The Spreading of Misinformation online: 3D Simulation

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

Fadi Safieddine
School of Business and Management
Queen Mary University of London
London, UK
F.Safiedinne@qmul.ac.uk

***Abstract*— Social media is becoming the de-facto platform for the dissemination of information as research suggests more Internet users are using social media as their main source of news. In this model, the spread of unverified information is becoming a common place where some could share misinformation as fact. News sharing on social media lacks the traditional verification methods used by professional media. In previous publications, the authors presented a model that shows the extent of the problem thus suggesting the design of a tool that could assist users to authenticate information using a conceptual approached called 'right-click authenticate' button. A two-dimensional simulation provided bases for a proof-of-concept and identification of key variables. This paper uses Biolayout three-dimensional modelling to expand their simulations of different scenarios. Using the given variables and values, this paper presents a better understanding of how misinformation travels in the spatial space of social media. The findings further confirmed that the approach of 'right-click authenticate' button would dramatically cut back the spread of misinformation online.**

Keywords— Misinformation; Social Media; Cascades; three-dimensional simulation; Biolayout.

I. Introduction

Social media nowadays is attracting millions of users to its various platforms, enabling them to spread information and share their interests across the web easily. Due to the huge amount of unverified information presented as facts, most of what is seen online cannot and could not be trusted. Malicious users who have motives to sway other users' opinions and beliefs tend to be the source of spreading misinformation. Misinformation could be in the form of chain emails, spam, fake news, dotted images, out of context images, out of context videos, misleading news and many more. The spread of this misinformation does not only waste users' time and efforts, but could also be dangerous. Therefore, there have been attempts to find means or tools that would limit the spread of misinformation on social media, hence improving the users' experience in general and bring some credibility to verifying content shared online [1][2]. The approach consists of developing a technique that limits the spread of fake news by allowing users to authenticate it from within their web browsers. If this piece of information was deemed to be unauthentic, then the user will likely stop sharing it with others out of social responsibility, and hence will drastically limit its spread.

II. Literature Review

Online social networks are becoming one of the key sources of information and news especially among younger generations, according to the results of the Oxford Internet Survey [3]. Online applications and social media tools such as Facebook, Twitter, etc. are considered as one of the leading methods of distributing news and user-generated content, which facilitate the creation and exchange of the most up-to-date information. However, sharing inaccurate pieces of information, referred to as misinformation in [4] is widespread in this medium. Misinformation is also defined as "piece of malicious information intentionally made to cause undesirable effects in the general public, such as panic and misunderstanding; or to supplant valuable information" [5]. Moreover, arrangements such as rumours, false messages, and illegal propaganda can be considered a variety of misleading information that the term 'misinformation' is referring to [6]. Having misinformation shared on social media on a daily basis breaches the reliability of those tools and can create misunderstanding among societies on particular cases. Also, the aggregation of people around common interests, worldviews, and narratives is simplified with the wide availability of user-provided content in social media. As stated in [7], misinformation propagation occurs when malicious individuals utilise Social media tools to distribute misinformation.

In [8] researchers report that the increase in social media users has resulted in the increase in misinformation distribution. Social media has become a major tool for the propagation of misinformation since proper filtering techniques similar to reviewing and editing information in traditional publishing is not in place to fulfil the lack in social media users' accountability [9]. Moreover, the majority of social media users may not be attentive to the untruth story as a consequence of sharing huge volumes and diverse forms of information, misinformation, and propaganda in social media.

In [10] Libicki explains that prior beliefs and opinions of people influence their decision in accepting misleading information.

Moreover, in [11] Kumar and Geethakumari discuss that people believe things which support their past judgments without questioning them. False information spreads just like accurate information. However, the role of information context is central. This links with the survey findings by [3] that shows topics on technology, finance, politics and health are the ones that interest the social media users the most and are considered as the key sources of misinformation.

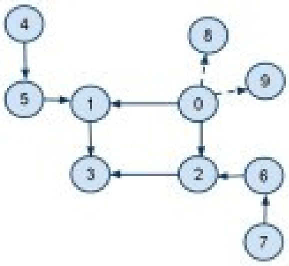

Fig. 1. Misinformation travels in solid lines or blocked in dotted lines. [9]

Looking at social media as a tool for assisting in malicious activities and misbehaviours, it is reported that groups and campaigns having malicious intentions are the driving force for sharing misinformation as well as mimicking widespread information diffusion behaviour [6][11]. As a result, easing the way of distributing misinformation has raised the motivation of users having malicious intentions to spread misinformation, which happens to be greater support to cult-like views in a wide range of topics. One essential aspect in such online environment is to provide practical methods for undertaking detailed analysis in order to prevent such activities or at least to detect and stop them from going further [12][13]. Users, however, are given an excellent opportunity, having lack of accountability and verifiability, to distribute false stories through the medium while not discouraging freedom of expression and freedom of ideas. In [9] researchers presented the first tempt to model travel of information or misinformation online, see Fig.1. In this model, there are multiple starting nodes: 0, 4, and 7, suggesting that misinformation can spread from a variety of sources beyond social media. Misinformation can crisscross and travel in a variety of ways. The paper uses network algorithm to test two competing campaigns as means of testing the accuracy of the information. In such a scenario, Budak in [9] suggested the need for 'influential' people to counter the 'bad' campaign and limit misinformation as a means to fight misinformation. Nowadays, with the enormous volume of information propagation finding a reliable piece of information in social media needs sifting-out different types of misinformation, which is computationally a difficult task [6]. As part of a research project at Colombia University [14], researchers have developed a real-time rumour tracker that looks into the ways in which unverified information and rumour are reported in media. Using their tool, the user is facilitated to view a list of rumours being tracked on their homepage knowing their current state: True, False, and Unverified. Additionally, users can view the page that visualises the sources reporting the rumour, and a breakdown of social shares per source. However, the downside is that it is by no means comprehensive, often not covering many major topics.

A. The Right-click Authenticate Method

For effectively preventing misinformation propagation, it is essential to understand the process of misinformation propagation in social media. In [15], the paper presents an approach based on operative techniques and strategies for controlling misinformation propagation in social media. This would represent an important step is to analyse and predict the dynamic trend of misinformation propagation. Modelling and simulation of involved variables in such ecosystem that describes the process of misinformation propagation can provide an understanding of misinformation propagation precisely and test the efficiency of a control strategy before the actual implementation of the control strategy which in this case is introduced as "Right-click Authenticate" button [15]. The authentication button aims at allowing users to right-click on a piece of news, image, or even video to allow a real-time check on where it has been reported in the past, original metadata that could help identify its source; editorial cited observations and crowd-sourced feedback.

The follow-up to the paper, [16], sets out to demonstrate proof-of-concept using 2D modelling and identified the variables involved in the travel of information, see Fig. 2.

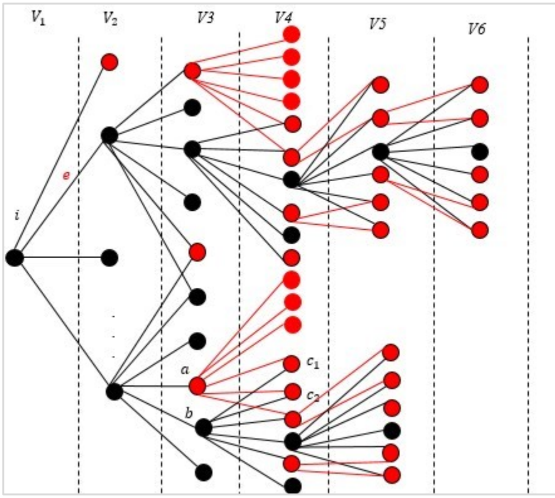

Fig. 2. Passing on rate, and Cross-Wire rate simulation [16]

The paper identified eight key variables and applied theoretical values to demonstrate their applicability. These variables are: i as the first vertex and jn is the last vertex of the given simulation. $V1$ representing the first phase of spread the of misinformation and l representing the maximum possible reach of information through the network. The paper concludes that combating misinformation online is also influenced by the following variables: rate the of authentication A, rate of sharing S, passing on information rate P, average cross-wire rate Cw, success rate of the Same Level communication rate Sl, and Reverse Validation rate Rv. By applying the following values, l = 100, A = 0.3, S = 6, P = 0.2, Cw = 0.2, Sl = 0.2, and Rv = 0.5, the paper demonstrated near elimination of spread of misinformation online whereby the red nodes represented individuals who do not longer believe the misinformation, see Fig. 3. This demonstrated that providing easily accessible tools that would allow users to authenticate images and text, could effectively cascade the process back to the source or at least to the layer immediate to the source.

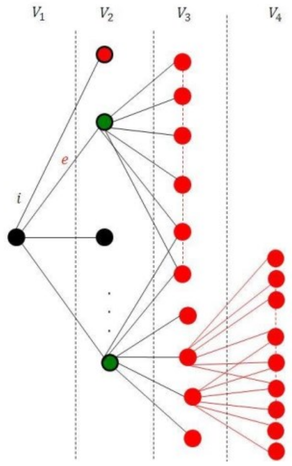

Fig. 3. The outcome of the 2D [16]

While some headway has been achieved, the paper acknowledges that there is still more to be understood in order to develop a representative formula and understand the algorithms required to develop this browser tool. A research limitation identified is related to the fact that two-dimensional simulations did not reflect the method misinformation travels in a spatial space. Hence, as part of the future research direction of the last paper, the paper acknowledges the need for further three-dimensional simulation to be conducted using Biolayout [17] to illustrate better the flow of misinformation in social media and the ways in which it can be minimised and eventually prevented [16].

III. Research Methodology

This paper attempts to answer two research questions:

1. Can the spread of misinformation and the effective use of the "Right-click Authenticate" button be further proven to be effective using three-dimensional simulation?
2. Would the outcomes of a three-dimensional simulation of misinformation and use of the "Right-click Authenticate" button be consistent with outcomes of the two-dimensional simulation?

To answer these questions, this paper applies graph theory in three-dimensional computational simulations with observational research method [18]. Using the variables identified in the literature [16], this paper uses reflective analysis [19] to review progressively different scenarios in the spread of information and misinformation on social media. This approach is comparable to other approaches identified in the literature [20][21][22]. However, this paper is different from previous papers in that it demonstrates this progress in the three-dimension spatial environment. In lab conditions, the team observed the different three-dimensional simulations of information as it travelled from the source to a theoretical maximum reach. These simulations intended to represent the real-world multi-dimensional simulation of information. Biolayout, as a three-dimensional modelling tool, allowed better visualisation of how misinformation can cross-wire and be shared at the same and different levels. The software is an open source tool developed by scientists at Edinburgh University and EMBL-EBI researchers, allowing visualising and analysis of biological networks [17]. Using similar principles of virus infections, and how interaction with infected subjects has a probability of spreading the infection, the team are able to simulate the spread of misinformation in a similar pattern. Successively analysing and observing simulations of scenarios, the paper subsequently evolved the model of simulation to observe the effect on misinformation and success in combating it. With the introduction of new variables, the results show the impact of the new variable on the simulation. One of the main assumptions accepted at the start of this and previous simulations is that the phenomena by which information and misinformation travels can be simulated despite unpredictability generally dominating human behaviour online. This assumption is consistent with other academic publishers in this area of research [16][20][21].

IV. 3D Simulation Results

The paper outlines the steps of the experiment as follows.

1. For a population of 100, sharing rate of 10 and passing rate of 20%, the first simulation is conducted assuming no validation of any sort is done on the misinformation, resulting in having the misinformation reaching the whole population of the experiment.
2. The experiment is run again assuming the best scenario in which one in 100 would take it upon them to validate the information themselves.
3. A series of simulations are run in which the authentication button is assumed to be made accessible. Using random node selection, the simulation is run to consider the impact a 10%, 20%, and 30% of the population have access to the authentication button to validate the misinformation.
4. While assuming 30% of the population uses the authentication button, the next simulation considers the impact of Cross-wire communication between the nodes of 20%.
5. Keeping the variables constant from point 4, the next simulation considers the impact of 'Same Level Communication' rate of 20%.
6. Keeping the variables constant from point 5, the next simulation considers the impact of Reverse Validation rate of 50%.
7. Finally, the paper presents a comparison of the outcomes of the two-dimensional outcome of [16] with the findings of the three-dimensional simulation of this paper. A summary of these variables is presented in Table I.

TABLE I. CRITICAL VARIABLES FOR COMBATING MISINFORMATION ONLINE

Variables	**Notation**
Maximum population	(l)
Sharing	(S)
Passing on information	(P)
Authentication	(A)

Crosswire	(Cw)
Same Level (Cluster) Communication	(Sl)
Reverse Validation	(Rv)

Identified variables have been applied in different percentage to simulate the behaviour of users in network exposed to misinformation spreading. The graph theory is used to model the network and to apply identified variables in this dynamic environment.

In this simulation, this paper considers a weighted directed graph $G = (V, E)$ consisting of V vertices - maximum population of users of the network and edges E which represents the connections between users. (S) is a variable that represents the maximum reach of each user. (P) is a variable that represents the rate of users who read the information and then perform an action of actively disseminate it further. (A) is a variable that represents the rate of users willing to authenticate the information. (Cw) is a variable that represents the probability which users who received different information from different sources will react to validate. (Sl) is a variable that represents the probability that the user who authenticates information and leaves feedback encourages other users from the same level also to authenticate. (Rv) represents the probability that the user who initially believed the misinformation, while being informed by other users through their feedback that the information is not true, either removes the post or rectifies the post. In the first simulation, the paper assumes that there is no authentication. The setups of variables are as follows: l = 100, S = 10 and P = 0.2. The rest of the variables are set to be 0. This scenario is representing spreading of misinformation without any effort to fight it. The result of that behavior or better no behavior at all, shows that misinformation spread reached the maximum population of 100 nodes, and eventually all users have believed the rumor as is shown in Fig. 4, where all nodes are colored in blue. In the second scenario, the simulation demonstrates what would happen if early in the process at least one user decides to check and authenticate the information. The setup of experiment variables are as follows: l = 100, S = 10, P = 20%, A = 1%. The rest of the variables have been setup to be 0. The simulation presented in Fig. 5 shows probabilistic behavior of a network. If the user who authenticates is not a user who shares, then the impact is minimal. Otherwise, if the user who authenticates is a person who shares, then the impact is maximized. In the best scenario where the self-authentication is done early on by someone who shares, 75% of users will continue to be exposed to misinformation. In any other scenario, 99% of users will continue to be exposed to misinformation.

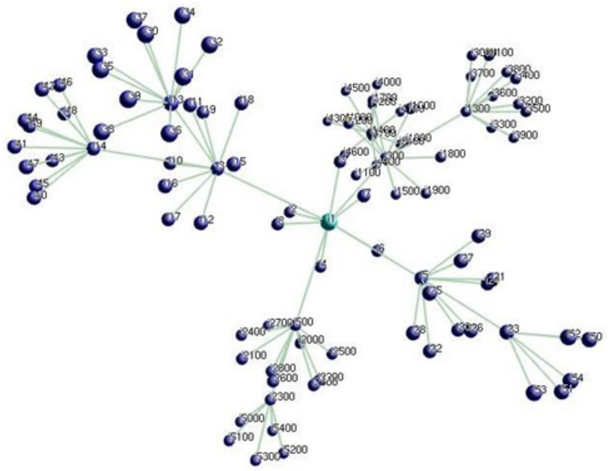

Fig. 4. Simulation 1: *P* = 20% and *S* = 10

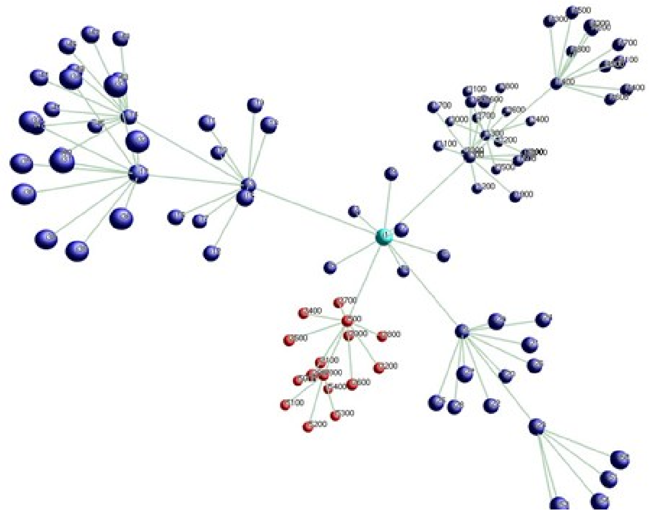

Fig. 5. Simulation 2: *A* = 1% and *S* = 10

In the third run, the simulation starts to consider an authenticate button and the ability to authenticate becomes more accessible. In this scenario, the assumption given is that 30 percent of users, chosen randomly among the population, would authenticate.

Furthermore, the simulation projects in the previous scenario to observe the impact by varying to be 10, 20 and 30 percent; the latter simulations is shown in Fig. 6. Naturally, the simulation shows that the higher percentage of people who are able to authenticate, the fewer misinformation travels. These can be observed by changing the colour of users from blue to red meaning they stop believing in the rumour.

However, the blue nodes at the extremities of the tree in Fig. 6, represent some users at the extremities of the tree who still believe misinformation, which suggests that should the population exceeds 100 then misinformation likely continues to spread.

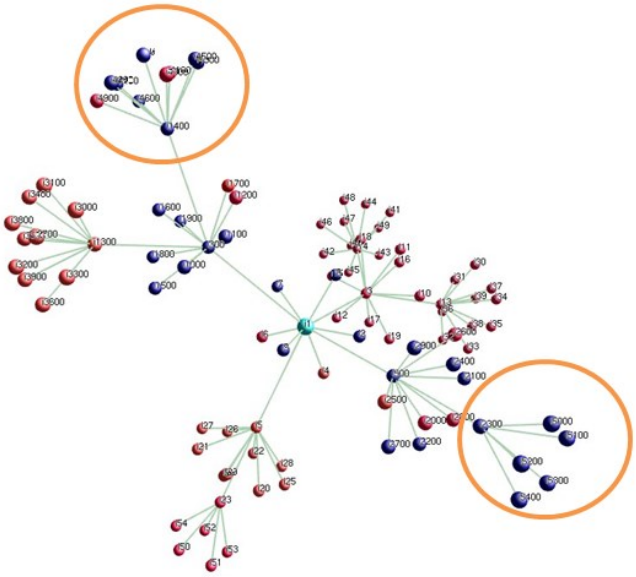

Fig. 6. Simulation 3: A = 30% and S = 10

For the fourth run, the simulation considers Cross-wire (Cw) in that a user will get the information from two sources which may include a source that happens to have validated the misinformation. In this scenario, Cw is set at 20 percent. Again, running the simulations randomly as in previous experiments to see the impact of variable Cw demonstrated the outcome in Fig. 7.

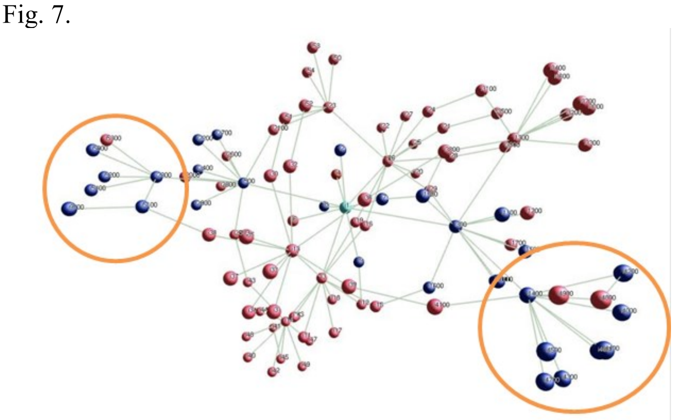

Fig. 7. Simulation 4: Cw = 20%

As evident from what can be seen in Fig. 7, the ability of misinformation to spread has been reduced significantly. However, the simulation showed a way for the rumour to pass through. For the fifth simulation, Same Level communication Sl variable represents users who authenticate information and leave feedback therefore encouraging other users from the same cluster to authenticate. Thus, some users who will see the misinformation and validate it would take it upon themselves to let users read this misinformation and be informed that the picture or article is not true. In this scenario, Sl is set at 20 percent. It is evidence from Fig. 8 that there is near elimination of misinformation and for the first time misinformation is locked in a way that prevents it from expanding further. In a simulation of this nature, it would also suggests that in scenarios of 100+ users, the outcome of such simulations should be the same. Nevertheless, this scenario shows that there were two pockets of misinformation. In one pocket, the left blue node was left as the only user in the cluster who believes this misinformation.

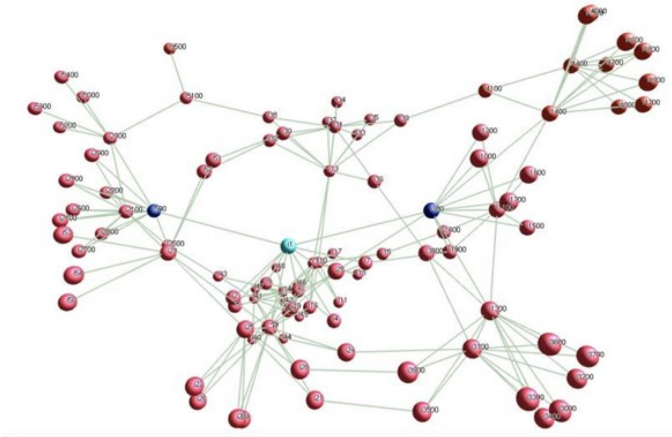

Fig. 8. Simulation 5: A = 30% and Sl = 20%

For the last run, the simulation considers the impact of reverse validation (Rv). Reverse validation is when a sub-source of misinformation either reverses or removes their post after realizing it is a misinformation. This is likely to be the case where all or most of the children of the node have turned red – indicating they do not believe this misinformation.

In this scenario, reverse validation (Rv) is set to take place in 50 percent of the time. The author ran a random simulation and of the last two blue users, one turned green as is shown in Fig. 9.

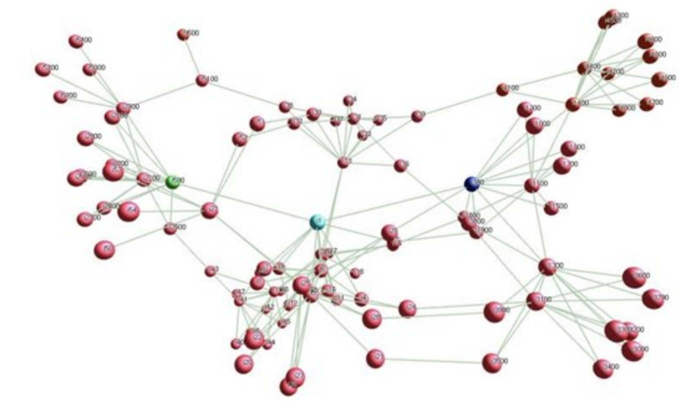

Fig. 9. Simulation 6: Rv = 50%

Simulations further confirmed that the number of users becomes irrelevant as the extremities of the ‘tree’ are eliminated, and that misinformation will be confined to the first source and first line beyond which misinformation will not be able to travel easily.

V. ANALYSIS AND OUTCOMES

The graph analysis of both two dimensional and three-dimensional simulations demonstrated that given the same variables, the outcomes of the simulation would be identical as demonstrated in Fig. 3 and Fig. 10 close up view.

In both simulations and given the same set of variables, misinformation failed to expand beyond the second layer $V2$. In both simulations, misinformation cascaded back to the source, resulting in child nodes as early as $V2$ being informed that this piece of news is not true. In both cases, misinformation could not continue to expand and the combination of the last two variables suggests it significantly halted the expansion.

Finally, both simulations suggest that the size of the population may not be a relevant factor if an accessible authentication tool is provided. Therefore, in answering the research questions set out in this paper:

1. The results show that the spread of misinformation and the effective use of the "right-click authenticate" button is further proven to be effective using three-dimensional simulation.
2. The outcomes of the three-dimensional simulation of misinformation and use of the "right-click authenticate" button are proved to be consistent with outcomes of the two-dimensional simulation.

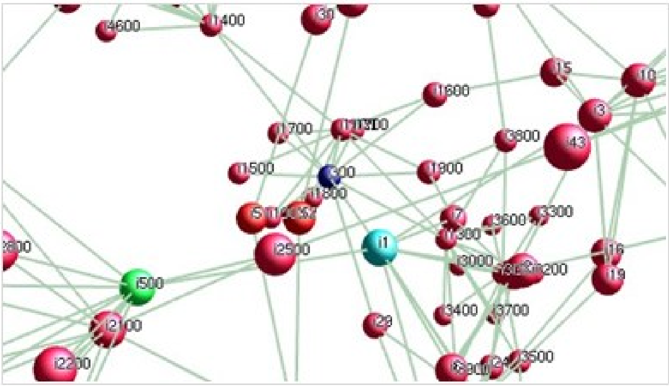

Fig. 10. Final outcomes: Simulation close up.

VI. Limitations

Although the three-dimensional simulations have been successful in visualising how misinformation travels in real life, the paper makes several assumptions regarding the values provided to key variables. The assumptions the paper uses are mainly based on reflective analysis subjective to individual experiences and representing online one speculative scenario. It is worth noting though that this approach is comparable to similar research on modelling the travel of misinformation [20]. Moreover, in addition to conducted studies in [23] [24], this paper acknowledges that further research should be conducted to investigate the effect of more potential variables on the travel of information and means of combating misinformation online. And where possible, more accurate data needs to be collected on the average values associated with the variables identified in their studies.

VII. Concluding remarks

This paper has been able to demonstrate how an authentication method could greatly reduce the spread of misinformation on social media and improve the users' experience. The three-dimensional simulations combined with graph theory have further helped demonstrate the variables governing the way misinformation travels, and how this could be greatly minimised by authenticating information before it is shared. There is potential for this study to be further extended by conducting more simulations, on different scenarios, and by including more variables that could have an effect on misinformation spread such as amplifiers (i.e. news agencies), and their role in combating misinformation spread. Further research, including the development of an algorithmic formula for predicting the spread of misinformation with the aim of programming the first fully functional browser that would be capable of running live authentication.

References

[1] P. Pourghomi, F. Safieddine, W. Masri, and M. Dordevic, "How to stop spread of misinformation on social media: Facebook plans vs. right-click authenticate approach." IEEE Engineering & MIS (ICEMIS), 2017, pp 1-8.

[2] A. A. Halimeh, P. Pourghomi, and F. Safieddine, "The Impact of Facebook's News Fact-Checking on Information Quality (IQ) Shared on Social Media." MIT ICIQ 2017 International Conference on Information Quality, 2017, pp 2-11.

[3] W. H. Dutton, G. Blank, D. and Gorseli, "Cultures of the Internet: The Internet in Britain." Oxford Internet Survey 2013 Report, University of Oxford.

[4] Kumar, KP Krishna, and G. Geethakumari. "Information diffusion model for spread of misinformation in online social networks." in proceedings of the international Conference on Advances in Computing, Communications and Informatics (ICACCI), 2013. IEEE, 2013, pp 1172–1177.

[5] X. Wang, Y. Lin, Y. Zhao, L. Zhang, J. Liang, and Z. Cai, "A novel approach for inhibiting misinformation propagation in human mobile opportunistic networks." Peer-to-Peer Networking and Applications, vol. 10, 2016, pp. 1-18.

[6] N. A. Karlova, and K. E. Fisher, "Plz RT: A social diffusion model of misinformation and disinformation for understanding human information behaviour." Inform Res, vol. 18, 2013, pp. 1-17.

[7] S. Lewandowsky, U. K. Ecker, C. M. Seifert, N. Schwarz, and J. Cook, "Misinformation and its correction: Continued influence and successful debiasing." Psychological Science in the Public Interest, vol. 13, 2012, pp. 106-131.

[8] World Economic Forum Report, "Top 10 trends of 2014: The rapid spread of misinformation online." 2014.

[9] C. Budak, D. Agrawal, and A. El Abbadi, "Limiting the spread of misinformation in social networks." in proceedings of the 20th international conference on World Wide Web, ACM, 2011, pp. 665-674.

[10] MC. Libicki, "Conquest in cyberspace: National security and information warfare." in Cambridge University Press, New York, USA.

[11] K.K. Kumar, and G. Geethakumari, "Detecting misinformation in online social networks using cognitive psychology." Human-centric Computing and Information Sciences, vol. 4, 2014, pp. 1-22.

[12] M.E. Keim, and E. Noji, "Emergent use of social media: a new age of opportunity for disaster resilience." American journal of disaster medicine, vol. 6, 2011, pp.47-54.

[13] W. De Neys, S. Cromheeke, and M. Osman, "Biased but in doubt: Conflict and decision condence." PLoSONE, vol. 6, 2011.

[14] C. Silverman. About Emergent. Retrieved from: http://www.emergent.info/about (Last Accessed on 14 February 2018)

[15] F., Safieddine, W. Masri, and P. Pourghomi, "Corporate responsibility in combating online misinformation," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 7, 2016, pp.126-132.

[16] M. Dordevic, F. Safieddine, W. Masri, and P. Pourghomi, "Combating Misinformation Online: Identification of Variables and Proof-of-Concept Study," in Conference on e-Business, e-Services and e-Society, pp. 442-454, Springer International Publishing, September 2016, pp. 442-454.

[17] D. W. Wright, T. Angus, A.J. Enright, and T.C. Freeman, "Visualisation of BioPAX Networks using BioLayout Express3D", F1000Research 2014.

[18] J. Altmann, "Observational study of behavior: sampling methods.Behaviour," 1974, pp. 227-266.

[19] J. Osmond, and Y. Darlington, "Reflective analysis: Techniques for facilitating reflection." Australian social work, 2015, pp. 3-14.

[20] K. Lee, J. Mahmud, J., Chen, M. Zhou, and J. Nichols, "Who will retweet this? Automatically identifying and engaging strangers on twitter to spread information." in proceedings of the 19th international conference on Intelligent User Interfaces, ACM, 2014, pp. 247-256.
[21] T. A. Hoang, and E. P. Lim, "Virality and Susceptibility in Information Diffusions." In proceedings of the 6th international AAAI conference on weblogs and social media (ICWSM), 2012.
[22] F. Jin, E. Dougherty, P. Saraf, Y. Cao, and N. Ramakrishnan, "Epidemiological modeling of news and rumors on twitter." in proceedings of the 7th Workshop on Social Network Mining and Analysis, ACM, 2013, p.8.
[23] P. Pourghomi, A.A Halimeh, F. Safieddine, and W. Masri, "Right-click Authenticate adoption: The impact of authenticating social media postings on information quality." in proceedings of the IEEE International Conference on Information and Digital Technologies (IDT) , 2017, pp. 1-7.
[24] F. Safieddine, M. Dordevic, and P. Pourghomi, "Spread of misinformation online: Simulation impact of social media newsgroups." in proceedings of the IEEE international Computing conference, 2017, pp. 899 – 906.