FAKE NEWS DETECTION ON SOCIAL MEDIA USING GEOMETRIC DEEP LEARNING

Federico Monti¹,² Fabrizio Frasca¹,² Davide Eynard¹,² Damon Mannion¹,²
Michael M. Bronstein¹,²,³

¹Fabula AI (UK), ²USI Lugano (Switzerland), ³Imperial College of London (UK)

ABSTRACT

Social media are nowadays one of the main news sources for millions of people around the globe due to their low cost, easy access, and rapid dissemination. This however comes at the cost of dubious trustworthiness and significant risk of exposure to ‘fake news’. Recent studies have empirically shown that fake and real news spread differently on social media, forming propagation patterns that could be harnessed for automatic fake news detection. In this paper, we show a novel automatic fake news detection model based on geometric deep learning. The underlying core algorithms are a generalization of classical convolutional neural networks to graphs, allowing the fusion of heterogeneous data such as content, user profile and activity, social graph, and news propagation.

1 INTRODUCTION

In the past decade, social media have become one of the main sources of information for people around the world. Yet, using social media for news consumption is a double-edged sword. On the one hand, it offers low cost, easy access, and rapid dissemination. On the other hand, it comes with the danger of exposure to ‘fake news’ containing poorly checked or even intentionally false information. Unfortunately, automatically detecting fake news poses challenges that defy existing content-based analysis approaches. One of the main reasons is that often the interpretation of the news is highly nuanced and requires the knowledge of political or social context, or “common sense”, which even the currently most advanced natural language processing algorithms are still missing. Furthermore, fake news is often intentionally written by bad actors to appear as real news but containing false or manipulative information in ways that are hard even for trained human experts to detect.

Prior works. Existing approaches for fake news detection can be divided into three main categories, based on content, social context, and propagation (Shu et al. (2017); Zhou & Zafarani (2018)). Content-based approaches, which are used in the majority of works on fake news detection, rely on linguistic (lexical and syntactical) features that can capture deceptive cues or writing styles (Afroz et al. (2012); Rubin et al. (2016); Rashkin et al. (2017); Potthast et al. (2017); Pérez-Rosas et al. (2017)). The main drawback of content-based approaches is that they can be defied by sufficiently sophisticated fake news that does not immediately appear as fake. Furthermore, most linguistic features are language-dependent, limiting the generality of these approaches. Social context approaches rely on features such as user demographics (Shu et al. (2018); Long et al. (2017)), social network structure (Shu et al. (2019b,a)) and user reactions (Ruchansky et al. (2017); Tacchini et al. (2017)). Propagation-based approaches are perhaps the most intriguing and promising research direction based on studying the news proliferation process over time. It has been argued that the fake news dissemination process is akin to infectious disease spread (Kucharski (2016)) and can be understood with network epidemics models. There is substantial empirical evidence that fake news propagate differently from true news (Vosoughi et al. (2018)) forming spreading patterns that could potentially be exploited for automatic fake news detection. By virtue of being content-agnostic, propagation-based features are likely generalized across different languages, locales, and geographies, as opposed to content-based features that must be developed separately for each language.
Main contribution. In this paper, we propose learning fake news specific propagation patterns by exploiting geometric deep learning, a novel class of deep learning methods designed to work on graph-structured data (Bronstein et al. (2017)). The model proposed in this paper is trained in a supervised manner on a large set of annotated fake and true stories spread on Twitter in the period 2013-2018. Our solution achieves very high accuracy (nearly 93% ROC AUC), requires very short news spread times (just a few hours of propagation), and performs well when the model is trained on data distant in time from the testing data.

2 Our model

Geometric deep learning. Most of popular deep neural models, such as convolutional neural networks (CNNs) (LeCun et al. (1998)), are based on classical signal processing theory, with an underlying assumption of grid-structured (Euclidean) data. In recent years, there has been growing interest in generalizing deep learning techniques to non-Euclidean (graph- and manifold-structured) data. The modern interest in deep learning on graphs can be attributed to the spectral CNN model of Bruna et al. (2014). Broadly speaking, graph CNNs replace the classical convolution operation on grids with a local permutation-invariant aggregation on the neighborhood of a vertex in a graph. In spectral graph CNNs (Bruna et al. (2014)), this operation is performed in the spectral domain, by utilizing the analogy between the graph Laplacian eigenvectors and the classical Fourier transform; the filters are represented as learnable spectral coefficients. Follow-up works showed that the explicit eigendecomposition of the Laplacian can be avoided by employing functions expressible in terms of simple matrix-vector operations, such as polynomials (Defferrard et al. (2016); Kipf & Welling (2017)) or rational functions (Levie et al. (2017)). The Laplacian operator is only one example of local permutation-invariant aggregation operation amounting to weighted averaging. More general operators have been proposed using edge convolutions (Wang et al. (2018)), neural message passing (Gilmer et al. (2017)), local charting (Monti et al. (2017)), and graph attention (Velickovic et al. (2018)).

Architecture and training settings. We used a four-layer Graph CNN with two convolutional layers (64-dimensional output features map in each) and two fully connected layers (producing 32- and 2-dimensional output features, respectively) for predicting the veracity of the considered piece of news. One head of graph attention (Velickovic et al. (2018)) was used in every convolutional layer to implement the filters together with mean-pooling for dimensionality reduction. We used Scaled Exponential Linear Unit (SELU, Klambauer et al. (2017)) as non-linearity throughout the entire network. Hinge loss was employed to train the neural network (we preferred hinge loss to the more commonly used mean cross entropy as it outperformed the latter in early experiments). No regularization was used with our model.

3 Results

We considered two different settings of fake news detection: URL-wise and cascade-wise, using the same architecture for both settings. In the first setting, we attempted to predict the true/fake label of a URL containing a news story from all the tweets it generated. In the latter setting, we assumed to be given only one cascade (i.e. one tweet and all its retweets) arising from a URL and attempted to predict the label associated with that URL. Our assumption is that all the cascades associated with a URL inherit the label of the latter. For each URL/cascade, we provide as input to our model an induced subgraph from Twitter where nodes are tweets/retweets associated to the considered URL/cascade and edges are connections among users producing such (re)tweets. Features encoding information about news spreading, user profile, user activity and tweet content have been used to characterize nodes and edges in the considered subgraphs (Supplementary material, Section 5.2). All our experiments have been realized on a dataset of 1,129 URLs that spread on Twitter on 158,951 cascades, for a total of 4,416,284 tweets. Such dataset has been gathered and annotated as part of this study (Supplementary material, Section 5.1).

Hereinafter, results are discussed for the first scenario (i.e. URL-wise classification); the second one (cascade-wise classification) is addressed in supplementary material (Section 5.3).
Figure 1: (a) Performance of URL-wise fake news detection using 24hr-long diffusion time. Shown are ROC curves averaged on five folds (the shaded areas represent the standard deviations). ROC AUC is 92.70 ± 1.80%.

(b) Ablation study result on URL-wise fake news detection, using backward feature selection. Shown is performance (ROC AUC) for our model trained on subsets of features, grouped into four categories: user profile (UP), network and spreading (N/S), content (C), and user activity (UA). Groups are sorted for importance from left (most important) to right (least important).

Model performance. For URL-wise classification, we used five randomized training/test/validation splits. On average, the training, test, and validation sets contained 677, 226, and 226 URLs, respectively, with 83.26% true and 16.74% false labels (±0.06% and 0.15% for training and validation/test set respectively). Only tweets/retweets produced in the first 24hr of life of each URL have been considered as input to our model. Our neural network was trained for $25 \times 10^3$ iterations in the present setting, using AMSGrad (Reddi et al. (2018)) with learning rate of $5 \times 10^{-4}$ and mini-batches of size one. Figure 1a depicts the performance of URL-wise fake news classification represented as a tradeoff (ROC curve) between false positive rate (fraction of true news wrongly classified as fake) and true positive rate (fraction of fake news correctly classified as fake). We use area under the ROC curve (ROC AUC) as an aggregate measure of accuracy. On the above splits, our method achieved a mean ROC AUC of 92.70 ± 1.80%.

Ablation study. To further highlight the importance of the different categories of features provided as input to the model, we conducted an ablation study by means of backward-feature selection. We considered four groups of features (Supplementary material, Section 5.1): user profile, user activity, network and spreading, and content. The results of ablation experiment are shown in Figure 1b. User profile and network/spreading appear as the two most important feature groups, allowing to achieve satisfactory classification results (near 90% ROC AUC) with the proposed model.

News spreading over time. One of the key differentiators of propagation-based methods from their content-based counterparts, namely relying on the news spreading features, potentially raises the following question: how long do news have to spread before we can classify them reliably? We conducted a series of experiments to study the extent to which this is the case with our approach. For this purpose, we truncated the spreading at time $t$ wrt the first tweet, with $t$ varying from 0 (effectively considering only the initial tweet mentioning the considered URL) to 24 hours with one hour increments. The model was trained separately for each value of $t$. Five-fold cross validation was used to reduce the bias of the estimations while containing the overall computational cost.

Figure 2 depicts the performance of the model (mean ROC AUC) as function of diffusion time. As expected, performance increases with the cascade duration, saturating roughly after 15 hours. We note that, remarkably, just a few (~2) hours of news spread are sufficient to achieve above 90% mean ROC AUC. Furthermore, we observe a significant jump in performance from the 0 hr setting (effectively using only user profile, user activity, and content features of the first tweet) to ≥1 hr settings (considering additionally the news propagation), which we interpret as another indication of the importance of propagation-related features.
Model aging. We live in a dynamic world with constantly evolving political context. Since the social network, user preferences and activity, news topics and potentially also spreading patterns evolve in time, it is important to understand to what extent a model trained in the past can generalize to such new circumstances. In the final set of experiments, we study how the model performance ages with time. These experiments aim to emulate a real-world scenario in which a model trained on historical data is applied to new tweets in real time.

For the present URL-wise setting, we split our dataset into training/validation (80% of URLs) and test (20% of URLs) sets; the training/validation and test sets were disjoint and subsequent in time. We assessed the results of our model on subsets of the test set, designed as partially overlapping (mean intersection over union equal to $0.56 \pm 0.15$) time windows. Partial overlap allowed us to work on larger subsets while preserving the ratio of positives vs negatives, providing at the same time smoother results as with moving average. This way, each window contained at least 24% of the test set (average number of URLs in a window was $73 \pm 33.34$) and the average dates of two consecutive windows were at least 14 days apart, progressively increasing.

Figure 2 captures the variation in performance due to aging of the training set. Our model exhibits a slight deterioration in performance only after 180 days. We attribute this deterioration to the change in the spreading patterns and the user activity profiles.
4 CONCLUSIONS

In this paper, we presented a geometric deep learning approach for fake news detection on Twitter social network. Our solution achieves very high accuracy and robust behavior in several challenging settings involving large-scale real data, pointing to the great potential of geometric deep learning methods for fake news detection. In future works we intend to explore additional applications of our model in social network data analysis, such as news topic classification and virality prediction.

ACKNOWLEDGMENTS

We gratefully acknowledge the generous support by ERC Consolidator Grant No. 724228 (LEMAN), ERC Proof of Concept grant No. 812672 (GoodNews), multiple Google Research Faculty awards and Nvidia equipment grants, Amazon AWS Machine Learning Research grant, Dalle Molle Foundation prize, and Facebook Computational Social Science Methodology award. MB is also partially supported by the Royal Society Wolfson Research Merit award and Rudolf Diesel industrial fellowship at TU Munich. FF’s PhD scholarship is supported by the SNF Grant No. 200021E/176315.
5 SUPPLEMENTARY MATERIAL

5.1 DATASET

One of the key challenges in machine-learning based approaches in general, and in automatic fake news detection in particular, is collecting a sufficiently large, rich, and reliably labelled dataset on which the algorithms can be trained and tested. Furthermore, the notion of ‘fake news’ itself is rather vague and nuanced. To start with, there is no consensus as to what would be considered ‘news’, let alone the label ‘true’ or ‘false’. A large number of studies exploit the notion of reliable or unreliable sources as a proxy for true or false stories. While allowing to gather large datasets, such approaches have been criticized as too crude (Vosoughi et al. (2018)). In our study, we opted for a data collection process in which each ‘story’ has an underlying article published on the web, and each such story is verified individually. In our classification of true or false statements we rely on professional non-profit journalist fact-checking organizations such as Snopes, PolitiFact and Buzzfeed. We note that our use of the term fake news, though disliked in the social science research community for its abuse in the political discourse, refers to both misinformation and disinformation, i.e. unintentional as well as deliberate spread of misleading or wrong narrative or facts.

Data collection protocol. Our data collection process was inspired by and largely followed the pioneering work of Vosoughi et al. (2018). We used a collection of news verified by fact-checking organizations with established reputation in debunking rumors; each source fact-checking organization provides an archive of news with an associated short claim (e.g. ‘Actress Allison Mack confessed that she sold children to the Rothschilds and Clintons’) and a label determining its veracity (‘false’ in the above example).

First, we gathered the overall list of fact-checking articles from such archives and, for simplicity, discarded claims with ambiguous labels, such as ‘mixed’ or ‘partially true/false’. Second, for each of the filtered articles we identified potentially related URLs referenced by the fact-checkers, filtering out all those not mentioned at least once on Twitter. Third, trained human annotators were employed to ascertain whether the web pages associated with the collected URLs were matching or denying the claim, or were simply unrelated to that claim. This provided a simple method to propagate truth-labels from fact-checking verdicts to URLs: if a URL matches a claim, then it directly inherits the verdict; if it denies a claim, it inherits the opposite of the verdict (e.g. URLs matching a true claim are labeled as true, URLs denying a true claim are labeled as false). URLs gathered from different sources, with same veracity and date of first-appearance on Twitter were additionally inspected to ensure they referred to different articles.

The last part of the data collection process consisted of the retrieval of Twitter data related to the propagation of news associated with a particular URL. Following the nomenclature of Vosoughi et al. (2018), we term as cascade the news diffusion tree produced by a source tweet referencing a URL and all of its retweets. For each URL, we searched for all the related cascades and enriched their Twitter-based characterization (i.e. users and tweet data) by drawing edges among users according to Twitter’s social network (see example in Figure 4).

With regard to this last step of data collection, our approach is significantly different from the protocol of Vosoughi et al. (2018), where tweets linking to a fact-checking website were collected, thus essentially retrieving only cascades in which someone has posted a ‘proof-link’ with the veracity of the news. Though significantly more laborious, we believe that our data collection protocol produces a much cleaner dataset.

Statistics. Figures 5–6 depict the statistics of our dataset. Overall, our collection consisted of 1,084 labeled claims, spread on Twitter in 158,951 cascades covering the period from May 2013 till January 2018. The total number of unique users involved in the spreading was 202,375 and their respective social graph comprised 2,443,996 edges. As we gathered 1,129 URLs, the average number of article URLs per claim is around 1.04; as such, a URL can be considered as a good proxy for a claim in our dataset. We also note that, similarly to Vosoughi et al. (2018), a large proportion of
Published as a conference paper at ICLR 2019

Figure 4: Example of a single news story spreading on a subset of the Twitter social network. Social connections between users are visualized as light-blue edges. A news URL is tweeted by multiple users (cascade roots denoted in red), each producing a cascade propagating over a subset of the social graph (red edges). Circle size represents the number of followers. Note that some cascades are small, containing only the root (the tweeting user) or just a few retweets.

Figure 5: Distribution of cascade sizes (number of tweets per cascade) in our dataset.

cascades were of small size (the average number of tweets and users in a cascade is 2.79, see also Figure 5 depicting the distribution of cascade sizes), which required to use a threshold on a minimum cascade size for classifying these independently in some experiments (Section 5.3).

Features. We extracted the following features describing news, users, and their activity, grouped into four categories: User profile (geolocalization and profile settings, language, word embedding of user profile self-description, date of account creation, and whether it has been verified), User activity (number of favorites, lists, and statuses), Network and spreading (social connections between the users, number of followers and friends, cascade spreading tree, retweet timestamps and source device, number of replies, quotes, favorites and retweets for the source tweet), and Content (word embedding of the tweet textual content and included hashtags).

Credibility and polarization. The social network collected in our study manifests noticeable polarization depicted in Figure 7. Each user in this plot is assigned a credibility score in the range $[-1, +1]$ computed as the difference between the proportion of (re)tweeted true and fake
Figure 6: Distribution of cascades over the 930 URLs available in our dataset with at least six tweets per cascade, sorted by the number of cascades in descending order. The first 15 URLs (~1.5% of the entire dataset) correspond to 20% of all cascades.

Figure 7: Subset of the Twitter network used in our study with estimated user credibility. Vertices represent users, gray edges the social connections. Vertex color and size encode the user credibility (blue = reliable, red = unreliable) and number of followers of each user, respectively. Numbers 1 to 9 represent the nine users with most followers.

news (negative values representing fake are depicted in red; more credible users are represented in blue). The node positions of the graph are determined by topological embedding computed via the Fruchterman-Reingold force-directed algorithm (Fruchterman & Reingold (1991)), grouping together nodes of the graph that are more strongly connected and mapping apart nodes that have weak connections. We observe that credible (blue) and non-credible (red) users tend to form two distinct communities, suggesting these two categories of tweeters prefer to have mostly homophilic interactions. While a deeper study of this phenomenon is beyond the scope of this paper, we note that similar polarization has been observed before in social networks, e.g. in the context of political discourse (Conover et al. (2011)) and might be related to ‘echo chamber’ theories that attempt to explain the reasons for the difference in fake and true news propagation patterns.
Ablation study. Following what already presented in the paper for the URL-wise setting, we with 81.73% true and 18.27% false labels (see Figure 5). Since our approach relies on the spreading of news across the Twitter social network, (i.e. all cascades originated by URL \( u \) retweets belonging to the same cascade and authored by users \( \{a_u^0, \ldots, a_u^{n-1}\} \)).

To identify the minimum useful cascade size, we investigated the performance of our model in the cascade-wise setting using cascades of various minimum sizes (Figure 9). As expected, such examples may be hard to classify, as too small cascades may manifest no clear diffusion pattern.

Our neural network was trained for \( 50 \times 10^3 \) iterations, using AMSGrad (Reddi et al. (2018)) with learning rate of \( 5 \times 10^{-4} \) and mini-batches of size one.

Figure 8 depicts for completeness both the ROC curves of URL- (blue) and cascade-wise (red) fake news classification. On the mentioned splits, our method achieves a mean ROC AUC of 88.30±2.74% in the cascade-wise setting.

Influence of minimum cascade size. One of the characteristics of our dataset (as well as the dataset in the study of Vosoughi et al. (2018)) is the abundance of small cascades containing just a few users (see Figure 5). Since our approach relies on the spreading of news across the Twitter social network, such examples may be hard to classify, as too small cascades may manifest no clear diffusion pattern. To identify the minimum useful cascade size, we investigated the performance of our model in the cascade-wise classification setting using cascades of various minimum sizes (Figure 9). As expected, the model performance increases with larger cascades, reaching saturation for cascades of at least 6 tweets (leaving a total of 5,976 samples). This experiment motivates our choice of using 6 tweets as the minimum cascade size in cascade-wise experiments in our study.

Ablation study. Following what already presented in the paper for the URL-wise setting, we conducted an ablation study for identifying the most relevant categories of features for cascade-wise classification. The results of such ablation experiment are shown in Figure 10. User-profile and network/spreading appear again as the two most important feature groups for the proposed model.

4For tweet content and user description embeddings we averaged together the embeddings of the constituent words (GloVe (Pennington et al. (2014)) 200-dimensional vectors pre-trained on Twitter).
Figure 8: Performance of URL-wise (blue) and cascade-wise (red) fake news detection using 24hr-long diffusion time. Shown are ROC curves averaged on five folds (the shaded areas represent the standard deviations). ROC AUC is $92.70 \pm 1.80\%$ for URL-wise classification and $88.30 \pm 2.74\%$ for cascade-wise classification, respectively. Only cascades with at least 6 tweets were considered for cascade-wise classification.

Figure 9: Performance of cascade-wise fake news detection (mean ROC AUC, averaged on five folds) using minimum cascade size threshold. Best performance is obtained by filtering out cascades smaller than 6 tweets.

Interestingly, in the cascade-wise setting, while all features were positively contributing to the final predictions at URL-level, removing tweet content from the provided input improves performance by 4%. This seemingly contradictory result can be explained by looking at the distribution of cascades over all the available URLs (Figure 6): 20% of cascades are associated to the top 15 largest URLs in our dataset ($\sim 1.5\%$ out of a total of 930). Since tweets citing the same URL typically present similar content, it is easy for the model to overfit on this particular feature. Proper regularization (e.g. dropout or weight decay) should thus be introduced to avoid overfitting and improve performance at test time. We leave this further study for future research. For simplicity, by leveraging the capabilities of our model to classify fake news in a content-free scenario, we decided to completely ignore content-based descriptors (tweet word embeddings) for cascade-wise classification and let the model exploit only user- and propagation-related features.

News spreading over time. As for URL-wise classification, we studied for how long a provided cascade has to spread before being successfully classified. For this purpose, we truncated the cascades after time $t$ starting from the first tweet, with $t$ varying from 0 (effectively considering only the initial tweet, i.e. the ‘root’ of each cascade) to 24 hours (the full cascade duration) with one hour increments. The model was trained separately for each value of $t$. Figure 11 depicts the performance of the model (mean ROC AUC) as function of the cascade duration. Again, performance increases with the cascade duration, saturating roughly after 7 hours. This different behavior wrt URL-wise
classification is mainly due to the simpler topological patterns and shorter life of individual cascades. Seven hours of spreading encompass on average around $91\%$ of the cascade size; for the URL-wise setting, the corresponding value is $68\%$. A similar level of coverage, $86\%$, is achieved after 15 hours of spreading in the URL-wise setting.

**Model aging.** We finally present the performance of our model wrt aging of the training set. The split into training/validation and test sets and the generation of the time windows was done similarly to the URL-wise experiment (first $80\%$ of cascades for training and last $20\%$ for testing). Each time window in the test set has an average size of $314 \pm 148$ cascades, and two consecutive windows had a mean overlap with intersection over union equal to $0.68 \pm 0.21$. Figure 12 summarizes the performance of our model. In this case, our NN shows a more robust behavior compared to the URL-wise setting, losing only $4\%$ after 260 days.

This different behavior is likely due to the higher variability that characterizes cascades as opposed to URLs. As individual cascades are represented by smaller and simpler graphs, the likelihood of identifying recurrent rich structures between different training samples is lower compared to the URL-wise setting and, also, cascades may more easily involve users coming from different parts of the Twitter social network. In the cascade-wise setting, our propagation-based model is thus forced to learn simpler features that on the one hand are less discriminative (hence the lower overall
Figure 12: Effects of training set aging on the performance of cascade-wise fake news detection. Shown is the test performance obtained by our model with 24 hr diffusion (solid blue), test performance obtained with same model just using the first tweet of each cascade (0hrs diffusion, dashed orange), and test performance obtained training on our original uniformly sampled five folds (veracity predictions are computed for each cascade when this appears as a test sample in our 24hrs five fold cross-validation, green).

performance), and on the other hand appear to be more robust to aging. We leave a deeper analysis of this behavior to future research, which might provide additional ways improving the fake news classification performance.

REFERENCES


