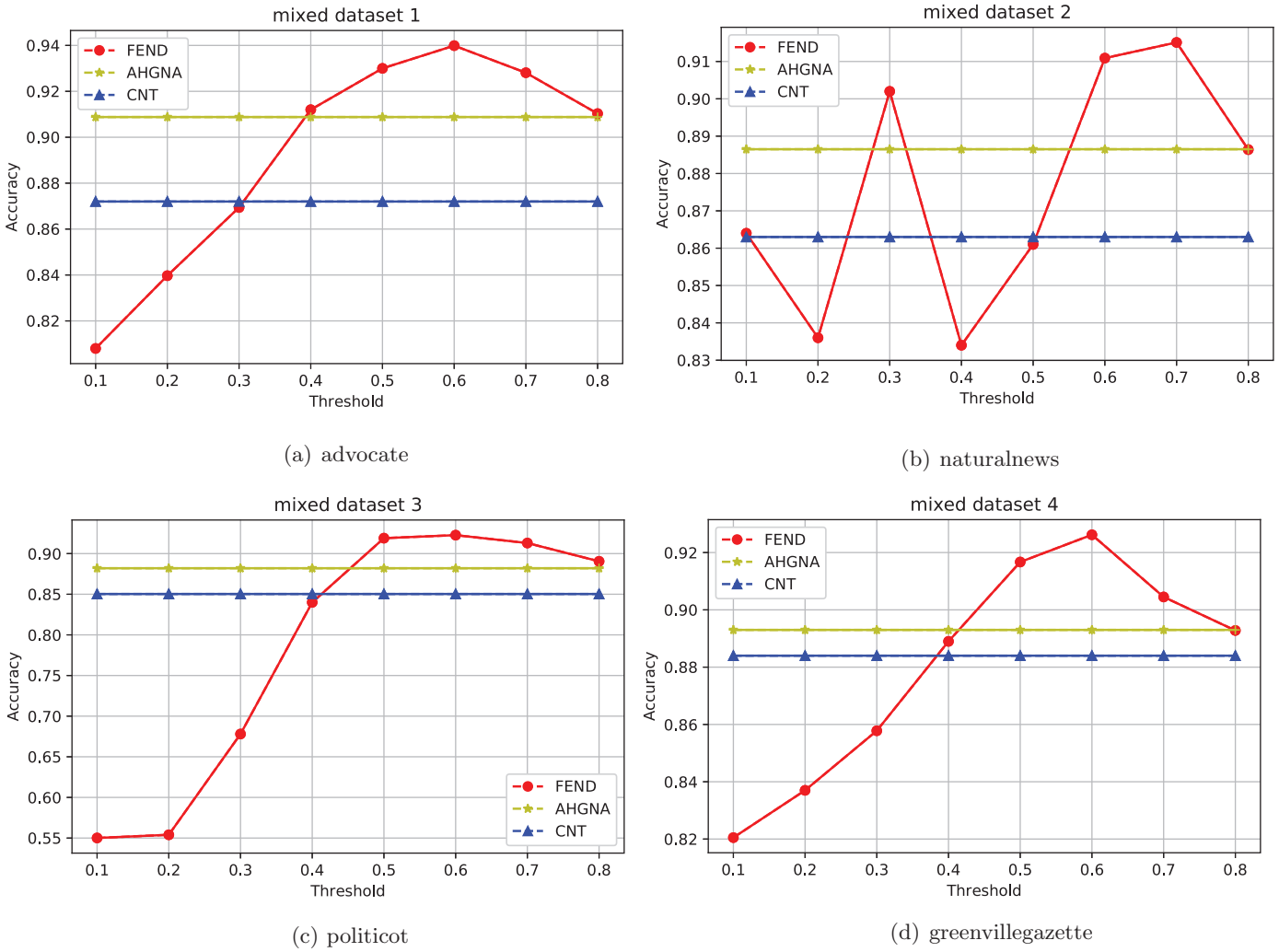


Fig. 9. Performance Comparisons among CNT, AHGNA and proposed *FEND* approach based on mixed datasets.

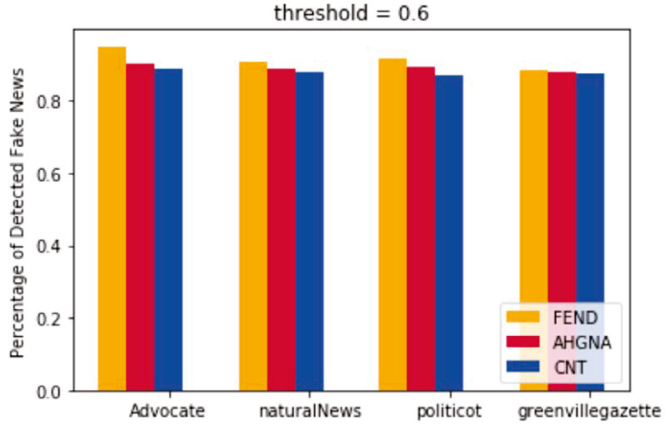


Fig. 10. F-score comparison between FEND, AHGNA, and CNT when $\omega = 0.6$.

them. This study uses clustering approaches to segregate fake news from the real news. Future work on fake news detection can focus on using advanced approaches such as deep learning. The validation of the *FEND* system that implements the proposed framework is done using the fake news repository developed from four different web sources. Future work ought to utilize more data from wide sources of fake news outlets. Such data could also be supplemented from social media sources such as Facebook, Twitter, Reddit, etc. While this study was conducted on a single node graphical processing unit (GPU), development of real time analytics approaches that utilize streaming data from social media sources and the capabilities of GPU enabled computing clusters could help with real-time identification of fake news. This study is an important attempt towards curbing the risks imposed by fake news through timely identification using analytics approaches. Additionally, we believe that allowing users to specify the importance of each event by assigning a weight based on their knowledge of the event could further improve our proposed model. A large weight value indicates an event is more important than the other event. This enables an individual's knowledge to be factored into the model.

A majority of news articles are time sensitive, implying that better fake-news detection may be handled in real-time. To deal with real-time news, models need to incorporate a pre-processing module to process real-time properties of news articles. The development of such real-time pre-processing module is beyond the current scope of this study but is an interesting topic for future research. Such a model will have the capabilities to also handle new and emerging fake news topics.

Please cite this article as: C. Zhang, A. Gupta and C. Kauten et al., Detecting fake news for reducing misinformation risks using analytics approaches, European Journal of Operational Research, https://doi.org/10.1016/j.ejor.2019.06.022

Appendix A. The web crawler

Algorithm 1: The process of web crawler design.

```
Input : A list – list – urls for URLs of all desired websites' homepage
Output: A collection of csv files for all websites
for parse url from list – urls: do
    save all urls which are parsed from url into list – sub – urls.;
    name = get name of current website;
    new name.csv for data saving.;
    for sub – url in list – sub – urls do
        if sub – url is Null then
            continue list – sub – urls.next;
        else
            content = get content from sub – url;
            author = get author name from sub – url;
            ejodate = get published time from sub – url;
            section = get article section from sub – url;
            url = get url from sub – url;
        end
        save url in name.csv;
        if author is Null then
            author = 'unknown';
            save author in file.csv;
        end
        if date is Null then
            date = 'unknown';
            save date in file.csv;
        end
        if section is Null then
            section = 'unknown';
            save section in file.csv;
        end
    end
end
```

The raw data collected by the web crawler include news from both authentic news websites and a set of fake news websites. We develop and implement a universal web crawler to aggregate data from various types of legitimate and fake news websites. The web crawler implementation is non-trivial, because various websites use very different tagging methods. A novel feature of our web crawler developed for this purposes is to tackle such a tagging – diversity problem since fake news data originates from a variety of web sources.

In the web crawler algorithm, we apply the *regular expression* approach for accomplish tags searching. While various websites may adopt different tagging methods, website designers typically use meaningful tags for the convenience of management. For example, the tag of news content should include keywords – 'content', or the tag of news authors should include keywords – 'author'. It is worth noting that not all of the 'content' tags meet the analysis needs due to tag 'noises' to be removed prior to model training. Tags in HTML are formed in a tree structure, where each tag has two attributes, namely, title and depth. Given a news website, we observe that news contents to be collected share the similar depth, suggesting that the web crawler may acquire news contents using the depth of tags. Note that these tags may have various depths in different websites. To address this concern, we add a third attribute – length – to recognize the content of interest in a webpage. If tag lengths is below a fixed threshold, corresponding news articles are treated as noise. This is because short articles fail in furnishing rich information for data analysis. The pseudocode for the web crawler collecting raw data is described above.

Appendix B. Link for data and codes

Links for data and code have been redacted for review purposes. They will be inserted after the review process is complete.

References

Abrahams, A. S., Fan, W., Wang, G. A., Zhang, Z. J., & Jiao, J. (2015). An integrated text analytic framework for product defect discovery. *Production and Operations Management, 24*(6), 975–990. doi:10.1111/poms.12303. https://onlinelibrary.wiley.com

Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Technical report*. National Bureau of Economic Research.

Angeli, G., Premkumar, M. J. J., & Manning, C. D. (2015). Leveraging linguistic structure for open domain information extraction. In *Proceedings of the fifty-third annual meeting of the association for computational linguistics and the seventh international joint conference on natural language processing (volume 1: Long papers): 1* (pp. 344–354).

Banko, M., Cafarella, M. J., Soderland, S., Broadhead, M., & Etzioni, O. (2007). Open information extraction from the web.. In *Proceedings of the IJCAI: 7* (pp. 2670–2676).

Bast, H., & Haussmann, E. (2013). Open information extraction via contextual sentence decomposition. In *Proceedings of the 2013 IEEE seventh international conference on Semantic computing (ICSC)* (pp. 154–159). IEEE.

Berkeley, C. (2018). Evaluating resources: Scholarly & popular sources. http://guides.lib.berkeley.edu/c.php?g=83917&p=3747680 [Online; accessed 20-Feb-2018].

Bird, S., Klein, E., & Loper, E. (2009). *Natural language processing with Python: Analyzing text with the natural language toolkit*. O'Reilly Media, Inc..

Chen, C., Wang, Y., Zhang, J., Xiang, Y., Zhou, W., & Min, G. (2017). Statistical features-based real-time detection of drifted twitter spam. *IEEE Transactions on Information Forensics and Security, 12*(4), 914–925.

Cinque, G. (2014). The semantic classification of adjectives: A view from syntax. *Studies in Chinese Linguistics, 35*(1), 1–30.

Conroy, N. J., Rubin, V. L., & Chen, Y. (2015). Automatic deception detection: Methods for finding fake news. *Proceedings of the Association for Information Science and Technology, 52*(1), 1–4.

Del Corro, L., & Gemulla, R. (2013). Clausie: Clause-based open information extraction. In *Proceedings of the twenty-second international conference on world wide web* (pp. 355–366). ACM.

Deoras, A., Yao, K., He, X., Deng, L., Zweig, G. G., Sarikaya, R., Yu, D., Hwang, M.-Y., & Mesnil, G. (2013). Assignment of semantic labels to a sequence of words using neural network architectures. US Patent App. 14/016,186.

Dormehl, L. (2017). A 19-year-old Stanford student has created a fake news detector AI. https://www.digitaltrends.com/cool-tech/fake-news-detector-ai/ [Online; accessed January 20, 2017].

Dueck, D., & Frey, B. J. (2007). Non-metric affinity propagation for unsupervised image categorization. In *Proceedings of the IEEE eleventh international conference on Computer vision, 2007. ICCV 2007* (pp. 1–8). IEEE.

Etzioni, O., Fader, A., Christensen, J., Soderland, S., & Mausam, M. (2011). Open information extraction: The second generation.. In *Proceedings of the IJCAI: 11* (pp. 3–10).

Fader, A., Soderland, S., & Etzioni, O. (2011). Identifying relations for open information extraction. In *Proceedings of the conference on empirical methods in natural language processing* (pp. 1535–1545). Association for Computational Linguistics.

Fellbaum, C. (2010). Wordnet. In *Theory and applications of ontology: Computer applications* (pp. 231–243). Springer.

Feng, S., Banerjee, R., & Choi, Y. (2012). Syntactic stylometry for deception detection. In *Proceedings of the fiftieth annual meeting of the association for computational linguistics: Short papers-volume 2* (pp. 171–175). Association for Computational Linguistics.

Fisher, M. (2014). Who cares if it's true? Modern-day newsrooms reconsider their values. *Columbia Journalism Review, 52*(6), 14.

Fusilier, D. H., Montes-y Gómez, M., Rosso, P., & Cabrera, R. G. (2015). Detecting positive and negative deceptive opinions using pu-learning. *Information Processing & Management, 51*(4), 433–443.

Ghosh, S., & Ghosh, K. (2016). Overview of the fire 2016 microblog track: Information extraction from microblogs posted during disasters. In *Fire (Working notes)* (pp. 56–61).

Golbeck, J., Mauriello, M., Auxier, B., Bhanushali, K. H., Bonk, C., Bouzaghrane, M. A., … Everett, J. B., et al. (2018). Fake news vs satire: A dataset and analysis. In *Proceedings of the tenth ACM conference on web science* (pp. 17–21). ACM.

Gross, M. (2017). The dangers of a post-truth world.

Guess, A., Nyhan, B., & Reifler, J. (2018). Selective exposure to misinformation: Evidence from the consumption of fake news during the 2016 U.S. presidential campaign. *Technical Report*. Dartmouth College. https://www.dartmouth.edu/~nyhan/fake-news-2016.pdf

Hancock, J. T., Woodworth, M. T., & Porter, S. (2013). Hungry like the wolf: A word–pattern analysis of the language of psychopaths. *Legal and Criminological Psychology, 18*(1), 102–114.

Hua, W., Wang, Z., Wang, H., Zheng, K., & Zhou, X. (2017). Understand short texts by harvesting and analyzing semantic knowledge. *IEEE Transactions on Knowledge and data Engineering, 29*(3), 499–512.
Iyengar, A., Kalpana, G., Kalyankumar, S., & GunaNandhini, S. (2017). Integrated spam detection for multilingual emails. In *Proceedings of the 2017 international conference on Information communication and embedded systems (ICICES)* (pp. 1–4). IEEE.
Jang, S. M., Geng, T., Li, J.-Y. Q., Xia, R., Huang, C.-T., Kim, H., & Tang, J. (2018). A computational approach for examining the roots and spreading patterns of fake news: Evolution tree analysis. *Computers in Human Behavior, 84*, 103–113.
Jin, Z., Cao, J., Jiang, Y.-G., & Zhang, Y. (2014). News credibility evaluation on microblog with a hierarchical propagation model. In *Proceedings of the 2014 IEEE international conference on Data mining (ICDM)* (pp. 230–239). IEEE.
Klein, D. O., & Wueller, J. R. (2017). Fake news: A legal perspective. *Journal of Internet Law, 20*(10), 1,6–13.
Lau, R. Y. K., Zhang, W., & Xu, W. (2018). Parallel aspect-oriented sentiment analysis for sales forecasting with big data. *Production and Operations Management, 27*(10), 1775–1794. doi:10.1111/poms.12737. https://onlinelibrary.wiley.com/doi/abs/10.1111/poms.12737
Li, H., Gupta, A., Zhang, J., & Flor, N. (2018). Who will use augmented reality? An integrated approach based on text analytics and field survey. *European Journal of Operational Research*. doi:10.1016/j.ejor.2018.10.019.
Lin, Y.-S., Jiang, J.-Y., & Lee, S.-J. (2014). A similarity measure for text classification and clustering. *IEEE Transactions on Knowledge and Data Engineering, 26*(7), 1575–1590.
Manning, C., Surdeanu, M., Bauer, J., Finkel, J., Bethard, S., & McClosky, D. (2014). The stanford corenlp natural language processing toolkit. In *Proceedings of fifty-second annual meeting of the association for computational linguistics: system demonstrations* (pp. 55–60).
McMenamin, G. R. (1993). *Forensic stylistics*. Elsevier Science Ltd.
Michalon, O., Ribeyre, C., Candito, M., & Nasr, A. (2016). Deeper syntax for better semantic parsing. In *Coling 2016*.
Miller, G. A. (1995). Wordnet: a lexical database for english. *Communications of the ACM, 38*(11), 39–41.
Mitchell, A. (2014). Which news organization is the most trusted? The answer is complicated.http://www.pewresearch.org/fact-tank/2014/10/30/which-news-organization-is-the-most-trusted-the-answer-is-complicated/ [Online; accessed OCTOBER 30, 2014].
Mullick, A., Maheshwari, S., C. Soumya, Goyal, P., & Ganguly, N. (2017). A generic opinion-fact classifier with application in understanding opinionatedness in various news section. In *Proceedings of the twenty-sixth international conference on world wide web companion*. In *WWW '17 Companion* (pp. 827–828). Republic and Canton of Geneva, Switzerland: International World Wide Web Conferences Steering Committee. doi:10.1145/3041021.3054270.
Nickerson, R. S. (1998). Confirmation bias: A ubiquitous phenomenon in many guises.. *Review of General Psychology, 2*(2), 175–220. doi:10.1037/1089-2680.2.2.175.
Nyhan, B., & Reifler, J. (2010). When corrections fail: The persistence of political misperceptions. *Political Behavior, 32*(2), 303–330.
OpenSources (2017). OpenSources professionally curated lists of online sources, available free for public use. https://docs.google.com/document/d/10eA5-mCZLSS4MQY5QGb5ewC3VAL6pLkT53V_81ZyitM/preview [Online; accessed April 28, 2017].
Pariser, E. (2012). *The filter bubble: how the new personalized web is changing what we read and how we think*. Penguin Books.
Pennycook, G., & Rand, D. G. (2017). Who falls for fake news? The roles of analytic thinking, motivated reasoning, political ideology, and bullshit receptivity. *SSRN Electronic Journal, September*, 1–63. doi:10.2139/ssrn.3023545.
Qazvinian, V., Rosengren, E., Radev, D. R., & Mei, Q. (2011). Rumor has it: Identifying misinformation in microblogs. In *Proceedings of the conference on empirical methods in natural language processing* (pp. 1589–1599). Association for Computational Linguistics.
Rashkin, H., Choi, E., Jang, J. Y., Volkova, S., & Choi, Y. (2017). Truth of varying shades: Analyzing language in fake news and political fact-checking. In *Proceedings of the 2017 conference on empirical methods in natural language processing* (pp. 2931–2937). Association for Computational Linguistics. doi:10.18653/v1/D17-1317.
Ravenscraft, E. (2016). B.S. detector lets you know when you're reading a fake news source. https://lifehacker.com/b-s-detector-lets-you-know-when-youre-reading-a-fake-n-1789084038. [Online; accessed November 19, 2016].
Roy, A. (2013). Pants on fire: Politifact tries to hide that it rated 'true' in 2008 obamacare's 'keep your health plan' promise. https://www.forbes.com/sites/theapothecary/2013/12/27/in-2008-politifacts-2013-lie-of-the-year-that-you-could-keep-your-health-plan-under-obamacare-it-rated-true [Online; accessed December 27, 2013].
Rubin, V. L., Chen, Y., & Conroy, N. J. (2015a). Deception detection for news: three types of fakes. *Proceedings of the Association for Information Science and Technology, 52*(1), 1–4.
Rubin, V. L., Chen, Y., & Conroy, N. J. (2015b). Deception detection for news: Three types of fakes. In *Proceedings of the seventy-eighth ASIS&T annual meeting: Information science with impact: Research in and for the community*. In *ASIST '15* (pp. 83:1–83:4). Silver Springs, MD, USA: American Society for Information Science.
Rubin, V. L., Conroy, N. J., Chen, Y., & Cornwell, S. (2016). Fake news or truth? Using satirical cues to detect potentially misleading news. In *Proceedings of NAACL-HLT* (pp. 7–17).
Rubin, V. L., & Lukoianova, T. (2015). Truth and deception at the rhetorical structure level. *Journal of the Association for Information Science and Technology, 66*(5), 905–917.
Sahu, I., & Majumdar, D. (2017). Detecting factual and non-factual content in news articles. In *Proceedings of the fourth ACM IKDD conferences on data sciences*. In *CODS '17* (pp. 17:1–17:12). New York, NY, USA: ACM. doi:10.1145/3041823.3041837.
Shin, J., & Thorson, K. (2017). Partisan selective sharing: The biased diffusion of fact-checking messages on social media. *Journal of Communication, 67*(2), 233–255. doi:10.1111/jcom.12284.
Siering, M., Koch, J.-A., & Deokar, A. V. (2016). Detecting fraudulent behavior on crowdfunding platforms: The role of linguistic and content-based cues in static and dynamic contexts. *Journal of Management Information Systems, 33*(2), 421–455.
Silverman, C. (2015). Lies, damn lies, and viral content: How news websites spread (and debunk) online rumors, unverified claims, and misinformation. *Technical Report*. New York, NY: Tow Center for Digital Journalism, Columbia Journalism School, Columbia University.
Socher, R., Perelygin, A., Wu, J., Chuang, J., Manning, C. D., Ng, A., & Potts, C. (2013). Recursive deep models for semantic compositionality over a sentiment treebank. In *Proceedings of the 2013 conference on empirical methods in natural language processing* (pp. 1631–1642).
Staff (2015). List of how many homes each cable network is in as of July 2015. https://tvbythenumbers.zap2it.com/reference/list-of-how-many-homes-each-cable-network-is-in-as-of-july-2015/ [Online; accessed JULY 21, 2014].
Stepinski, A., & Mittal, V. (2007). A fact/opinion classifier for news articles. In *Proceedings of the thirtieth annual international ACM sigir conference on research and development in information retrieval*. In *SIGIR '07* (pp. 807–808). New York, NY, USA: ACM. doi:10.1145/1277741.1277919.
Swartz, J. (2017). The world wide web's inventor warns it's in peril on 28th anniversary. *USA Today*. www.usatoday.com/story/tech/news/2017/03/11/world-wide-webs-inventor-warns-s-peril/99005906/
Tang, R., Ouyang, L., Li, C., He, Y., Griffin, M., Taghian, A., … Hughes, K. (2018). Machine learning to parse breast pathology reports in chinese. *Breast Cancer Research and Treatment*, 1–8.
Venkatesan, S., Han, W., Kisekka, V., Sharman, R., Kudumula, V., & Jaswal, H. S. (2013). Misinformation in online health communities'. In *WISP 2012 Proceedings* (p. 28).
Venkatesan, S., Han, W., & Sharman, R. (2014). A response quality model for online health communities. In *Proceedings of the thirty fifth international conference on information systems* (p. 28).
Tsai, M.-F., & Wang, C.-J. (2017). On the risk prediction and analysis of soft information in finance reports. *European Journal of Operational Research, 257*(1), 243–250.
Wang, P., Xu, B., Xu, J., Tian, G., Liu, C.-L., & Hao, H. (2016). Semantic expansion using word embedding clustering and convolutional neural network for improving short text classification. *Neurocomputing, 174*, 806–814.
Wei, T., Lu, Y., Chang, H., Zhou, Q., & Bao, X. (2015). A semantic approach for text clustering using wordnet and lexical chains. *Expert Systems with Applications, 42*(4), 2264–2275.
Wood, T., & Porter, E. (2018). The elusive backfire effect: mass attitudes' steadfast factual adherence. *Political Behavior*, 1–29.
Wu, H. C., Luk, R. W. P., Wong, K. F., & Kwok, K. L. (2008). Interpreting TF-IDF term weights as making relevance decisions. *ACM Transactions on Information Systems (TOIS), 26*(3), 13.
Xavier, C. C., & de Lima, V. L. S. (2014). Boosting open information extraction with noun-based relations. In *Proceedings of the LREC* (pp. 96–100).
Xu, J., & Taft, M. (2015). The effects of semantic transparency and base frequency on the recognition of english complex words.. *Journal of Experimental Psychology: Learning, Memory, and Cognition, 41*(3), 904.
Yang, X.-F., & Siu, W.-C. (2017). Vehicle detection under tough conditions using prioritized feature extraction with shadow recognition. In *Proceedings of the 2017 twenty-second international conference on digital signal processing (DSP)* (pp. 1–5). IEEE.

Please cite this article as: C. Zhang, A. Gupta and C. Kauten et al., Detecting fake news for reducing misinformation risks using analytics approaches, European Journal of Operational Research, https://doi.org/10.1016/j.ejor.2019.06.022