Identifying Fake News from the Variables that Governs the Spread of Fake News.

Milan Dordevic, Pardis Pourghomi
College of Engineering and Technology
American University of the Middle East Egaila, Kuwait
{Milan.Dordevic, Pardis.Pourghomi}@aum.edu.kw

Fadi Safieddine
School of Architecture, Computing, and Engineering.
University of East London, London, UK
F.Safieddine@uel.ac.uk

Abstract— Several researchers have attempted to investigate the processes that govern and support the spread of fake news. This paper collates and identifies these variables. This paper then categorises these variables based on three key players that are involved in the process: Users, Content, and Social Networks. The authors conducted an extensive review of the literature and a reflection on the key variables that are involved in the process. The paper has identified a total of twenty-seven variables. Then, the paper presents a series of tasks to mitigate or eliminate these variables in a holistic process that could be automated to reduce or eliminate fake news propagation. Finally, the paper suggests further research into testing the method in lab conditions.

Keywords— Misinformation; Social Media; Fake News; Variables; Propagation.

I. INTRODUCTION

The spread of fake news has been likened to the spread of disease [1],[2],[3], & [7]. And medical researchers attempt to understand the range of a given disease by learning how it starts, transmits, behaves, disappears, those it infects and those it does not affect. In short, we understand better how to fight an epidemic by understanding the variables that govern the propagation of the virus. This paper proposes a holistic approach that is based on this ethos. The paper identifies the various variables the govern the transmission of fake news. In the process, this paper identifies four key players in facilitating such transmissions: Users, Content, and the Social Media Network. For social media users, the paper presents rumours and individual need to seek information that affirms that users with regards to users' behaviour is an attraction to rumours, predisposition to seek information that affirms that users believe, probability of taking action, and probability to verifying the information.

The study of rumours and how they propagate has long been linked to the study of epidemiology. Links that show rumours tend to spread very much in a similar way to how disease spreads have been demonstrated using mathematical epidemiology [4]. Daley and Kendall were able to confirm this spread using a variety of scenarios. Naturally, one would argue that real-world spread of rumours is different from social media online. Nevertheless, several of these characteristics are similar. The work in [5] proved that specific events involving the spread of rumour had been successfully modelled using epidemiologically modelling tools. Thus, Bettencourt et al. have been able to provide real-world examples that prove the theory that rumours resemble the spread of diseases. These experiments have helped identify critical variables such as individual contact rates, duration of the infectious period, and incubation time. One may argue that in the context of sharing of fake news, there is no incubation time online. Another variable we are able to discount is the recovery state of a user. While a user may never forget the fake news they read, this will not have implication when a user discovers a piece of news is fake.

[5] are the first to narrow these variables to four variables Susceptible, Exposed, Infected, Sceptic (SEIZ). In the SEIZ model, Susceptible is the degree a person is willing to accept a fact-based on their predisposition to believe it, Exposed is the number of times it takes for a user to believe the news, before this user is Infection with the fake news. In this context, infected means they start to believe it.
A model for the dissemination of fake news is shown in Figure 1 [6]. In this model, the user engages in the vulnerable state by using social media; they are exposed to the fake news; they then get infected. From that point, a user may move into Sceptics state after verifying the fake news. In this instance, the user who recovers can exist the process as they will not likely to be fooled by that same lie again.

Figure 1 A model for the dissemination of fake news [6, p.135].

In [7], the authors also used epidemiology inspired models to represent the spread of fake news on social media. By using these models, the authors have been able to prove SEIZ model to be supporting real-world simulations. Part of the process of how news spreads on multifaceted social media networks [7]. The authors in [7] used a mathematical system that demonstrated transitions of news from one state to another. By using probabilistic rules, the authors are able to prove the existence of a critical threshold after which rumours spread or otherwise the post would fail to go viral.

To understand the context of users on social media, [2] identified Susceptible- Ignorant (SI) model to argue the dynamics of rumour sharing verses anti-rumor dissemination on a multifaceted social media network. In the context of their study, Ignorant referred to those individuals who are not aware of the rumour yet. Thus, the ignorant user can be infected or vaccinated. Those infected ones may relay their infection (willingly) to other users. Whereas vaccinated users are those immunised by the anti-rumour messaging. What follows is an online war of rumour versus anti-rumour users. Key to these battles is the size of the population, connections of travel, and the number of people infected along the way.

One of the main issues in social network analysis is the impact of influential nodes. Several models can simulate the spread of rumours, fake news, innovations, diseases, etc. on social networks.

The susceptible/infected/susceptible (SIS) model is also presented in [9]. In this model, several nodes can be activated to illustrate the real scenario where users are bombarded by a piece of fake news that is eventually believed or disbelieved by users. The advantage that SIS model brings compare to the earlier described SIR model is that the computational complexity of SIS is a lot more than SIR since nodes can be activated multiple times.

A study on the dissemination of misinformation on social networks conducted by [10] investigates the effect of bad information campaigns which lead to misinformation diffusion on social networks. Influential users who can potentially start a counter-campaign to lessen the impact of those bad campaigns are their central factor of consideration in their study. They argue that counter-campaigns have their limitations. They named the main limitation as eventual influence limitation problem, which addresses the implication that starting the campaign early or late could have. Moreover, their study examines the problem of influence limitation in the presence of missing information. For this problem, they suggest an optimisation technique where the nodes that are probably infected by bad campaigns are selected.

Table 1 illustrates a list of the variables identified for Users

<table>
<thead>
<tr>
<th>Variables</th>
<th>Notation</th>
<th>Explanation</th>
<th>Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Rate</td>
<td>CR</td>
<td>The number of people who would get in contact with the fake news.</td>
<td>[5]</td>
</tr>
<tr>
<td>Susceptible</td>
<td>S</td>
<td>Individuals who likely believe fake news.</td>
<td>[5]</td>
</tr>
<tr>
<td>Exposed</td>
<td>E</td>
<td>The time it takes users from first exposed to fake news before they move to the next stage of believing in fake news.</td>
<td>[5]</td>
</tr>
<tr>
<td>Infected</td>
<td>I</td>
<td>The rate or number of people who believe the fake news.</td>
<td>[5]</td>
</tr>
<tr>
<td>Sceptic</td>
<td>Z</td>
<td>The rate or number of people who will question the fake news.</td>
<td>[5]</td>
</tr>
<tr>
<td>Recovered</td>
<td>R</td>
<td>The rate or number of people who may have believed the fake news but later debunked it.</td>
<td>[7]</td>
</tr>
<tr>
<td>Total population</td>
<td>N</td>
<td>The maximum population that given fake news can reach.</td>
<td>[2]</td>
</tr>
<tr>
<td>Edges</td>
<td>E</td>
<td>The connections between individuals as fake news travel.</td>
<td>[2]</td>
</tr>
<tr>
<td>Vertices</td>
<td>V</td>
<td>Individual exposed as fake news travel. Individuals can have different states: ignorant, infected, or vaccinated. These variables correspond to earlier variables S, I, and R.</td>
<td>[2]</td>
</tr>
<tr>
<td>Influential Node</td>
<td>IN</td>
<td>A node with many followings and much influence on several nodes. Therefore, it can propagate the spread of fake news. Thus, these can be characterised as 'bad campaign.'</td>
<td>[9, 10]</td>
</tr>
<tr>
<td>Counter Influence Node</td>
<td>IC</td>
<td>A node with many followings and much influence on several nodes. But counter influence nodes will use influence to counter fake news.</td>
<td>[10]</td>
</tr>
</tbody>
</table>
Threshold | Th | The rate or number of re-posting/retweeting rate that is needed for a post to go viral. | [8] 

**B. Content:**

In [11], the authors used a decision tree-based model to investigate News Content (NC). The authors confirmed that news posts with time-sensitive subjects have more significant influence to spread than other content and thus can be separated mechanically. Trending news has features to include an address to a resource on the Internet and to have a much deeper propagation tree. Therefore, their research showed that the level of social network trustworthiness of a trending news post could be measured based on the source of the news and propagation tree. Factual news is broadcasted through authors who have previously posted a high number of news posts, originate at a single or a few users in the network, and have many re-posts. These characteristics cannot be replaced easily by a fake news originator. By demonstrating their approach, the researchers analysed microblog postings related to trending topics and were able to categorise them as credible or not credible. The results revealed a substantial variance in the algorithm news is broadcasted, and consequently, they were able to categorise posts automatically as probable genuine or not.

In addition, misinformation detection can be regulated through Support Vector Machine (SVM), which is a machine learning method which enables the organisation of particular data into different clusters [12]. The vector machines function by training specific data that are organised into different clusters. The objective of the SVM method is to categorise data into rumour data or non-rumour data and to maximise the border between these two clusters. The remunerations of applying the SVM approach are that it has an affinity to be precise and performs well on datasets that are smaller and more concise. However, SVM required a long time to train and supported by a large dataset. The classification can also be less effective when confronted with distorted datasets and overlapping classes.

One of the proposed SVM models was presented by [13] utilised Dynamic Series Time Structure (DSTS) with an idea to model the variation of news characteristics. These DSTS discovered that there is a variation of numerous social context features over time. An event is reflected as a set of microblogs associated with some particular topic. To sort the number of manageable structures, they converted the uninterrupted time stream of microblogs into fixed time intervals. Additionally, the authors presented a technique to represent using discrete quantities of the time stream for generating time stamps. Results showed that DSTS model with the time series achieved improvement in the detection of fake news given the lifecycle of events at the early stage of spreading.

Another such SVM model is the Radial Basis Function kernel (RBF) proposed in [14]. The authors collected a set of rumourrelated blogs from Sina Weibo - China’s leading blogging service provider. The researchers collected an extensive assembly of microblogs which were identified to be fake news. Moreover, they studied a set of structures extracted from microblogs and trained a classifier to automatically detect fake news from a mixed set of genuine and non-genuine information. Furthermore, the researchers restrained the impact of features on the clustering performance for the fake news quantity.

In [15], the authors presented a decision tree based ranking approach for detecting fake news through Enquiry Phrases (EP). The idea is to focus on searching for signal tweets and then group similar posts, accordingly, calling these an Enquiry Phrase. Additionally, the connected posts that do not enclose these phrases are collected together. Authors have identified phrases that seem to be used in early detecting of fake news. The critical phrases like "What?" "Is this true?" "Really?" indicated to be a part of posts that have a tendency in the dissemination of fake posts. Furthermore, the authors revealed that tweets asking verification questions or making adjustments to controversial declarations are a very important indicator of fake news spreading early in the life cycle.

Additionally, the researchers recognised various statistical variables, some proving to be more valuable than others. The key variables recognised are linked to the source where it evaluates average of tweet length, percentage of signal tweets, average numbers of words, URLs and mentions per any tweet in the cluster. There is no indication that any specific variable identified on its own has a high relationship in identifying rumours but rather their combination. Since these variables are linked to evaluating the source of fake news, one can look into including this part as the source evaluation variable.

**Table 2 Variables linked to content posted on Social Media**

<table>
<thead>
<tr>
<th>Variables</th>
<th>Explanation</th>
<th>Notation</th>
<th>Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Sensitive</td>
<td>Time-sensitive subjects have a more significant influence on the spread of news.</td>
<td>(TS)</td>
<td>[11]</td>
</tr>
<tr>
<td>Reference Source</td>
<td>Rating of the source for reliability based on historical track on re-posting of their news posts and organisation source.</td>
<td>(RS)</td>
<td>[11]</td>
</tr>
<tr>
<td>Fake News Dataset</td>
<td>Linguistic analysis that compares a given post with a dataset of posts that are categorised as fake news. Factors could lean towards indicating fake news.</td>
<td>(FN-DS)</td>
<td>[12]</td>
</tr>
<tr>
<td>Dynamic Timestamp</td>
<td>Setting a timestamp on posts and tracking their timeline allows better estimation if the news post is factual or fake.</td>
<td>(DT)</td>
<td>[13]</td>
</tr>
<tr>
<td>Enquiry Phrases</td>
<td>Analysis of the comments made by users to the post, allowing early detection of possible fake news.</td>
<td>(EP)</td>
<td>[15]</td>
</tr>
</tbody>
</table>
The authors in [16] recognised attributes related to the user, linguistic, network and temporal features of fake news and compared their characteristics in categorising fake news over time. The researchers considered the major dissimilarity between fake and non-fake news. The conducted research clarifies the spreading patterns of fake news over time. The suggested model is using a machine-learning algorithm to identify differences between the fake news and genuine posts continually. Moreover, the authors proposed two methods for fake news classification. Furthermore, the proposed algorithms intend to create a clear border between facts and fiction. More recent, [17] proposed a baseline model for early detection of rumours on social media through sorting news propagation paths using recurrent and convolutional networks. Their proposed method contains four major constituents. The first element is the propagation of path construction and transformation. The first is to identify the users involved in the dissemination of the news. The second element of the model is the Gated Recurrent Unit (GRU) propagation path representation which offers a vector representation for each transformed propagation path. The third element is the Convolutional Neural Networks (CNN) propagation path representation. CNN is, in short, a machine learning algorithm that is usually used to analyses visual imagery and consequently be able to draw analysis from the propagation path tree. The last element of the model is the propagation path classification. The authors performed tests on different datasets. Results demonstrated that the proposed method exhibit effective and efficient performance in detecting fake news online. Moreover, the authors emphasise that the algorithm depends mostly on common user characteristics and not complex attributes such as linguistic or structural features.

These variables described in this subsection characterise the Content factors, and they are summarised in table 2.

### C. Social Media Networks:

Probably the least researched actor in the process of fake news propagation; most likely due to the challenges it presents in quantifying the impact of SMNs. It is no secret that many of these online networks have various tools that play a role in supporting the spread of fake news, and these have been presented part of the content section.

In [18], the authors identified a collection of variables that tend to be shared among many social media platforms. The authors showed that fighting fake news online are governed by the following variables: authentication, passing on information, cross-wire, same level communication, and reverse validation. However, possibly the prime influencers in the spread of fake news are newsgroups, cyber-bots, and user influencers. In reviewing the influence of social media newsgroup in the dissemination of misinformation, the work of [3] showed the impact of what was found earlier as the protagonist of influencers. The tests demonstrated how authentication algorithms could significantly reduce the dissemination of misinformation on social media. The results revealed that social newsgroups have a critical power on the outburst of rumours as well as fighting fake news online.

This section, however, focuses on the backend of social media networks, such as platform algorithm that encourages dissemination and connections among users with similar interest – a process some have dubbed as 'filter bubble' [19]. There is evidence that there are circumstances were filter bubbles create an unhealthy one-sided environment were users view one-sided arguments on everyday issues. Researchers found evidence of filter bubble in groups that support antivaccination, deny global warming, support flat-earth belief, as well as when key political events take place in the form of elections and referendums [19].

In recent times, many of these SMNs have put in policies to combat fake news, including restrictions on advertising political posts or promoting political campaign [20].

<table>
<thead>
<tr>
<th>Table 3 Variables linked to Social Media platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Variables</strong></td>
</tr>
<tr>
<td>Sharing</td>
</tr>
<tr>
<td>Passing on information</td>
</tr>
<tr>
<td>Authentication</td>
</tr>
<tr>
<td>Crosswire</td>
</tr>
<tr>
<td>Same Level (Cluster) Communication</td>
</tr>
<tr>
<td>Reverse Validation</td>
</tr>
<tr>
<td>Newsgroup</td>
</tr>
<tr>
<td>Filter Bubble</td>
</tr>
</tbody>
</table>
Put together with the first three sets of variables; one can see the challenges platforms have in controlling the spread of fake news.

III. RESEARCH METHODOLOGY

This paper attempts to answer two research questions:

1. What are the key variables in the spread of fake news?
2. Can the understanding of these variables support an approach to automate the detection of fake news?

To answer these questions, the paper conducted a detailed literature review of journals and academic publication on the subject of variables linked to spread of Fake News. The paper then attempted to identify the key players and the variables that govern their interaction with social media posts. The paper focuses on its research on theories and applications where these variables have been demonstrated to impact the process of fake news propagation.

Put together the paper is able to generate a table that it believes covers all key variables that are at play in the ecosystem of fake news. From the list, the paper proposes a process that would allow a more efficient and effective method to the identification of fake news. The automated solution works by addressing each variable and proposing the steps required to develop an automated process that allows a faster and more robust way of identifying fake news while respecting individuals' right for freedom of expression and speech.

IV. IDENTIFYING FAKE NEWS FROM ITS VARIABLES

Based on the identified variables, it is easy to see how mitigating the different variables would result in better fake news detections and reduction in fake news propagation. By starting with the users, the analysis suggests having a healthy scepticism view of social networks postings regardless of the number of times one user may get the same message. Several elements in a social network post could be explored separately:

A. Source and text content:

Social media platforms should immediately flag posts which do not have a cited source, have an unfamiliar source, or have a questionable source as non-news related. Since one would expect the source of a reliable news article is a reputable media, the platform can provide links to the same news posts that been shared by more of those established sources.

One platform that lists multiple sources for a news article is Google news search. Google's platform facilitates the possibility of checking the sources of one piece of news simultaneously. Other platforms such as Yahoo News and Bing News also facilitate similar functionality but, in both platforms, only one is able to search the sources. If multiple sources are not found, one must explore the content. This step is linked to Reference Source (RS) factor, Authentication rate (A), and Recovery (R) when identifying it is fake.

B. Images:

Many of the news postings on social networks are distributed through visual aids such as images. This is to provide credibility to the post. Several browsers provided a right-click option to search the Internet for where an image appears. This is usually referred to as 'Reverse Image Search'. By examining the sources of these images, it can transpire if the image has been used in different contexts, recycled, or misrepresented. This step is also linked to Reference Source (RS) factor, Authentication rate (A) and Recovery (R) when identifying it is fake.

C. Date identification:

A mismatch between the date of the original source of an image or content can be an indicator of authenticity. In [6], the authors discussed the example of social media posts that went viral following the earthquake in Nepal in 2015. The picture is that of a brother and sister were a reverse image search identifies it as from Vietnam in 2007 and as such, is sufficient to debunk the claim. This approach links to Dynamic Timestamp (DT).

D. Flagging of Fake News

Many of the social networking platforms provide users with the option of reporting a specific post as fake. This does not need an explanation from the user's side; however, it requires several steps. Stopping the post spreading may hinder it from reaching the Threshold (Th).

E. Facilitate sharing and trending:

In the case of questionable content, social media should not block the post. Users should be allowed to raise their concerns, write it as a comment and share it. Other users will see this in the social network where they might add to the first comment and share the post to support the first user's opinion. If particular research shows that a specific post is fake, users who report this should have their comments highlighted or promoted as 'relevant'. The same should be done when a piece of fake news is debunked by a fact-checking website and be shared across the platform. The primary purpose of sharing is to raise awareness about posted fake news than whether the fake news is of interest itself. Another reason for actively sharing the fakeness of a post is that these users will get the momentum to expand their base. This could have an impact on the algorithm but will most definitely have an effect on Same Level (Cluster) communication (SL) and possibly Reverse Validation (RV).

F. Hinder the sharing and trending:

For Time-sensitive information (TS), such as breaking news that is based on users' accounts, should be slowed or hindered until a time when it is independently verified from multiple media.
This is particularly important when users are questioning a post. Allowing the unhindered sharing of such posts opens new opportunities for it to expand with impact on the Sharing variable (S) and may enforce the news to people who have already heard it from other sources with effect on Contact Rate (CR).

G. Actively removing the filter bubble:
To tackle the spread of fake news, platforms should facilitate positive influencers. This includes reliable newsgroups and media outlets. The promoting of a variety of sources that means readers get to see both sides of a given argument. In [20], the authors argue that social media platform promote posts from groups one may not agree with. Allow civil dialogues and the sharing of rational counter posts, users should share satirical posts to counter their argument. The worse that could happen is that some tribalists would block those users. However, this will have an impact in breaking the Filter bubble (F) where people cannot see other views, but also where more people respond and report fake news, it could impact the dynamics of closed newsgroups (NG).

H. Using A.I. as a supportive tool and not a censorship
Allowing the identification of linguistic identification of text that appears to be fake news and presented as factual news to be flagged and automatically reported to third-party factcheckers would facilitate the speedy identification of fake news. Having A.I. active behind filter bubbles can help stop the spread of anti-vax and other dangerous fake news posts from being spread.

Other variables are outside our control. Platform policies (PP), Counter Influencer Node (INc), how far the news spreads (N), automated or semi-automated authentication tools linked to increased authentication rate (A), and analysis of the post language based on a dataset (FN-DS).

V. LIMITATIONS
Although every effort has been made to collate all the variables presented in the literature on this subject, this paper did not have the opportunity to conduct meta-analysis on this subject. The paper does not claim to have been able to cover every possible study on this subject. It is possible that some more variables are yet to be identified.

The proposed process to automating the process of fake news identification is based on the variables identified and could be subject to limitations where additional variables are identified. The paper acknowledges that the proposed process could be a steppingstone towards a complete automation process. Such a process will have to be tested in lab conditions as well as real-life conditions. The process of testing this approach will help researchers further refine and polish the process.

VI. CONCLUDING REMARKS
In paper has reviewed a variety of variables identified by researches in the field of understanding the factors that influence fake news. The variables show a significant overlap in views but also concentration on different players. As such, the paper collated all these variables and redistributed them based on the key players. This has helped build a holistic and bigger picture of the environment in which Fake News thrives. The variables identified pinpointed some areas where one can see how different social media platform have attempted to combat fake news and failed. The next stage in this research is to test the eight-step process in a lab environment to assess the impact these can have in improving fake news identification and reducing the propagation of fake news.

REFERENCES


