Is it Fake? News Disinformation Detection on South African News Websites

Harm de Wet
Department of Computer Science
University of Pretoria
Pretoria, South Africa
harmdewet01@gmail.com

Vukosi Marivate
Department of Computer Science
University of Pretoria
Pretoria, South Africa
vukosi.marivate@cs.up.ac.za

Abstract—Disinformation through fake news is an ongoing problem in our society and has become easily spread through social media. The most cost- and time-effective way to filter these large amounts of data is to use a combination of human and technical interventions to identify it. From a technical perspective, Natural Language Processing (NLP) is widely used in detecting fake news. Social media companies use NLP techniques to identify the fake news and warn their users, but fake news may still slip through undetected. It is especially a problem in more localised contexts (outside the United States of America). How do we adjust fake news detection systems to work better for local contexts such as in South Africa. In this work we investigate fake news detection on South African websites. We curate a dataset of South African fake news and then train detection models. We contrast this with using widely available fake news datasets (from mostly USA website). We also explore making the datasets more diverse by combining them and observe the differences in behaviour in writing between nations’ fake news using interpretable machine learning.

Index Terms—disinformation, fake news, machine learning, natural language processing

I. INTRODUCTION

Modern technology makes it easy for anyone with access to a cell phone or computer to publish anything online, regardless of expertise on the topics. For humans, it is getting harder to distinguish between factual news and fake news [1]. It is not feasible for online companies to have a team of people read everything that is being portrayed as news for validity. Although research has been done and tools, e.g. machine learning, are in place at some social media companies to identify and warn users [2], there is still a lot of fake news on these platforms. This could be due to localisation or national differences in the way people write and/or conceal fake news. For example, the way South Africans and Americans speak and write English is not the same. South Africa further may have instances of code-switching [3].

In this work, we investigate developing a machine learning model to detect South African fake news websites/content. We investigate the impact of using US fake news datasets against using a new dataset that is focused on South African fake news. For people to trust such a model to analyse news for them, the model should not be a black box where they cannot see how it classifies news as fake or factual. Thus, interpretable machine learning is used, highlighting on the articles’ text used for evaluation and testing how much which parts contributed to the prediction [4]. The stylistic differences or behavioural characteristics between writing fake news and real news are also investigated in the interpretable articles when the model predicts on an article although it is not very obvious to spot these differences. We further release, with this paper, the South African fake news website dataset.

II. BACKGROUND

A survey from 2016 by BuzzFeed [1] found that 75% of American adults are fooled by the fake news headlines. If this study should reflect a wider part of the world’s population to a reasonable extent, the damage that fake news can cause becomes serious. It should be clear that fake news has the potential to ruin people’s lives and businesses. It should also be clear that fake news can be used for other agendas such as misleading people to vote for another party amongst other things. This is well documented as Information Disorder [5]. South Africa is not immune and has had its own challenges with disinformation [6]. Because of increased demand in fact-checking for fake news detection, multiple researchers have tried multiple Natural Language Processing (NLP) techniques to automate the task because of the large amount of data available. Fact-checking by a person requires researching and identifying evidence, understanding the information and what could be inferred from it which is a tedious task for everything that has to be checked. Thus a human has to be in the loop.

Natural language processing is a range of computerised computational techniques used to analyse text linguistically such that a computer can achieve a human-like language processing for real world application. The text used to train, evaluate and use the model has to be in a language used by humans to communicate and not constructed for analytical purposes [7]. There are multiple approaches to NLP, the two popular ones are statistical (mathematical) and machine learning (artificial intelligence) based approaches. Statistical approaches use mathematical techniques to model linguistic phenomena and only use observable data as a source of evidence. As part of machine learning we have neural network based approaches that take large amounts of text data into consideration when creating a model, taking into account the purpose of the model resulting in a more robust model [7].
Supervised learning, an artificial intelligence learning approach, learns a function that maps input (n-dimensional vectors) to their respective desired output [8]. Typically, the training data is given to the model as example input-output pairs without any specific rules. To create the mapping function, neurons are created with some arbitrary values called weights. These weights are changed in the training process to ensure each example input maps to its desired output, or as close to it as possible. In most fake news detection models, supervised learning is the training method of choice. Using existing articles and or statements that has been classified by means of fact-checking [9]. A typical text classification problem, even more so for fake news detection, is that the evaluation of a claim requires more context than just the fact being evaluated. Another problem is that well-constructed sentences may also convey false information [9], thus the model would need to be trained with more context in mind.

Another approach that has been tested is using information surrounding the article like the author, origin, and credit history of the author [10]. The problem with this approach is that it can introduce bias to the model, thus we will only be using the text content of the articles. When the model does not have knowledge of the author, the model would not be able to successfully classify the article. Most research on fake news detection has been done using very specific attributes and only focusing on certain aspects of the problem. Various combinations of the following were used:

- Short political facts [11], [12].
- Social media statements [11], [13].
- Authors, location, affiliation, speaker title and credit history [12], [10].
- Number of followers, likes and comments (media platform dependent) [13].
- Authenticity [14], [15].
- Tone, emotion [14], [15].
- Lexical, syntactic, semantic and readability properties [10], [11].

Interpret means to “present in understandable terms” [16]. Which is an important aspect of machine learning as some countries require algorithms that make decisions on interpretations of humans to provide an explanation [17]. Interpretable machine learning can be divided into two broad categories, namely intrinsic interpretability and posthoc interpretability. Intrinsic interpretability [18] is the art of constructing the model itself to explain what it does. For intrinsic interpretability there are some trade-offs that one needs to be aware of, between prediction accuracy and interpretability. Post-hoc interpretability [18] is the art of creating a second model that can explain the main model by modelling what the main model has done then attempt to explain what the main model has done. This method only estimates what the main model had done but there are no trade-offs in the main model’s performance or accuracy.

We investigate the stylistic differences in writing between nations with machine learning in areas where it could play an important role, such as fake news detection.

### III. Dataset Creation and Exploration

#### A. South African Dataset

We used, as sources, investigations by the news websites MyBroadband [19] and News24 [1]. These articles covered investigations into disinformation websites in South Africa in 2018. They compiled lists of websites that were suspected to be disinformation. During the period from those articles to present, a number of the websites have become inaccessible or offline. We attempted to use the internet archives WayBack Machine [5] we could only get partial snapshots and error messages.

A web-scraper only worked for one of the sources although manual editing was still required to clean the text from Javascript code and some paragraph duplicates. On most of the other websites, a web-scraper did not work well as there were too many advertisements and broken parts of pages. Because of all these problems, most of the articles were manually copied and pasted and cleaned in flat files. In some cases, the text of articles could not be copied and was not made part of the South African disinformation corpus.

Real or truthful South African news used for training and evaluation of models was sourced from Media Monitoring Africa [1], an independent organisation that monitors South African news agencies. These articles were already cleaned, noise removed and duplicates extracted. The real and fake news from South Africa was combined to form the SA 1 dataset. You can see the summary statistics for the SA corpus data in Fig 1. We make available the South African fake news website data available through an online repository [https://github.com/dsfsi/sa-fake-news-2020](https://github.com/dsfsi/sa-fake-news-2020) or [https://doi.org/10.5281/zenodo.4682843](https://doi.org/10.5281/zenodo.4682843) for others to be able to use.

#### B. United States of America (USA) Dataset

The US datasets were used to evaluate how our approach to the South African disinformation detection could generalise across different news and disinformation sources as well as the other way round. Further, the USA data was used in combination with the SA corpus to create a combined model that straddles the two countries.
You can see the summary statistics for the US dataset has more data but upon inspection the data was found to contain more noise than the South African dataset. 

The scaled down dataset originated from a Kaggle dataset named Fake and real news dataset from Kaggle, names ... https://github.com/lutzhamel/fake-news.

We have two USA datasets, US 1 and US 2. US 1 data contains a scaled down dataset that originated from a Kaggle Dataset on Getting Real about Fake News. The scaled down dataset contains equal amounts of real and fake news data and is available on GitHub. The US 2 data is also from Kaggle, names Fake and real news dataset. The dataset has more data but upon inspection the data was found to contain more noise than US 1. We use it for generalisation evaluations. You can see the summary statistics for the US corpus data in Fig 5.

IV. MODELLING

There are three aspects to this research that build on top of each other:

• fake news classification,
• stylistic understanding,
• and making the results interpretable such that a person can understand the model’s prediction.

To evaluate the stylistic understanding of the models, two models of each neural network type were trained, one with SA corpus and the other with US corpus then each model’s test data was used to evaluate the other model trained with the different nation’s data.

A. Pre-processing

The text is cleaned from all punctuation and capitalization as it is assumed that it does not contribute to the context and behaviour in the article. Stopwords have also been removed from the text for some of the models stopwords do not contribute enough to the overall performance of the models and that it reduced the dataset size and computation time with minimal, if any, accuracy loss.

https://github.com/lutzhamel/fake-news
For the base models we used Term Frequency — Inverse Document Frequency (TF-IDF) encoding for the words, the length of the articles was not modified. For the Long short-term memory (LSTM) models, the first 500 words were used in training and testing. The mean length of each corpus is less than 500 words (see Table I). A tokenizer was used to encode the words, splitting the words into an array, turning each word into its numeric position in the word dictionary. For all articles under 500 words in length, the encoded list of vectors were padded with zeros.

Text augmentation was used in some cases to expand the limited dataset. From the accuracy table, it was shown that increasing the training data using augmentation proved to be effective [26]. WordNet based augmentation was used with the TextAugment library.

B. Models

1) Base Models: The starting point of the neural network experiments was to get a simple baseline model to evaluate the output of the more complicated models. Logistic regression with a TF-IDF bag-of-word encoding. For Logistic Regression and Passive Aggressive Classifier base models, the Scikitlearn libraries were used. These libraries determine the layers and nodes required for the models itself.

2) LSTM Models: For the LSTM models Keras was used and each layer customised, and layers put together to form the model. Word2Vec [27] was used to create a matrix of word representations for every word in the dictionary that is used by the tokenizer. These embeddings formed a matrix of values that became the weights for the untrainable embedding layer that receives the padded token sequences as input and turns it into the embedded representation of the word. The embedding layer made it possible to have a smaller memory footprint since it was not required to have the trained Word2Vec model in memory to embed words before the model can be used. The drawback of this approach was that words that are not in the dictionary but in the text that was predicted, will not be used as input for the prediction.

The embedding layer was followed by a dropout layer to add regularization to the model when training. Then, followed by the convolutional is the max pooling layers used to extract features and reduce the size of the model. Finally, the layers are followed by 2 LSTM layers ending in 3 layers feed-forward fully connected layers. The following activation functions were attempted in some of the layers of the LSTM models: Hyperbolic Tangent (TanH), Yann LeCun TanH, Elliot, Rectified Linear Unit (ReLU) and Sigmoid. Only ReLU and Sigmoid, in combination, produced report worthy results.

V. EXPERIMENTS

The data used to train the Logistic Regression models consisted of balanced classes. Training with the American corpus produced a better accuracy score than the model trained with the South African corpus. Predicting classes for the US corpus using the SA corpus trained model produced poor results. Refer to Table II. The F1 score for this experiment is 0.564 with a per class accuracy of 0.431 for fake news articles and 0.696 for true news articles. The drop in accuracy was expected but turned out to be more severe than the expectation. Predicting classes for the SA corpus using the US corpus trained model also produced poor results but even more so for classifying the fake news itself. With an F1 score of 0.473 and a per class accuracy of 0.260 for the fake news articles and 0.686 for the true news articles.

To preserve the context of word sequences, LSTM neural networks were constructed. To create an LSTM model baseline, equal numbers of articles of fake news and real news were used to train the models. The balanced classes trained and tested LSTM model trained with SA corpus achieved 0.520 accuracy and the US corpus trained model achieved 0.895 accuracy.

To increase the accuracy of the first LSTM models, a data imbalanced model was trained with the SA corpus, since there are more real than fake news in the real world, reaching an accuracy of 0.755. No training data imbalance was introduced to the American trained model as the data source only contained half of each class.

To increase the accuracy of the US corpus trained LSTM model, Wordnet based augmentation [26] was used to expand the dataset. The increased dataset size improved the model’s accuracy score from 0.755 to an average of 0.845. Augmenting the US corpus also increased the American trained models accuracy from 0.895 to an average of 0.968.

Combining the SA corpus and the US corpus (US 1) for training and testing another model, the model reached an average accuracy score of 0.884 and a peak of 0.906 which is better than testing different nations’ data on different models. The results were harder to analyse for behavioural characteristics and the accuracy a bit lower, but it performed better than training models with one nations data and testing with another nation’s data. The final LSTM models were trained 5 times to get an average accuracy score. Refer to Table II for results.

VI. MODEL PREDICTION INTERPRETABILITY

The logistic regression models’ results were made interpretable using Local interpretable model-agnostic explanations (LIME) [28]. Analysing the articles with the LIME explanations showed that the model relies on the presence and counts
of specific keywords to make its prediction, not taking enough context into account. The word based reliability can be seen in the Fig 4.

Intrinsic interpretability was used to make these LSTM models interpretable. Two permutation layers were added and the weights of the second permutation layer was extracted from the model. These weights were used as values to indicate how much which words in the text contributed to the classification. When a piece of text was processed by the model, a breakdown of how much each word contributed to the classification was given as a bar graph with only the contributing words and the text itself. The words are highlighted lighter or darker according to the weight that it contributed to the classification. See Fig 5.

A. Discussion and observations

The following were the behavioural factors contributing to the classification for the trained models

1) SA corpus models: There was sentence repetition in some of the fake news that was not found in the real news. The fake news contained more exaggerated words and phrases than real news and in some articles multiple exaggerations for example:

- “billion rand taken tenders worth billions” - article 3
- “deadly pandemic” - article 4
- “deep loss” - article 5
- “unbearable pain” - article 5
- “work tirelessly” - article 5
- “wanton violence” - article 5
- “deep pain” - article 5

In some cases it seems like the model takes simplified words and speech as an indication that an article is fake news, this could be the reason why some real articles have been classified as fake, for example:

- “hes giving all thanks” - article 1
- “fix issues” - article 3
- “lucky” - article 4
- “employers and employees who actually employ” - article 4
- “crash” - article 1

Counter examples for the simplified words and speech:
- “selection criteria focussed on” - article 7
- “own constitution on eligibility” - article 7
- “warned defaulting municipalities” - article 9

In some articles phrases highlighting the biased and opinionated behaviour of the writer was used as contributing factor to a fake news classification for example:

- “da understands better than anyone” - article 3
- “people are supposed to” - article 4

2) US corpus models: There is fewer repetition of sentences than in the South African fake news, but in most cases with repetition, the second and third time the same sentence is present, the wording is slightly changed. The fake news was also found to be more opinionated than the real news for example one could see the author referred to themselves as being part of some group where injustice occurred. “these people must think the Americans are stupid” - article 4

There was also some places where it seemed like the model used exaggeration as part of the classification of fake news: “have seen countless aggravated assaults” and “down right murders” -article 4. But then there were also cases where a fake article was marked as real with high probability where exaggeration is present like in article 13. In both South African and American fake news, it appears that third person speech is more prevalent in fake news than in real news and first person speech more prevalent in real news than in fake news.
Also found in both nations’ data is racial words and expressions and curse words, with the correct and the wrong spelling, that the models used to distinguish the fake and real news from each other as a basis to classify articles as fake news, but not in all cases. One nation’s model performed poorly classifying another nations data because the data used for the training might not be diverse enough and the different nations’ datasets news categories also do not overlap enough. After an analysis of the two different US corpus, the news diversity was poor since the model trained with the one set performed poorly on the other set, however in the same set, the models achieved good prediction accuracy on the test data because we have a lot of data for each source.

The South African model also reached acceptable results with the SA corpus. This model could reach better performance with more data that is more diverse data. Better manual classification and inspection of training data could be part of the reason why the US corpus trained models performed better on their own data but poor on the other nation’s data. The model where both nations data was used together for training and testing also presented similar interpretable output with the same behavioural characteristics although it was difficult to spot them as it seemed a bit more random.

VII. CONCLUSION

In this work we have investigated the creation of fake news website detection models using a new South African dataset as well as two US datasets. We further provide insight into the behavioural factors that may lead the models to classify the websites as fake or not. This is just the beginning of providing models that are better suited for South Africa. We also release the South African fake news dataset as an online dataset for others to use and also expand on. There is still more work to be done. Investigations into changes into how fake news spread in South Africa is still to be done. What happens when the websites themselves change how they write to avoid detection. The archiving of past fake news websites is important as they tend to disappear after a few years. As such there is a need for archiving tools for such websites as they provide good data for future models.

VIII. ACKNOWLEDGEMENTS

The authors would like to thank Media Monitoring Africa for their support. Further, we would like to thank the reviewers for their feedback and Tshephisho Sefara for proof reading.

REFERENCES

[1] C. Silverman and J. Singer-Vine, “Most americans who see fake news believe it, new survey says,” Buzzfeed, 2017. [Online]. Available: https://www.buzzfeednews.com/article/craigsilverman/fake-news-survey
[2] A. Mosseri, “Working to stop misinformation and fake news,” Facebook, 2017. [Online]. Available: https://about.fb.com/news/2017/04/working-to-stop-misinformation-and-false-news
[3] R. Meshtrie and E. Hurst, “Slang registers, code-switching and restructured urban varieties in south africa: An analytic overview of sociotails with special reference to the cape town variety,” Journal of Pilgim and Creole Languages, vol. 28, no. 1, pp. 103–130, 2013.
[4] F. Doshi-Velez and B. Kim, “Towards a rigorous science of interpretable machine learning,” stat, vol. 1050, p. 2. 2017.
[5] C. Wardle and H. Derakhshian, “Information disorder: Toward an interdisciplinary framework for research and policy making,” Council of Europe report, vol. 27, 2017.
[6] H. Wasserman, “Fake news from africa: Panics, politics and paradoxisms,” Journalism, vol. 21, no. 1, pp. 3–16, 2020.
[7] E. D. Liddy, “Natural language processing,” in Encyclopedia of Library and Information Science, J. Fagerberg, D. C. Mowery, and R. R. Nelson, Eds. Marcel Decker, 2001.
[8] S. J. Russell and P. Norvig, “Artificial intelligence: a modern approach,” in Artificial Intelligence: a Modern Approach, 2013.
[9] A. Vlachos and S. Riedel, “Fact checking: Task definition and dataset construction,” in Proceedings of the ACL 2014 Workshop on Language Technologies and Computational Social Science. Baltimore, MD, USA: Association for Computational Linguistics, Jun. 2014, pp. 18–22. [Online]. Available: https://aclanthology.org/W14-2508
[10] Y. Long, Q. Lu, R. Xiang, M. Li, and C.-R. Huang, “Fake news detection through multi-perspective speaker profiles,” in Proceedings of the Eighth International Joint Conference on Natural Language Processing (Volume 2: Short Papers), 2017, pp. 252–256.
[11] V. Pérez-Rosas, B. Kleinberg, A. Lefevre, and R. Mihalcea, “Automatic detection of fake news,” 2017.
[12] W. Y. Wang, “’liar, liar pants on fire’: A new benchmark dataset for fake news detection.” 2017.
[13] K. Shu, A. Sliva, S. Wang, J. Tang, and H. Liu, “Fake news detection on social media: A data mining perspective,” ACM SIGKDD Explorations Newsletter, vol. 19, 2017.
[14] N. K. Conroy, V. L. Rubin, and Y. Chen, “Automatic deception detection: Methods for finding fake news,” Proceedings of the Association for Information Science and Technology, vol. 52, no. 1, pp. 1–4, 2015.
[15] V. Singh, R. Dasgupta, D. Sonagra, K. Raman, and I. Ghosh, “Automated fake news detection using linguistic analysis and machine learning,” 2017.
[16] “Merriam webster: Definition of interpret.”
[17] E. P. P. office of the eu, “Official journal of the european union,” data retrieved from, https://op.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba0a-01aa75ed71a1
[18] M. Du, N. Liu, and X. Hu, “Techniques for interpretable machine learning,” Communications of the ACM, vol. 63, no. 1, pp. 68–77, 2019.
[19] MyBroadband Forum, “List of known fake news sites in south africa (and beyond),” 2017, article accessed, https://mybroadband.co.za/forum/threads/list-of-known-fake-news-sites-in-south-africa
[20] M. Risdal, “Getting real about fake news,” 2019, data retrieved from Kaggle, https://www.kaggle.com/mrisdal/fake-news
[21] G. McIntire, “How to build a “fake news” classification model,” 2017, article accessed, https://opendatascience.com/how-to-build-a-fake-news-classification-model
[22] C. Bisaillon, “Fake and real news dataset,” 2020, data retrieved from Kaggle, https://www.kaggle.com/clemenbisaillon/fake-and-real-news-dataset
[23] H. Saif, M. Fernandez, Y. He, and H. Alani, “On stopwords, filtering and data sparsity for sentiment analysis of twitter,” in LREC 2014, Ninth International Conference on Language Resources and Evaluation. Proceedings, 2014.
[24] C. Silva and B. Ribeiro, “The importance of stop word removal on recall values in text categorization,” in Proceedings of the International Joint Conference on Neural Networks, 2003., vol. 3. IEEE, 2003, pp. 1661–1666.
[25] A. Scholfield, M. Magnusson, and D. Mimno, “Rethinking stopword removal for topic models,” in Proceedings of the 15th Conference of the European Chapter of the Association for Computational Linguistics: Volume 2, Short Papers, 2017, pp. 432–436.
[26] V. Marivate and T. Sefara, “Improving short text classification through global augmentation methods,” Machine Learning and Knowledge Extraction. CD-MAKE 2020. Lecture Notes in Computer Science. 2020.
[27] T. Mikolov, I. Sutskever, K. Chen, G. S. Corrado, and J. Dean, “Distributed representations of words and phrases and their compositionality,” in Advances in neural information processing systems, 2013, pp. 3111–3119.
[28] M. T. Ribeiro, S. Singh, and C. Guestrin, “why should i trust you?” explaining the predictions of any classifier,” in Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining, 2016, pp. 1135–1144.