

Exploring Fake News Detection Techniques via Graph Neural Networks: An Overview

Vandana Rai¹, Dr. Sakshi Rai²

Research Scholar, Department of Computer Science & Engineering, LNCT University, Bhopal¹ Professor, Department of Computer Science & Engineering, LNCT University, Bhopal² *Email: vandana.rai2113@gmail.com¹*, Sakshirai.sr29@gmail.com²

Abstract: In today's world, there's a ton of information everywhere, but alongside it, there's also a big problem: fake news. This fake stuff makes it hard to trust what we read or hear. It's a big deal for all of us - individuals, groups, and whole societies. The old ways of finding these fakes aren't keeping up because fake news keeps changing. The solution of this problem is Graph neural network (GNN). The paper firstly introduces the background and overview related to fake news, fake news detection, and GNNs. Second, we provide a GNN taxonomy-based fake news detection taxonomy and review and highlight models in categories. Subsequently, it compares critical ideas, advantages, and disadvantages of the methods in categories. This paper also dives into how GNNs can help spot fake news by looking at how all the different parts of information are connected. It's like solving a puzzle to figure out how fake news spreads through these connections.

Keywords: Fake News, Graph Neural Networks, Survey, Misinformation, Machine Learning, Social Networks, Detection

1. Introduction

Social networks have become the main platform for spreading information. However, due to the growing number of users, social media platforms tend to be highly vulnerable to the spread of misinformation, making detecting fake news a challenging task [1]. Data validity is not just about data quality or its perceived accuracy. The legitimacy of the data stems from the belief that we collectively believe that the data is legitimate, legitimate, and worthwhile [2]. It is an important part of integrity. The fight against falsehoods eliminates the integrity of social networking information and data usage in the application layer. Exposure to false content means damage to processing and network resources [3]. In addition, it poses a significant threat to the reliability of the information and the reliability of the service provided. Therefore, sharing false information affects the Quality of Trust (QoT) used in news distribution, based on how much the user trusts the content of a particular source [4]. False stories are now one of the biggest threats to the very essence of truth, with the potential for the collapse of democracy, journalism, justice, and even the economy. In this context, there is a growing collective effort of the academic community to develop methods that can analyze, identify and intervene in the processing of this misleading content [5]. Scientific

evidence has already shown that humans are in a position to distinguish truth from falsehood [6].

Concept of News

News is understood as meta-information and can include the following [7]:

- Source- Publishers of news, such as authors, websites, and social networks.
- Headline- Description of the main topic of the news with a short text to attract readers' attention.
- Body content- Detailed description of the news, including highlights and publisher characteristics.
- Image/Video- Part of the body content that provides a visual illustration to simplify the news content..
- Links- Links to other news sources.

Based on the characteristics of fake news, we provide a new definition of fake news as follows. "Fake news" is news containing non factual statements with malicious accounts that can cause the echo chamber effect, with the intention to mislead the public. Various concepts regarding fake news exist. Using the characteristics of fake news, Table 1 redefines these concepts to distinguish them as follows.



Table 1: Types of News			
Type of News	Description		
False news	It is news containing nonfactual statements from malicious accounts that can cause the echo chamber effect with undefined intentions.		
Disinformatio n	It is news or non-news containing non- factual statements from malicious accounts that can cause the echo chamber effect, with the intention to mislead the public.		
Cherry- picking	It is news or non-news containing common factual statements from malicious accounts and can cause the echo chamber effect, with the intention to mislead the public.		
Rumor	It is news or non-news containing factual or non- factual statements from malicious accounts and can cause the echo chamber effect with undefined intentions.		
Fake information	It is news or non-news of nonfactual statements from malicious accounts that can cause the echo chamber effect, with the intention to mislead the public.		
Manipulation	It is news on markets containing nonfactual statements from malicious accounts that can cause the echo chamber effect, with the intention to mislead the public.		
Deceptive news	It is news containing nonfactual statements from malicious accounts that can cause the echo chamber effect, with the intention to mislead the public.		
Satire news	It is news containing factual or nonfactual statements from malicious accounts that can cause the echo chamber effect, with the intention to entertain the public.		
Misinformati on	It is news or non-news containing non- factual statements from malicious accounts that can cause the echo chamber effect with undefined intentions.		
Clickbait	It is news or non-news containing factual or nonfactual statements from malicious accounts that can cause the echo chamber effect, with the intention to mislead the public.		
Fake facts	They are undefined information (news or non- news) comprising nonfactual statements from malicious ac- counts that can cause the echo chamber effect, with the intention to mislead the public.		
Propaganda	It is biased information (news or non-news) comprising undefined statements (factual or nonfactual) regarding mostly political events from malicious accounts and that can cause the echo chamber effect, with the intention to mislead the public.		
Sloppy journalism	It is unreliable and unverified information (news or non-news) comprising undefined statements shared by journalists that can cause the echo chamber effect, with the intention to mislead the public.		

Hence, the impact of fake news has been developing, from time to time extending to the offline international and threatening public safety.

Echo Chamber Effect

The echo chamber effect refers to the situation where individuals are exposed primarily to information or opinions that reinforce their existing beliefs or viewpoints, creating a kind of "reinforcement loop." In this scenario, people tend to surround themselves with like-minded individuals or sources that share similar perspectives, leading to a limited exposure to diverse or opposing

viewpoints [8]. In the context of fake news and misinformation, the echo chamber effect plays a significant role. When people only engage with information that aligns with their beliefs, they might not encounter contrasting or fact-checked information. This reinforces their existing beliefs, making them more susceptible to believing and spreading misinformation that On social media platforms and online communities, algorithms often personalize content based on a user's previous behavior and preferences. This customization can inadvertently create echo chambers by presenting information that aligns with the user's existing views, further narrowing their exposure to diverse opinions. The echo chamber effect contributes to the rapid spread and persistence of fake news. It intensifies confirmation bias, making individuals more likely to accept, believe, and share information that confirms their existing beliefs without critically evaluating its authenticity or accuracy. Addressing the echo chamber effect involves promoting media literacy, encouraging exposure to diverse perspectives, and fostering critical thinking skills. By encouraging individuals to seek out and consider information from various sources, it becomes possible to mitigate the effects of echo chambers and reduce the influence of misinformation.

2. Fake News Detection Methods

The wide usage of social media platforms worldwide has provided a fertile ground for the widespread dissemination of online fake news in an unprecedented way [8]. The social network is flooded with massive, diverse, and heterogeneous information (both real and fake), and spreads rapidly on these platforms causing severe impact to the whole society. Therefore, many researchers and technical giants are working together to detect fake news on online media [9]. The traditional automatic rumour detection methods were based on hand crafted feature but with the advent of big data and a huge base of user generated data we have seen a shift to deep-level features [10]. In this section, we discuss various state-of-the-art studies on fake news detection under the broader umbrella of content and social context of the news article as shown in figure 1.



Figure 1: Fake News Detection Methods



Content Based- The content-based fake news detection method aims to detect fake news by analysing the content [11] i.e. either the text or image or both within the news article. Knowledge-based approaches utilize fact checking method in which the given claim is compared with the external sources to verify the authenticity of the given claim. The expert-based methods use expert-oriented approach and rely on human experts working in specific domains for decision making. For crowd sourced approaches, "wisdom of crowd" helps to check the accuracy of the news articles. A similar approach is used that provides a platform for people to discuss important news articles and finds out their accuracy. Crowd-sourced fact-checking is even though relatively difficult to manage, biased, has conflicting annotations, is less credible but has better scalability as compared to expert-based factchecking.

Style Based- Style-based fake news detection follows the same approach like knowledge-based fake news detection of analyzing the news content. However, instead of evaluating the authenticity of news content this method assess the intention of writer to mislead the public [12]. Fake news publishers usually have intent to influence large communities while spreading distorted and misleading information. To make the titles catchy fake titles use mostly all capitalized words, significantly more proper nouns, and fewer stop words.

Linguistic Based- Twenty-six linguistic based textual features were proposed which has an enhanced set of linguistic features to discriminate between fake and real news. Researchers have used network account features in addition to the linguistic features and also proposed Social Article Fusion (SAF) model that uses social engagements features along with linguistic. They have used linguistic features to distinguish real form fake news content [13].

Visual Based- Visual content is often viewed as evidence that can increase the credibility of the news article [14] and hence the fake news publishers tend to utilize provocative visual content to attract and mislead readers. Various visual and statistical image features are extracted for news authentication. Verifying Multimedia Use task under the MediaEval-16 benchmark addresses the problem of detecting digitally manipulated (tampered) images.

Network Based- Network-based fake news detection studies different social networks like friendship, tweetretweet, post-repost networks to detect fake news. It detects who spreads the fake news, relationships among the spreaders and how fake news propagates on social networks. Users tend to create various networks on online platforms media in terms of their common interests and similarities, these networks serve as paths for information diffusion. There are various networks on social media which gives valuable insights about spreaders of the news and how spreaders connect with each other [15].

Temporal Based- Studies have shown that news stories on the Internet are not static but are constantly evolved over time by adding new information or twisting the actual claim. This is very much evident in cases where the rumors resurge multiple times after the original news article is posted. The lifecycle analysis of rumour helps in understanding this phenomenon and examined the recurring rumors at the message level across different time periods. Researchers have provided deep understanding into the diffusion patterns of rumors over time [14].

Credibility Based- The credibility of claim, publisher, and spreader is often assessed by its news quality and trustworthiness/ credibility. It identifies the users spreading rumour by leveraging the concept of believability. Researchers have focused on assessing credibility of the given claim and proposed a credibility analysis system for evaluating credibility of a Tweet and prevents the proliferation of fake or malicious information. TweetCred is a web-based system that evaluates credibility of the tweet in real time [15].

3. Deep Learning Approach For Fake News Detection

Deep learning models have seen exceptional growth in recent times owing to their promising success in several fields, including communication and networking, computer vision, intelligent transportation, speech recognition, as well as NLP. Deep learning systems have advantages over traditional machine learning methods. Deep learning is a sub field of machine learning strategies, which displays high precision and exactness in fake news detection. In contrast, DL systems can acquire hidden representations from less complex inputs. The hidden features can be extracted from both the news content and context varieties. A study has also shown that deep neural networks (DNNs) require less time than other ML-based classification algorithms such as logistic regression, random forest (RF), and SVM, etc. However, DNNs use more memory. Convolutional neural network (CNN) and recurrent neural network (RNN) are two broadly utilized ideal models for deep learning in cutting-edge artificial neural networks. After inspecting previous studies, we found a general framework for deep learning-based fake news detection. The first step was to collect a dataset or create one. Most studies have used news articles collected from publicly available datasets. The pre-processing technique was applied after collecting the dataset to feed the data in a neural network. Word2vec and GloVe word embedding methods have mostly been used in previous studies to map words into vectors. We represent an overall process for fake news identification with deep learning in Figure 2 based on various studies.





Figure 2: The diagram illustrates the general deep learning-based architecture that was used in most studies.

4. Types of Neural Network Architectures

Given the significant breakthrough in neural network research, we used various versions of deep neural nets detailed in further sections. In this section we discuss different versions of neural network architectures used in common research.

Dense Neural Networks (DNN)- The fully connected dense neural network allows us to pass the input as sequence of words. The layered architecture allows us to experiment with the right depth that is needed for our task. The network consists of an input layer, an output layer and can consist of series of hidden layers as shown in figure 3.



Figure 3: Architecture of DNN

Convolution Neural Networks (CNN)- CNN are very similar to ordinary Neural Networks: they are made up of neurons that have learnable weights and biases. A CNN consists of an input and an output layer, as well as multiple hidden layers. The hidden layers of a CNN typically consist of convolutional layers, pooling layers, fully connected layers and normalization layers as shown in figure 4.

Recurrent Neural Networks (RNN)- RNN are popular with sequential data as each unit can have memory about the state of previous unit. This is particularly useful in natural language processing because it helps gain deeper understanding of language. RNN's have an input layer, output layer and can have a number of hidden recurrent units which have memory gates as shown in figure 5.



Figure 5: Architecture of RNN

Graph Neural Network (GNN)- GNN is a form of neural network that operates on the graph structure directly. Node classification is a common application of GNN. Essentially, every node in the network has a label, and the network predicts the labels of the nodes without using the ground truth. The network extends recursive neural networks by processing a broader class of graphs, including directed, undirected graphs, and cyclic, and it can handle node-focused applications except any pre-processing steps.



Figure 6: Architecture of the Graph Convolution Neural network Model

The network extends recursive neural networks by processing a broader class of graphs, including cyclic, directed, and undirected graphs, and it can handle nodefocused applications without requiring any pre-processing procedures cite190. GNN captures global structural features from graphs or trees better than the deep-learning models discussed above. GNNs are prone to noise in the datasets. Adding a little amount of noise to the graph via node perturbation or edge deletion and addition has an antagonistic effect on the GNN output. Graph convolutional network (GCN) is considered as one of the basic graph neural networks variants. The overall architecture of GNN model is given in Figure 6.



Generative Adversarial Network (GAN)- GANs are deep learning based generative models. The GAN model architecture consists of two sub-models: a generator model for creating new instances and a discriminator model for determining whether the produced examples are genuine or fake generated by the generator model as shown in figure 7. Existing adversarial networks are often employed to create images that may be matched to observed samples using a mini max game framework. The generator model produces new images from the features learned from the training data that resemble the original image. The discriminator model predicts whether the generated image is fake or real. GANs are extremely successful in generative modelling and are used to train discriminators in a semi supervised context to assist in eliminating human participation in data labelling. Furthermore, GANs are useful when the data have imbalanced classes or underrepresented samples.



5. Literature Survey

Previous studies for fake news detection models based on GNNs are compared in Table 2. We presented the main steps, advantages, and disadvantages of GNN-based methods for fake news detection. Some of our assessments are as follows: Regarding the extracted features,[11] used only user-based features; [12] used features based on networks, users, and linguistics; and [15] used linguisticbased features (textual analysis). Meanwhile, [13] used features related to networks and linguistics. Regarding graph structure, [11, 12, and 14] constructed a homogeneous graph. However, unlike [11, 14] only one graph was constructed, and [12] created two sub graphs to represent news sources and news users. Meanwhile, [13] built a heterogeneous graph with two types of nodes and edges. However, although the graph structure of [13] is better than that of the other three models, [14] provide the best performance. This result may be because [12] can better extract meaningful features in fake news detection. Therefore, to develop new GNN-based models in the future, more attention should be given to extracting excellent features and building good standard data instead of focusing on improving the graph structure.

Figure 7: GAN architecture

Table 2:	Comparison	of GNN	methods

References	Critical idea	Advantage	Disadvantage
Yi Han et al. [11]	Propagation-based fake news detection method They have focused on continual learning and incremental training techniques and used two techniques: EWC and GEM	Can improve the performance of conventional methods without using any text information. It can handle unseen data and new data	Ignore the selection of features or the finding of "universal" features
Fang [12]	Contextual fake news detection method – Focus on representation quality by capturing sharing patterns and social structure	Improve representation quality, Can use to a limited training dataset, Can capture temporal patterns of fake news	Stance detection and textual encode have not been jointly optimized, Sharing contents and hyperlinks become obsolete quickly
Safer [13]	Contextual fake news detection method – Focus on combining information: content nature, user behaviors, and users social network	Improve the performance of the traditional GNNs, Can add more layers to identify more efficacy neighbourhood	Sensitive to bottleneck and over smoothing problems
Benamira et al. [14]	Focus on analyzing the news content using semi-supervised learning. They have used Binary classification model	Can obtain high efficacy with limited labelled data	Have not been evaluated with big data and multi labelled data
FakeNews [15]	Focus on two tasks aiming to analysis and detect fake news via news textual and news structure	Can use to multi-classification tasks, Binary classification task obtains significantly higher performance than the ternary ones	Tasks implement separately corresponding to information textual and structure



6. Evaluation Metrics

Although a model may have a higher classification result once constructed, it must be determined whether it can address the specific problem in different circumstances. Classification accuracy alone is usually insufficient to make this judgment. Other assessment metrics are necessary for proper evaluation. Since a promising method is required to pass the assessment metric's evaluation, it is easy to create a model, but it is more challenging to create a promising strategy. Diverse evaluation metrics are used to evaluate the model's efficiency. The evaluation matrix is an essential device for arranging and organizing an evaluation. The confusion matrix shows an overview of model performance on the testing dataset from the known true values. It provides a review of the model's success and useful results of true positive, true negative, false positive, and false negative. We provide some evaluation metrics that were widely used in previous studies:

Accuracy- The accuracy score, also known as the classification accuracy rating, is determined as the percentage of accurate predictions in proportion to the total predictions made by the model. The accuracy (A) can be depicted by the given below formula:

 $A = \frac{TruePositive + TrueNegative}{TotalNumberofPredictions}$

Precision- Precision (P) is defined as the number of actual positive findings divided by the total number of positive results, including incorrectly recognized ones. The precision can be computed by the given below formula:

$$P = \frac{TruePositive}{Positive + FalsePositive}$$

Recall- When the total number of samples that should have been identified as positive is used to divide, the number of true positive results is referred to as recall (R). The recall can be computed by the given below formula:

$$R = \frac{TruePositive}{TruePositive + FalseNegative}$$

F1-Score- The model's accuracy for each class is defined by the F1-score (F1). If the dataset is not balanced, the F1score metric is typically used. The F1-score is often used as an assessment matrix in fake news detection [41], [157], [158]. F1-score computation can be performed by the given below formula:

$$F1 = 2 \times \frac{precision \times recall}{precision + recall}$$

ROC Curve and AUC- The Receiver Operating Characteristics (ROC) curve shows the success of a classification model across several classification thresholds. True Positive Rate (Recall) and False Positive Rate (FPR) are used in this curve. AUC is an abbreviation for "Area under the ROC curve". In other words, AUC tests the whole two-dimensional field under the entire ROC curve. The FPR can be defined by the given below formula:

 $FPR = \frac{FalsePositive}{FalsePositive + TrueNegative}$

7. Conclusions

With an increase in the popularity and usage of social media over the past few years, a huge population of readers prefer to consume news from social media instead of traditional news media. Keeping this in mind, many publishers use social media and Internet in general as breeding grounds for spreading propaganda and rumours rapidly which has strong negative impacts on the society. In this text we have mentioned several freely available Fake News Detection tools that should be used so that we forward only credible and genuine news. This survey looks at finding fake news, especially using Graph Neural Networks. It studies many different ways and problems, and talks about how these networks help fight wrong information. It combines lots of research to give a big picture of how these networks work in stopping fake news. It gives us good ideas for more research and new ways to make better tools to stop fake news from causing problems in society. By analysing a wide array of methodologies, challenges, and advancements, this survey offers a comprehensive overview of GNN-based approaches in terms of fake news detection.

Reference

- [1] Tian Bian, Xi Xiao, Tingyang Xu, Peilin Zhao, Wenbing Huang, Yu Rong, and Junzhou Huang. 2020. Rumor Detection on social media with Bi-Directional Graph Convolutional Networks. (2020), arXiv:2001.06362
- [2] Semi-Supervised Learning and Graph Neural Networks for Fake News Detection Adrien Benamira, Benjamin Devillers, Etienne Lesot, Ayush K. Ray, Manal Saadi, Fragkiskos D. Malliaros, CentraleSupelec, University of Paris-Saclay, France Email: {adrien.benamira, benjamin.devillers, etienne.lesot, manal.saadi}@supelec.fr, ayush.rai2512@student-cs.fr†Inria Saclay, France Email: fragkiskos.malliaros@centralesupelec.fr
- [3] Guacho, G. B., Abdali, S., Shah, N., Papalexakis, E. E. (2018, August). Semi-supervised Content-based Detection of Misinformation via Tensor Embeddings. In 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM) (pp. 322-325). IEEE.
- [4] Thekumparampil, K. K., Wang, C., Oh, S., Li, L. J. (2018). Attentionbased graph neural network for semi-supervised learning. arXiv preprint arXiv:1803.



- [5] Peters, M. E., Neumann, M., Iyyer, M., Gardner, M., Clark, C., Lee, K., Zettlemoyer, L. (2018). Deep contextualized word representations. arXiv preprint arXiv:1802
- [6] Horne, B. D., Adali, S. (2017). This just in: fake news packs a lot in title, uses simpler, repetitive content in text body, more similar to satire than real news. In Eleventh International AAAI Conference on Web and Social.
- [7] K. Shu, A. Sliva, S. Wang, J. Tang, and H. Liu. (2017). Fake news detection on social media: A data mining perspective. SIGKDD Explor. Newsl., 19(1)
- [8] CWSM. [16] V. Perez-Rosas, B. Kleinberg, A. Lefevre, and R. Mihalcea. (2018). 'Automatic detection of fake news. In ACL, pp. 339
- [9] H. Rashkin, E. Choi, J. Y. Jang, S. Volkova, and Y. Choi. (2017). Truth of varying shades: Analyzing language in fake news and political factchecking. In EMNLP, pp. 2931– 2937.
- [10] K. Shu, D. Mahudeswaran, S. Wang, D. Lee, and H. Liu. (2018). FakeNewsNet: A data repository with news content, social context and dynamic information for studying fake news on social media. arXiv
- [11] Y. Han, S. Karunasekera, C. Leckie, Graph neural networks with continual learning for fake news detection from social media, 2020, arXiv preprint arXiv:2007.03316.
- [12] V.-H. Nguyen, K. Sugiyama, P. Nakov, M.-Y. Kan, Fang: Leveraging social context for fake news detection using graph representation, in: Pro- ceedings of the 29th ACM International Conference on Information & Knowledge Management, 2020, pp. 1165–1174.
- [13] S. Chandra, P. Mishra, H. Yannakoudakis, M. Nimishakavi, M. Saeidi, E. Shutova, Graph-based modeling of online communities for fake news detection, 2020, arXiv preprint arXiv:2008.06274.
- [14] A. Benamira, B. Devillers, E. Lesot, A.K. Ray, M. Saadi, F.D. Malliaros, Semi-supervised learning and graph neural networks for fake news detection, in: 2019 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, ASONAM, IEEE, 2019, pp. 568–569.
- [15] A. Hamid, N. Shiekh, N. Said, K. Ahmad, A. Gul, L. Hassan, A. Al-Fuqaha, Fake news detection in social media using graph neural networks and nlp techniques: A COVID-19 use-case, 2020, arXiv preprint arXiv:2012.07517.