Unsupervised Fake News Detection: A Graph-based Approach


Published in:
31st ACM Conference on Hypertext and Social Media: Proceedings

Document Version:
Peer reviewed version

Queen's University Belfast - Research Portal:
Link to publication record in Queen's University Belfast Research Portal

Publisher rights
© 2020 ACM
This work is made available online in accordance with the publisher's policies. Please refer to any applicable terms of use of the publisher.

General rights
Copyright for the publications made accessible via the Queen's University Belfast Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The Research Portal is Queen's institutional repository that provides access to Queen's research output. Every effort has been made to ensure that content in the Research Portal does not infringe any person's rights, or applicable UK laws. If you discover content in the Research Portal that you believe breaches copyright or violates any law, please contact openaccess@qub.ac.uk.
Unsupervised Fake News Detection: A Graph-based Approach

Siva Charan Reddy Gangireddy
sivag@iiitd.ac.in
IIIT Delhi, India

Cheng Long
c.long@ntu.edu.sg
Nanyang Technological University, Singapore

Deepak P
deepaksp@acm.org
Queen’s University Belfast, UK

Tanmoy Chakraborty
tanmoy@iiitd.ac.in
IIIT Delhi, India

ABSTRACT
Fake news has become more prevalent than ever, correlating with the rise of social media that allows every user to rapidly publish their views or hearsay. Today, fake news spans almost every realm of human activity, across diverse fields such as politics and healthcare. Most existing methods for fake news detection leverage supervised learning methods and expect a large labelled corpus of articles and social media user engagement information, which are often hard, time-consuming and costly to procure. In this paper, we consider the task of unsupervised fake news detection, which considers fake news detection in the absence of labelled historical data. We develop GTUT, a graph-based approach for the task which operates in three phases. Starting off with identifying a seed set of fake and legitimate articles exploiting high-level observations on inter-user behavior in fake news propagation, it progressively expands the labelling to all articles in the dataset. Our technique draws upon graph-based methods such as biclique identification, graph-based feature vector learning and label spreading. Through an extensive empirical evaluation over multiple real-world datasets, we establish the improved effectiveness of our method over state-of-the-art techniques for the task.

ACM Reference Format:

1 INTRODUCTION
Fake news, a term that was barely used until a few years ago, has penetrated into the public discourse rapidly. The choice of post-truth and fake news as the word of the year by Oxford1 and Collins2 dictionaries respectively in consecutive years underlines widespread acknowledgment of its growing prominence. Fake News is commonly used to refer to deliberate presentation of misleading claims [11]. Of late, the news ecosystem has evolved from a small set of regulated and trusted sources to numerous online news sources and social media. Such new media sources come with limited liability for misinformation, and thus have been a major vehicle for fake news. It is also notable that the spread and impact of fake news is facilitated by intrinsic human tendencies such as confirmation bias [7] and the demonstrated inability of people to shrug off influence of fake news even after it has been debunked [29]. These, in the light of studies that suggest that an average US individual read one or more political fake news stories during the presidential election period in 2016 [2], have sparked off serious concerns on the threats that fake news pose to democracy and free debate.

Existing work on fake news detection largely relies on the usage of extensive historical labelled datasets and supervised learning methods that work over them. This is also true with related tasks within the same umbrella, such as rumour identification [34, 46] and hate speech [31]. Given that all of these tasks have a similar structure when viewed from a data science perspective, we will use fake news detection broadly to refer to all of these. Techniques for fake news detection in social media may be broadly seen as exploiting three kinds of information: (i) the (textual or other) content of the news item, (ii) the social network around the user who shares the news item, and (iii) temporal propagation information as gauged through re-tweets, re-shares and mentions. Some techniques have considered usage of only the temporal propagation information [23]; some others make use of both temporal and network information [39] while still not making use of content. While it may be safe to say that sophisticated usage of content has been lacking given most research has been driven by datasets from Twitter which have sparse content information, usage of content has ranged from shallow usage (e.g., counts of mentions, pictures and smileys [43], aggregated tf-idf [22]) to somewhat intricate modelling (e.g., pos-tag patterns [28] and psychological categories [20]).

While supervised methods are the natural first step towards addressing any labelling task, they suffer from several drawbacks. First, supervised methods require significant amounts of labelled data to learn meaningful models for effective detection of fake news. Obtaining manual annotations on veracity is labour-intensive as

1https://languages.oup.com/word-of-the-year/2016/
we as well as time-consuming, and efforts at crowdsourcing the data collection effort may entail quality deterioration [18]. Second, the usage of network and temporal features often lead to learning specific network and temporal behavioral patterns of individual users, sometimes making the effectiveness of the technique dependent on the permanence of users’ network positioning and their behavioral patterns. Third, techniques that make use of content information would be affected by topic drift besides being unable to generalize across natural languages. For example, unless making use of people names is explicitly avoided, an algorithm tuned well on 2016 presidential elections data would be ill-suited for the 2020 edition.

Within that backdrop, we consider the task of *unsupervised fake news detection*. The unsupervised task is significantly more challenging than the supervised version given that unsupervised techniques do not have the luxury of labelled data to guide the search process. Thus, such methods would need to be embedded with high-level assumptions on the user dynamics around fake news. As an example, a recent work on unsupervised fake news detection [41] uses the presumption that *verified users offer credible opinions on the veracity of a news piece*. In contrast to [41], we rely on observations and insights from the *dynamics of inter-user behavior* and use that to design our method for unsupervised fake news detection. Specifically, our technique is designed using the assumption that synchronized behavior in news propagation is intrinsically more prevalent among fake news (vis-a-vis legitimate news). This assumption is motivated by two main observations; (i) that fake news is often driven by monetary, electoral or other gains, making it more likely to be propagated through blackmarket services where collusive user behavior is common [9], (ii) fake news is often driven by the expression of one’s socio-political identity (as identified in a recent BBC study [5]) which would lead to implicit orchestrated behavior across specific cross-sections of the user base.

Our main contributions are as follows:

- We investigate, for the first time to our best knowledge, the usage of inter-user behavior dynamics for the task of unsupervised fake news detection.
- We propose an unsupervised learning method that is driven by graph-based techniques to identify fake and legitimate news.
- Through an extensive set of experiments across real-world datasets, we establish the effectiveness of our method over the state-of-the-art for unsupervised fake news detection.

## 2 RELATED WORK

We cover related work in fake news detection under several different heads as follows.

### Unimodal Approaches.

Majority of the studies on fake news detection are supervised in nature and focus only on the textual part, though some of them additionally use user metadata features. There are also attempts to detect the creator (user accounts) of such fake news. Past research that have successfully detected unreliable accounts include methods using clustering [40] and steganalysis [1] techniques. Researchers have also attempted with methods that target early detection [14]. In addition to this, techniques using random walk and entropy minimization discretization [10] were also experimented with. The other important aspect seen while forging the content is changing its writing style, which has impacts on the reader [27, 33]. This further led to addition of studying another important attribute that studies user opinions in detecting fake news. Another modality that has been popularly used in manipulating information present in news articles is images. The image splicing technique used in [15] takes into account the EXIF meta features to detect fake images. Recent research has also shown the use of GANs [24] forged images in the news articles.

### Multimodal Approaches.

As may be expected, using multiple information modalities for a task, when available, would be more beneficial than just one. Towards this direction, experiments were conducted by extracting features from two different modalities such as text and image. Works on that direction include EANN [37], MVAE [17], SpotFake [36] and SpotFake* [35]. The EANN model, short for event adversarial neural networks, for multimodal fake news detection proposed by [37] consists of three sub-modules namely, textual feature extractor, visual feature extractor and an event discriminator module that when combined together is successful in detecting fake news. Inspired by [37], [17] built a similar architecture, titled as Multimodal Variational Autoencoder for Fake News Detection (MVAE). This architecture too consists of three sub modules. Later methods for the task include SpotFake [36] and SpotFake* [35]. SpotFake extracted features from both the text and image modality. It differs from [17, 37] in not using a secondary task within the formulation. Other multimodal features that recently gained a lot of attention to solve the detection problem are those from social media. Various attributes in the form of user meta information, comments, likes etc. are being used to form a rich feature database that can better assist the detection task. Recently, Cui et al. [6] used opinions of the user gathered via Twitter to draw insights on information present in news that makes it unreliable. This method not only successfully detects a news article to be reliable or not but also adds an explainability quotient to it.

### Knowledge Graph based Approaches.

Analysing the facts in a news proves as an important factor in deciding an information to be true or not. Recent research (Pan et al. [26]) shows the use of knowledge graph in improving the fact checking quality in a news article. Such graphs are capable of modelling semantic information to assess the common sense reasoning present in a news article through statistical methods. For example, TransR model [21] can generate embeddings for entity relation triplets. To learn via KGE, the entities has to be projected from entity space to corresponding relation space. This helps in building translations between projected entities, which could yield insights that aid determining veracity.

### Social Context Based Approaches.

These methods use profile information, network structure and user’s past history to determine news credibility. Castillo et al. [4] used four types of features, namely message-based features, user based features, topic-based features and propagation-based features to classify tweets to be credible or not by a supervised classifier. Jin et al. [16] proposed a method to verify the news by analyzing the conflicting viewpoints of users about the news. They followed a three step process; first, a topic model is used to detect conflicting views about a news; second, a network is created whose vertices are tweets and edges indicate if tweets support or oppose each other; finally, an iterative method is used to deduce the credibility of a news and a process continues...
We use a more general high-level heuristic that relies on assumptions about the relationship between websites and the content present on these websites to determine the truthfulness of a story. An iterative method uses the truthfulness of a link and the trustworthiness of a website to identify a seed set of fake and legitimate articles. Our seed set depends on information used as well as the approach taken to address the task.

Unsupervised Approaches. There have been very limited attempts to detect fake news in an unsupervised manner. One of the prime reasons behind designing an unsupervised method is that fake news varies across the domains – political fake news may be different than the health-related fake news. Therefore, a model that is solely dependent on the content of the news (analyzes only the text) may not generalize well across all the domains. In this direction, Yin et al. [42] made an attempt to discover the true story from multiple sources of the web. They proposed TruthFinder, which considers the relationship between websites and the content present on these websites to determine the truthfulness of a story. An iterative method uses the truthfulness of a link and the trustworthiness of a website to detect the conflicting information present in multiple websites about a story. Recently, Yang et al. [41] proposed UFD, a generative framework based on Bayesian principles by leveraging the opinion of users on the news and their engagements with the social network. Their method relies on the hypothesized increased credibility of the views of verified users. They establish that the extent of engagement (liking, sharing, commenting) of a user varies over time as the news propagates through the network. Apart from the above that address the general fake news problem, there has been work addressing related problems such as identifying political propagandists - specifically, those who seek to align public opinion on contemporary events with the official ‘vision’ - within an unsupervised setting [25].

Differences from Existing Unsupervised Approaches. Our proposed method, GTUT, differs from the two unsupervised fake news detection approaches [41, 42] discussed above in both the kind of information used as well as the approach taken to address the task. We do not limit our approach to those websites where multiple opinions exist on the web (unlike [42]) nor do we limit the ambition to those that are shared by a significant number of verified users [41]. We use a more general high-level heuristic that relies on assumptions about synchronous user behavior, which we believe leads to a more generalizable method. However, we consider both the methods as our baselines for the comparison.

3 PROBLEM DEFINITION

Consider a dataset of news articles, $\mathcal{A} = \{\ldots, A, \ldots\}$, whose veracity needs to be ascertained by labelling them as either fake or legitimate. Let $\mathcal{U} = \{\ldots, U, \ldots\}$ be a set of users in a social network, the user dynamics of which we will use to perform unsupervised fake news detection. The footprint of the news articles within the social media network manifests as a set of posts, $\mathcal{P} = \{\ldots, P, \ldots\}$. Each post $P_i = [U_i, A_i, t_i, c_i]$ is created by a user $U_i$ comprising textual content denoted by $c_i$ mentioning news article $A_i$ at time $t_i$; we are only interested in posts that mention news articles, motivated by the nature of our task. Given that not all social networks expose the underlying social network (directly or indirectly), we make no assumptions about the knowledge of connections between users.

The target of the unsupervised fake news detection method is to make use of $\mathcal{A}$, $\mathcal{U}$, $\mathcal{P}$ in order to estimate a label from $\{F, T\}$ to each article in $\mathcal{A}$, denoted as $\mathcal{L}(A)$ (for $A \in \mathcal{A}$), where $F$ denotes fake and $T$ denotes legitimate/truthful. It may be noted that $\mathcal{U}$ and $\mathcal{P}$ are usually part of the public digital footprint that microblogging services expose, variously referred to as activity log or traces. Following the links within the posts in $\mathcal{P}$ would lead us to $\mathcal{A}$. Thus, all of $\{\mathcal{A}, \mathcal{U}, \mathcal{P}\}$ are easily available in typical scenarios.

3.1 Evaluation

The effectiveness of the unsupervised learning method would be determined on the basis of the correctness of the assigned labels gauged against a set of manually labelled articles. As may be obvious, the manual labellings would be used only for the purposes of evaluation and would be unavailable to the learning technique itself. We will use classical metrics such as precision, recall and F-measure, as will be detailed in the empirical evaluation section.

4 GTUT: OUR METHOD

We now describe our method for unsupervised fake news detection, codenamed GTUT, to indicate the usage of Graph mining methods over Textual, User and Temporal data from social network traces across $\{\mathcal{A}, \mathcal{U}, \mathcal{P}\}$. GTUT is a three phase method that starts by identifying seed fake and legitimate articles in the first phase, and progressively expands the labelling in the second and third phases to cover all articles in $\mathcal{A}$.

4.1 Phase 1: Label Seeding using Bi-cliques

This phase is primarily designed to exploit the high-level observation that fake news is often spread within a social network in a synchronized manner (relative to legitimate news) to ensure wide attention and reach in order to further the monetary, electoral or market incentives that motivate their creation. While this observation is particularly motivated by observing political perception campaigns on Twitter which often use slightly different wordings, this is also facilitated by observations that users’ expression of socio-political leanings yield to prompt propagation of fake news (BBC report [5]). However, given that fake news could propagate through other mechanisms and need not be fully identifiable through synchronized sharing, we only use it as a seeding heuristic in order to identify a seed set of fake and legitimate articles. Our seed set identification relies on identifying synchronous posting behavior involving same articles at similar times through textually similar posts.

We start by modelling a bi-partite graph $\mathcal{G}$ with nodes as articles (i.e., $\mathcal{A}$) and users ($\mathcal{U}$), with an edge induced between a particular user and article iff the user has authored a social media post mentioning the article. The edge, $E_{\mathcal{AU}}$, is labelled with the set of posts involving the user-article pair, given that a user could have authored multiple posts involving the same article.

$$\text{Label}(E_{\mathcal{AU}}) = \{P_i | P_i \in \mathcal{P} \land U_i \subseteq \mathcal{U} \land A_i \subseteq \mathcal{A}\}$$

where $P_i = [U_i, A_i, t_i, c_i]$ as outlined in Section 3. In the interest of identifying similar posting behavior across users involving the same articles, we first identify all maximal bi-cliques [44], denoted as $\mathcal{B}$, in the user-article graph. A bi-clique $B \in \mathcal{B}$ is formed by a set of users $B_U \subseteq \mathcal{U}$ and set of articles $B_A \subseteq \mathcal{A}$ such that there
exists an edge between each user in $B_U$ and each article in $B_A$. A maximal bi-clique is one which cannot be extended by adding users or articles (to the respective sets that form the bi-clique) while still retaining the property of being a bi-clique; maximal bi-clique finding disallows both bi-cliques and bi-cliques formed by their proper subsets being present in the result together, reducing redundancy and enhancing meaningfulness of result sets. Given that a bi-clique is expected to be fully connected, each bi-clique identifies a set of users $B_U$ who have all shared the same set of articles $B_A$. The definition of bi-cliques becomes vague when it approaches low values of $|B_U|$ and $|B_A|$; for example, each edge in the bi-partite graph is a bi-clique with $|B_U| = |B_A| = 1$. Thus, we would like to impose a minimum threshold on $|B_U|$ as well as on $|B_A|$ so we consider only bi-cliques with good connectivity of users and articles. As a thresholding strategy, we choose a threshold of 5 for the number of users, and choose a threshold on the number of articles such that the bi-cliques collectively cover around 40% of articles in the dataset. More details are in the experimental evaluation section.

Having identified users who tweet the same articles by way of bi-cliques, we would like to score the bi-cliques based on whether the component users tweet the articles at similar times using textually similar posts. First, we consider each bi-clique separately, and score each article within the bi-clique on the temporal coherence of social media footprint within the bi-clique. The temporal coherence of an article $A \in B_A$ is estimated as:

$$\text{Temporal}(A \in B_A, B) = \max \left\{ 1 - \frac{\text{BAS}(A,B)}{\tau_{\text{max}}}, 0 \right\}$$

(2)

where $\text{BAS}(A,B)$ denotes what we call as the bursty attention span of article $A$ among users within bi-clique $B$. The span of attention that an article $A$ had gathered among users in $B$ may simply be estimated as the time difference between the latest post involving $A$ and the earliest post involving $A$ (both obviously computed among posts within the bi-clique). However, such an attention span is sensitive to outlier behavior when a single user in $U_B$ posts about $A$ many days after the burst of attention has died down; we have observed cases of stray posts after a year, making this attention span definition very fragile. Thus, we define the bursty attention span as the smallest timespan that encompasses at least 80% of the posts posted about $A$ among users in $B$. The bursty attention span may be greedily computed by simply excluding posts from either end of the temporal window based on what shortens the remaining span maximally, until only 80% of posts remain. The article-specific temporal coherence, $\text{Temporal}(A \in B_A, B)$ of article $A$ within bi-clique $B$ is then computed as being inversely related to the bursty attention span, flattened off beyond a threshold of $\tau_{\text{max}}$. The temporal coherence of the bi-clique is then estimated as the average of the temporal coherence of articles within it:

$$\text{Temporal}(B) = \frac{\sum_{A \in B_A} \text{Temporal}(A,B)}{|B_A|}$$

(3)

We now turn our attention to similarly estimating the textual similarity of posts involving each article $A \in B_A$ within the context of bi-clique $B$. The article level textual similarity is estimated as:

$$\text{Textual}(A \in B_A, B) = \frac{\sum_{(P_x,P_y) \in \text{Posts}(B,A)} \text{sim}(\text{rep}(c_x), \text{rep}(c_y))}{(|\text{Posts}(B,A)|) \times (|\text{Posts}(B,A)| - 1)}$$

(4)

In other words, the above computes the average of pairwise similarities between the textual contents of posts mentioning $A$ posted by users in $B$ (denoted as $\text{Posts}(B,A)$). We use average of pre-trained word2vec representations for $\text{rep}()$ and use cosine as the similarity function $\text{sim}(..)$. Analogous to the temporal case, the textual similarities are aggregated to the bi-clique level:

$$\text{Textual}(B) = \frac{\sum_{A \in B_A} \text{Textual}(A,B)}{|B_A|}$$

(5)

We now score bi-cliques based on how well they fare across the textual and temporal coherence measures using an aggregate scoring modelled as a weighted sum.

$$\text{TTScore}(B) = \lambda \times \text{Temporal}(B) + (1 - \lambda) \times \text{Textual}(B)$$

(6)

We consistently set $\lambda = 0.5$ to give equal weighting for both the scorings. The above offers a bi-clique level scoring; however, given that our task is to label articles, we would like to transfer these scores to the articles. Observe that an article could be part of more than one bi-clique. We estimate the score of an article as the average of scores of the bi-cliques it is part of:

$$\text{TTScore}(A \in B) = \frac{\sum_{B \in B} \text{TTScore}(B)}{|B|}$$

(7)

where $\text{BiClique}(A, B)$ is the set of all bi-cliques in $B$ that contain article $A$. Based on our starting assumptions, articles scoring high on $\text{TTScore}(\cdot)$ would likely be fake and vice versa. We estimate our seed set of fake articles $F_{\text{seed}}$ as the $\tau$ articles that scored highest on $\text{TTScore}$ and the seed set of legitimate articles $T_{\text{seed}}$ as the $\tau$ articles that scored lowest on $\text{TTScore}$. While $\tau$ can be treated as a tunable hyper-parameter, we consistently set $\tau$ to be 5% of articles in $B$.

### 4.2 Phase 2: Label Spreading within Bi-cliques

Having identified seed fake and legitimate articles using synchronous behavior identification which is expected to be more prevalent among fake, we now consider spreading the labels more broadly within $B$ using heuristics that are broadly applicable across fake and legitimate classes. In this phase, our target is to label every article across bi-cliques in $B$. Our heuristic is that articles are likely to be of the same veracity label (i.e., fake or legitimate) if they are (i) part of the same bi-cliques, (ii) have a lot of common users among those who shared them, and (iii) are textually similar.

Towards this, we model a graph with articles across bi-cliques as vertices and edges between pairs of articles being weighted by a score that is computed as follows:

$$\text{Weight}(E(A, A')) = \alpha \times \frac{|\text{BiClique}(A) \cap \text{BiClique}(A')|}{|\text{BiClique}(A) \cup \text{BiClique}(A')|}$$

$$\beta \times \frac{|\text{Users}(A) \cap \text{Users}(A')|}{|\text{Users}(A) \cup \text{Users}(A')|} + (1 - \alpha - \beta) \times \text{Sim}(A, A')$$

(8)
Across the three phases, GTUT uses various criteria and methods to progressively label all articles in $\mathcal{A}$ as shown in Figure 1. A tabular overview of the labelling progression and methods used appear in Table 1, and a procedural overview appears in Algorithm 1. As an unsupervised method that does not have the luxury of labelled information to characterize, we employ the heuristic of higher prevalence of synchronous sharing among fake news to identify a seed set of fake and legitimate articles in Phase 1. Phase 2 and Phase 3 employ heuristics on bi-clique, user and text similarity that are broadly applicable across fake and legitimate classes of articles to spread the labels across all articles.

**Note on Scalability:** While the bi-clique enumeration step, as may be obvious, would be the most computationally expensive step in GTUT, recent research in enumerating cliques has yielded massive scalability improvements. In particular, a recent method [8] reports clique enumeration methods that can complete in a matter of seconds over million-sized graphs. Our implementation, based on [44], yielded response times in the order of minutes over benchmark datasets we use in our empirical evaluation. Further, our method is not designed for usage in a real-time environment, and is thus unlike real-time user-query based retrieval systems for which response time is critical.
5 EXPERIMENTAL EVALUATION

We now describe the experimental evaluation of our method vis-a-vis baseline methods. We first start with detailing the datasets, experimental setup and the baselines used in the comparative analysis. This is followed by our empirical results over the datasets and a deeper analysis of our method over various parameter settings.

5.1 Datasets and Experimental Setup

5.1.1 Datasets: We use the code from the FakeNewsNet repository [32] in order to collect the two benchmark datasets, PolitiFact and GossipCop. In PolitiFact, a dataset collected from the web portal with the same name4, journalists and domain experts review political news and provide fact-checking evaluation results to identify news articles as fake or real. GossipCop5, on the other hand, is a website for factchecking entertainment stories collected from various media outlets. They provide a rating score, ranging from 0 to 10, to classify an article from fake to real. These scores have been discretized into binary fake/real labels, as outlined in [32]. While these datasets are datasets of news stories, the social context behind these stories are captured using the Twitter Advanced API, as outlined in the same paper. Specifically, tweets that share the news story are collected, along with the userids of users who authored such tweet and the time of posting the tweet. The statistics for the datasets are shown in Tables 2 and 3 respectively. Articles are labelled as either fake or legitimate/real; each post is labelled with the label of the article which it posts about. Given the length limitation of tweets, we did not come across posts that mention multiple articles in the same tweet. For purposes of collecting statistics that are shown in the tables, we consider each user who has tweeted at least one legitimate/real article as a user who has tweeted a real article and each user who has tweeted at least one fake article as being a fake (tweeting) user. Evidently, such tweets could be users who have tweeted both real and fake articles, making these user sets overlapping. The extent of the overlap is also recorded in the tables. As may be observed from the description and the statistics of the datasets, the datasets are from disparate domains and also have very different distributions across the real and fake classes. While non-fake tweets and users dominate the PolitiFact dataset, the vice versa is true of the GossipCop dataset. The empirical evaluation over such widely varying benchmark datasets, we believe, will inspire confidence in the generalizability of our empirical study.

5.1.2 Baselines: As outlined in Section 2, there has been very limited work in the area of unsupervised fake news detection. The recent unsupervised fake news detection technique from [41], called UFD, forms our primary baseline in the empirical evaluation. We also use an early and very popular (cited 600+ times) fake news detection method, TruthFinder [42], as another baseline method for our empirical study. Our third baseline is the Majority Voting (MV) approach outlined in [41].

5.1.3 Evaluation Measures: Our unsupervised fake news detection task involves assigning a T/F label to each of the articles in the dataset, by making use of user and temporal patterns of sharing them, as available from Twitter. As a natural way of measuring the accuracy of the labelling output from the techniques, we use Precision, Recall and F-Score for each of the two classes (i.e., \{T, F\}) as evaluation measures [12]. Consider a single class, say F; precision and recall measure the number of fake articles as a fraction of those labelled fake by the method being evaluated and the gold-standard respectively. F-Score is the harmonic mean of precision and recall, which achieves high scores when both are high. Given that our methods do not yield scores but crisp labellings, conventional curves such as precision-recall or ROC curves are not applicable for this scenario. Further to these, we also examine the various methods on the overall accuracy, which is the fraction of correctly labelled instances.

5.1.4 Experimental Setup: We use python implementations of GTUT and the baseline methods in our empirical study. We use the recommended hyper-parameter settings for the baseline methods from their respective papers. GTUT has three hyper-parameters, \(\alpha\) and \(\beta\) from Phase 2, and \(\gamma\) from Phase 3. We consistently use \(\alpha = 0.4\), \(\beta = 0.4\) and \(\gamma = 0.75\) across our experiments unless otherwise mentioned.

5.2 Comparative Analysis

The results of the comparative analysis pitching GTUT against the three baseline methods is illustrated across Table 4 (PolitiFact Dataset Results) and Table 5 (GossipCop Dataset Results). As may

<table>
<thead>
<tr>
<th>Type</th>
<th>Truthful/Real</th>
<th>Fake</th>
</tr>
</thead>
<tbody>
<tr>
<td>Articles</td>
<td>369</td>
<td>367</td>
</tr>
<tr>
<td>Tweets</td>
<td>49805</td>
<td>355290</td>
</tr>
<tr>
<td>Users</td>
<td>283400</td>
<td>85208</td>
</tr>
<tr>
<td>Users posting both truthful and fake articles: 16060</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 2: Statistics of the PolitiFact dataset.

<table>
<thead>
<tr>
<th>Type</th>
<th>Truthful/Real</th>
<th>Fake</th>
</tr>
</thead>
<tbody>
<tr>
<td>Articles</td>
<td>600</td>
<td>450</td>
</tr>
<tr>
<td>Tweets</td>
<td>41580</td>
<td>123875</td>
</tr>
<tr>
<td>Users</td>
<td>6013</td>
<td>53288</td>
</tr>
<tr>
<td>Users posting both truthful and fake articles: 2520</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 3: Statistics of the GossipCop dataset.
Table 4: PolitiFact dataset results. The best result for each evaluation measure (i.e., each column) is shown in bold.

<table>
<thead>
<tr>
<th>Detection Method</th>
<th>True Precision</th>
<th>True Recall</th>
<th>True F-Score</th>
<th>False Precision</th>
<th>False Recall</th>
<th>False F-Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>UFD</td>
<td>0.72</td>
<td>0.83</td>
<td>0.77</td>
<td>0.62</td>
<td>0.46</td>
<td>0.53</td>
</tr>
<tr>
<td>TruthFinder</td>
<td>0.69</td>
<td>0.62</td>
<td>0.65</td>
<td>0.45</td>
<td>0.53</td>
<td>0.49</td>
</tr>
<tr>
<td>MV</td>
<td>0.74</td>
<td>0.81</td>
<td>0.77</td>
<td>0.62</td>
<td>0.52</td>
<td>0.57</td>
</tr>
<tr>
<td>GTUT</td>
<td><strong>0.77</strong></td>
<td><strong>0.83</strong></td>
<td><strong>0.80</strong></td>
<td><strong>0.83</strong></td>
<td><strong>0.76</strong></td>
<td><strong>0.79</strong></td>
</tr>
</tbody>
</table>

Table 5: GossipCop dataset results. The best result for each evaluation measure (i.e., each column) is shown in bold.

<table>
<thead>
<tr>
<th>Detection Method</th>
<th>True Precision</th>
<th>True Recall</th>
<th>True F-Score</th>
<th>False Precision</th>
<th>False Recall</th>
<th>False F-Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>UFD</td>
<td>0.58</td>
<td>0.85</td>
<td>0.69</td>
<td>0.81</td>
<td>0.51</td>
<td>0.62</td>
</tr>
<tr>
<td>TruthFinder</td>
<td><strong>0.75</strong></td>
<td>0.65</td>
<td>0.69</td>
<td>0.60</td>
<td><strong>0.71</strong></td>
<td>0.65</td>
</tr>
<tr>
<td>MV</td>
<td>0.58</td>
<td>0.75</td>
<td>0.65</td>
<td>0.45</td>
<td>0.27</td>
<td>0.34</td>
</tr>
<tr>
<td>GTUT</td>
<td>0.72</td>
<td><strong>0.93</strong></td>
<td><strong>0.81</strong></td>
<td><strong>0.87</strong></td>
<td>0.56</td>
<td><strong>0.68</strong></td>
</tr>
</tbody>
</table>

Table 6: Accuracy analysis.

<table>
<thead>
<tr>
<th>Method</th>
<th>PolitiFact</th>
<th>GossipCop</th>
</tr>
</thead>
<tbody>
<tr>
<td>UFD</td>
<td>0.70</td>
<td>0.66</td>
</tr>
<tr>
<td>TruthFinder</td>
<td>0.59</td>
<td>0.67</td>
</tr>
<tr>
<td>MV</td>
<td>0.65</td>
<td>0.55</td>
</tr>
<tr>
<td>GTUT</td>
<td><strong>0.80</strong></td>
<td><strong>0.77</strong></td>
</tr>
</tbody>
</table>

Table 7: GTUT Phase 1 Bi-clique selection.

<table>
<thead>
<tr>
<th>#minart</th>
<th>PolitiFact Dataset Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>48%</td>
</tr>
<tr>
<td>4</td>
<td>40%</td>
</tr>
<tr>
<td>5</td>
<td>31%</td>
</tr>
<tr>
<td>6</td>
<td>23%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#minart</th>
<th>GossipCop Dataset Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>45%</td>
</tr>
<tr>
<td>8</td>
<td>43%</td>
</tr>
<tr>
<td>9</td>
<td>41%</td>
</tr>
<tr>
<td>10</td>
<td>39%</td>
</tr>
<tr>
<td>11</td>
<td>37%</td>
</tr>
</tbody>
</table>

5.3.1 Article Cardinality Thresholds in Phase 1. As mentioned in Section 4.1, we use a minimum cardinality threshold on both the number of users and the number of articles within the bi-clique identification step, to avoid identifying meaningless small patterns as bi-cliques. Our strategy has been to impose a threshold of a minimum of 5 users, and a threshold on the number of articles in a way that the bi-cliques together cover around 40% of the dataset. The threshold as a function of the covered dataset proportion offers applicability across datasets of widely varying sizes. This strategy yielded a minimum article threshold of 4 and 9 for the PolitiFact and GossipCop datasets respectively. We analyze the covered dataset...
proportion around these chosen settings of minimum number of articles, or #minart for short, in Table 7. As may be seen therein, the dataset coverage could widely vary, making exact threshold attainment not always feasible. However, we observed that GTUT is not affected much by choosing dataset coverage thresholds anywhere in the 30% – 50% range.

<table>
<thead>
<tr>
<th>α</th>
<th>β</th>
<th>1 − α − β</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.45</td>
<td>0.35</td>
<td>0.20</td>
<td>0.82</td>
</tr>
<tr>
<td>0.35</td>
<td>0.45</td>
<td>0.20</td>
<td>0.82</td>
</tr>
<tr>
<td>0.30</td>
<td>0.55</td>
<td>0.15</td>
<td>0.83</td>
</tr>
<tr>
<td>0.25</td>
<td>0.65</td>
<td>0.10</td>
<td>0.81</td>
</tr>
</tbody>
</table>

Table 8: GTUT Study over phase 2 parameters.

5.3.3 Hyper-parameters from Phase 3. Phase 3, while being similar in construction to Phase 2, does not have the bi-clique similarity term, and thus, has one fewer hyper-parameter. γ determines the weight associated with the user similarity term, whereas 1 − γ is the weight for the textual similarity term. As seen in Section 5.3.2, the trends on γ also shows high stability over small variations.

<table>
<thead>
<tr>
<th>γ</th>
<th>1 − γ</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.80</td>
<td>0.20</td>
<td>0.77</td>
</tr>
<tr>
<td>0.75</td>
<td>0.25</td>
<td>0.80</td>
</tr>
<tr>
<td>0.70</td>
<td>0.30</td>
<td>0.78</td>
</tr>
</tbody>
</table>

Table 9: GTUT Study over phase 3 parameters.

6 CONCLUSIONS AND FUTURE WORK

We considered the task of unsupervised detection of fake news articles by making use of social media traces. Unsupervised fake news identification is significantly more challenging than its supervised counterpart due to the absence of labelled data to aid modelling the distinction between fake and legitimate news. We develop a three-phase graph-based approach, code-named GTUT, that uses a graph-based approach for the task. GTUT uses a three phase approach, wherein the first phase uses high-level assumptions of inter-user behavioral dynamics to identify a seed set of fake and real news articles. This is enabled through identification of bi-cliques and scoring them on textual and temporal coherence. The second phase expands the labelling from the seed set to all articles involved in bi-cliques making use of three kinds of similarity information, viz., bi-clique similarity, user similarity and textual similarity. This phase makes use of graph modelling followed by graph embeddings and label spreading. The third phase targets labelling the articles not involved in bi-cliques through graph modelling and label spreading to ensure that all articles in the dataset are assigned as either fake or real. Through an extensive set of experiments over popular real-world datasets used in the fake news detection task, we establish that GTUT significantly outperforms state-of-the-art and popular baselines for the task. In particular, GTUT is seen to achieve gains of over 10 percentage points on accuracy, achieving accuracies close to 80% for unsupervised fake news detection. We also performed an extensive study on the sensitivity of GTUT to its hyperparameters, and illustrated that GTUT is quite stable and insensitive to minor variations in the hyperparameters. Our extensive empirical analysis establishes the effectiveness of GTUT for unsupervised fake news detection.

Future Work. Our task in GTUT was to make use of social media traces, to ensure its applicability for cases where social media user connectivity information is not necessarily available. That said, social media connectivity would likely provide some useful information for the task. We are exploring the possibilities of characterizing network connectivity patterns in fake news propagation through high-level heuristics to inform the fake/real seeding phase in GTUT. Secondly, social media sharing of a news article often offers very vivid digital footprints. For example, a tweet may be re-tweeted, liked or shared, whereas a Facebook post can be ‘reacted to’ using emotionally rich responses. Given a large number of studies that relate fake news to emotions, we are considering the usage of emotion information within such social media traces in order to improve unsupervised fake news detection. Thirdly, the real-fake spectrum in news is often very broad and binary labellings, as used in fake news detection techniques including GTUT, may be criticized as an oversimplification. We are considering ways in which this binary labelling can be relaxed in order to offer more fine-grained labellings, staying within the graph-based framework. Other directions include generating interpretable results [3] and enriching semantic query expansion (e.g., [19]) with veracity orientation.

Acknowledgements

This work was supported by the MHRD (India) under the SPARC programme project #P620. The authors would like to thank Kaiqiang Yu (PhD candidate at NTU) for enriching discussions.
REFERENCES


