

Analyzing Disinformation with the Active Propagation Strategy

Chih-Hung Chen*, YiWei Ma**, Ying Hsun Lai***, Wen-Tsung Chang****, Shun-Ching Yang****

* Department of Computer Science and Information Engineering, National Taiwan Normal University, Taipei, Taiwan

** Department of Electrical Engineering, National Taiwan University of Science and Technology, Taipei, Taiwan

*** Department of Computer Science and Information Engineering, National Taitung University, Taitung, Taiwan

**** Cybersecurity Technology Institute, Institute for Information Industry, Taipei, Taiwan

honzonzone@gmail.com, yiweimaa@gmail.com, yhlai@nttu.edu.tw, wtchang@iii.org.tw,
shunchingyang@iii.org.tw

Abstract— In recent years, disinformation has had an increasingly detrimental effect on society. It is driving a wedge between people, causing a crisis of public trust and social unrest. Malicious spreaders often actively propagate disinformation on different social media, so people are exposed repeatedly to messages that deepen establish false memories. This “illusory truth effect” leads people to believe that the repeated disinformation is truthful. Eventually, people may generate a cognitive bias that makes their thinking more easily by others. This work focuses on identifying various features of information by analyzing the motivation for, purpose of, and methods of achieving the active propagation of false information. Then, behaviors that are associated with active propagation will be summarized to identify its sources. Finally, a framework for detecting actively propagated disinformation will be proposed. This framework can be used for gathering information about, and analyzing, and serving as an aid to decision-making.

Keywords— Disinformation, fake news, active propagation, case observation, information gathering and analysis

I. INTRODUCTION

Disinformation [1] has been a very difficult issue to resolve since ancient times. A creator of disinformation aims to mislead the public to provide commercial, political, or psychological benefits to particular individuals or groups. It differs from “fake news” [2] in that it is not endorsed by third-party media, and so might be expected to have no credibility and only a weak influence on people. However, with the rise of social media, people’s sources of information have shifted from traditional TV news, newspapers and magazines to various social platforms, such as Facebook, Dcard, or PTT. Nowadays, the disinformation is disseminated less by word of mouth, newspapers, and magazines, and more by such simple means as reposting and sharing on social platforms. With the help of social networks, mobile devices, and unlimited data phone plans, the spread of disinformation has become faster and the scope of its influence has increased [3].

Although social platforms have led to the real-time circulation of information, their negative effects have become

evident. Disinformation is emerging in an endless stream whose impact on human beings has been increasing continuously, as when the coronavirus caused the panic-buying of toilet paper [4] and fake news was reported during the 2016 Election [5]. Sometimes, the effect causes actual harm [6]. Over time, it is driving a wedge between people, eroding public trust, and causing social unrest. To fight against malicious propaganda and the dissemination of disinformation on various social platforms, relevant research must be performed. Therefore, this research study events and their communication behaviors on different social platforms to analyze relevant motives, purposes and intentions, and try to find out the key features of dissemination of disinformation.

The rest of this paper is organized as follows. Section II reviews related works on the topics under investigation. Section III analyses the active propagation strategy of disinformation. The proposed framework for early detection and warning of active propagation strategy in disinformation is presented in Section IV. Finally, the conclusions and challenges are summarized in Section V.

II. RELATED WORKS

Most research on the diffusion of disinformation on social media is concerns politics or Covid-19. Lin [6] explores the spread of fake news on different social platforms from the viewpoint of media convergence. Vosoughi *et al.* [7] focus on human emotions to analyze the factors that affect dissemination of disinformation. Ip [8] analyzes the factors that drive the spreading of fake news across platforms and proposes some possible solutions. Fu and Tao [9] explore the dissemination of disinformation on social media by using text analysis based on big data on Internet memes [10], Cheng [11] integrates STS (science and technology studies) with methods in communication research to explore how disinformation is spread on social platforms quickly. Cheng [12] proposes a framework involving multiple approaches to analyze the circulation and dissemination patterns of disinformation on social media. Wu and Liu [13] combine an LSTM-RNN (the Long Short-Term Memory cells into the RNN model) with an

embedding method to classify propagation pathways of a message. Dou *et al.* [14] analyze user preferences for the purposes of detection of disinformation. Shu *et al.* [15] established a fake news database FakeNewsNet to promote research into fake news and this database facilitates potential applications on fake news study on social media.

III. ANALYZING ACTIVE PROPAGATION STRATEGY

The dissemination of disinformation on social platforms has harmed people. But why have social media become a hotbed for disinformation propagation? The problem boils down to a single thing: everyone can create disinformation and disseminate it easily, but fact-checking is difficult and takes a long time. Additionally, sharing messages makes people have a connection with others, so more people care about the emotional connection on social media rather than the authenticity of the message. This is why many people habitually share news without verification. Moreover, when people give a like, upvote, or thumbs-up on social media, they unintentionally create an echo chamber [16] for themselves. Once disinformation is present in someone's echo chamber, he/she will hear it again and again. Subsequently, he/she will only be more likely to encounter disinformation that reflects and reinforces that previously shared. Ultimately, many people come to believe that the disinformation they have encountered is true [17]. This effect is known as the illusory truth effect [18]. And, the echo chamber and the illusory truth effect are tricks that are commonly used in the active propagation strategy for disinformation.

Nowadays, as a result of domestic efforts to combat the dissemination of disinformation, domestic governments, third-party groups and even social media companies are committed to the verification and clarification of information. But they still cannot effectively prevent the dissemination of disinformation. Studies have found that most disinformation is quickly generated and disseminated through social platforms. Creators of disinformation often use the active propagation strategy, as shown in Fig. 1, to push the same message on various social media, such as Facebook, Line, PTT, Dcard, and others. The recipients of this message then share the disinformation on various social media. Their goal is to mislead readers and to believe that the disinformation is true [19].

The active propagation strategy is often accompanied by collaborative propagation on different social media. After disinformation is generated on social platforms, the key to its active propagation lies in cross-platform collaborative communication. To share or retweet a message, there must be recipients who identify with the opinion of the message. In general, people who are in the same echo chamber have a stronger sense of identity. The higher the sense of identity, the greater the power of dissemination [20]. Spreaders share these messages to their own echo chamber, and then the messages are pushed on various social media by members in their echo chamber. In this way, messages are exposed repeatedly, and people may be affected by the illusory truth effect.

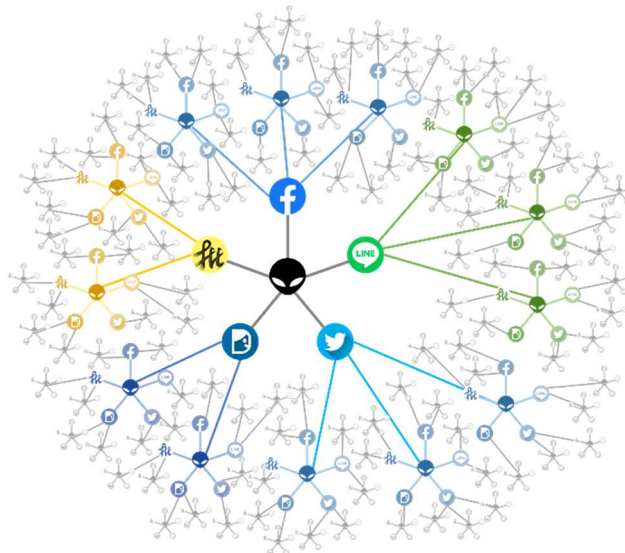


Figure 1. Illustration of active propagation network

IV. FRAMEWORK FOR ACTIVE PROPAGATION STRATEGY

This work uses the case study method to observe behaviors associated with collaborative propagation. Then, fact-checking tools, such as the Taiwan FactCheck Center, Cofacts, MyGoPen, and others, are used to identify the authenticity of the information. If an incident is judged to involve the dissemination of disinformation, we analyze the motivation for, purpose of, and methods of the disinformation. In order to observe fully the modes of dissemination of disinformation, the 5W1H (who, what, when, where, why, and how) method [21] is applied to analyze the responses of other users to the event and subsequent information-disseminating behaviors. The goals are to understand the process of information propagation on social media. The 5W1H are described as follows.

- Who was/were mentioned in the case and who did release this message?
- What issue was mentioned in the case?
- When did this case happen and when did this message start propagating?
- Where did this event happen and on which social media did this message be released?
- Why did this message be created and propagated around?
- How many shares and comments does this message have?

Disinformation can be observed from three aspects: the user accounts of spreaders, the content of messages, and the propagation on social media. And each aspect is discussed as follows.

A. User Accounts of Spreaders

Many studies [22]-[25] have shown that a good way for detecting disinformation is focusing on the user accounts of spreaders. People can detect disinformation by evaluating the credibility of user accounts. Follows are some account characteristics that can provide important clues for assessing suspicious sources of information.

1) User Profile: A user profile is a collection of information associated with a user. It contains the user name, user portrait,

the language used by the account, the locations of the account, the creation time of the account, and so on.

2) User Behavior: The behavior is an important feature of how spreaders interact within groups on social media. It contains how many posts does the account has and how often does the account post, reply, share, and so on.

3) Credibility of User: The credibility is also a good feature for evaluating malicious accounts on social media. It contains how many friends, followers, controversial history does the account has.

B. Content of Messages

The most common method for disinformation detection is based on content analysis [22]-[25]. There are many algorithms that are used for detecting online disinformation. Follows are some content characteristics that can help us to detect potential disinformation.

1) Exaggerated Title: The creators of disinformation usually compose sensational titles to catch people's attention. They aim to attract people to read the disinformation and share it with others.

2) Sentimental Content: The creators of disinformation often incite people's sentiment to change their minds, opinions, or stances on some issues.

3) Authenticity of the Story: To persuade people, the creators of disinformation usually provide knowledge from experts, statistical data, references, and visual representation to frame the story.

C. Propagation on Social Media

The identification of disinformation can not only depend on the user accounts of spreaders and the content of messages, but the propagation patterns on social media are also influential factors [22]-[25]. Follows are some propagation characteristics that can be used to capture patterns of disinformation.

1) Credibility of Sources: The credibility of the creators, publishers, and spreaders of the message sources can also be good indicators for evaluating information. A credible source makes people likely believe that the story is true and will prompt people to share the messages, especially when there are not enough resources available to check the authenticity of the messages.

2) Social Network: People create different echo chambers on social media in terms of backgrounds, interests, topics, stances, and relations. As mentioned before, the creator of disinformation tends to form an echo chamber that makes people keep on sharing the same information.

3) Propagation Pathway: The propagation of disinformation is often accompanied by collaborative propagation on different social media. After disinformation is generated, the creator of disinformation actively releases the message on various social media. The goal is to let people bring the message into their own echo chamber.

This work proposes a framework that combines features from the user accounts of spreaders, the content of messages, and the propagation on social media. Features are utilized to try to track the source of disseminated disinformation. Ultimately, the track of the coordinated dissemination is evaluated for early detection and early warning of active propagation strategy in disinformation. The overall research architecture is shown in Fig. 2.

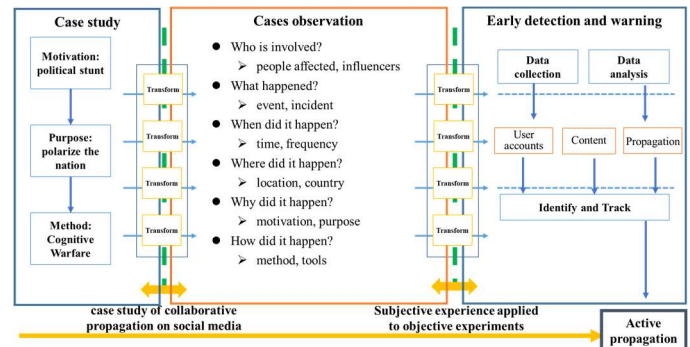


Figure 2. Architecture for early detection and warning of active propagation strategy in disinformation

V. CONCLUSIONS AND CHALLENGES

This work proposes a framework for analyzing disinformation using an active propagation strategy. It investigates the behavior of collaborative propagation on social media based on case observation. We propose a framework for understanding active propagation behaviors that may provide a solution to the problem of disinformation.

Unfortunately, disinformation will always exist if it is very lucrative to generate and use. The survey also highlights some challenges in current research and opportunities that go with these challenges. The challenges around disinformation are including the following.

- Social media are a hotbed for rapid propagation of disinformation because the sharing mechanism allows messages to be spread easily and fact-checking is difficult and slow.
- People are separated by political ideology and build echo chambers. They then tend to seek out information that reinforces their beliefs without exposure to opposing opinions. Ultimately, people develop cognitive biases that can polarize nations.
- People more care about the emotional connection on social media rather than the truth of information. Therefore, disinformation creators often stimulate readers' emotions - especially anger and fear - to motivate them to spread the disinformation further.
- Creators of disinformation receive feedback from fact-checking mechanisms and thus "improve" their content by mixing false and real information, adjusting their writing styles, and revising their semantics, making fact-checking increasingly difficult over time.
- Because the content detection technology has achieved a great performance, the presentation of disinformation has also been reinforced. Messages are presented from texts

to images (memes), video, and even live streaming. It makes disinformation detection become more and more difficult.

- It is becoming more and more difficult to track the source of disseminated disinformation. Because the battlefield has transferred from public communities to private.
- Due to the efforts to combat the dissemination of disinformation, if a message is reported as false on social platforms, it will be warned by signs. People may rely on the warning signs over time and believe those messages that are not marked as wrong.

ACKNOWLEDGMENT

This study is conducted under the “Pilot research and development of disinformation forensics for innovative digital trust services (1/1)” of the Institute for Information Industry which is subsidized by the Ministry of Economic Affairs of the Republic of China.

REFERENCES

- [1] J. H. Fetzer, “Disinformation: The Use of Disinformation,” *Minds and Machines*, vol. 14, pp. 231-240, 2004.
- [2] A. Gelfert, “Fake News: A Definition,” *Informal Logic*, vol. 38, no. 1, pp. 84-117, 2018.
- [3] K. Farhall, A. Carson, S. Wright, A. Gibbons, and W. Lukanto, “Political Elites’ Use of Fake News Discourse Across Communications Platforms,” *International Journal of Communication*, vol. 13, no. 23, 2019.
- [4] S.-Y. Hung, “‘Just Grab the Toilet Papers during Covid-19 Pandemics?’ A Content Analysis of News Coverage on Toilet Paper Craze,” Master’s Thesis, Shih Hsin University, Taipei, Taiwan, 2020.
- [5] H. Allcott and M. Gentzkow, “Social Media and Fake News in the 2016 Election,” *Journal of economic perspectives*, vol. 31, no. 2, pp. 211-36, 2017.
- [6] C.-c. Lin, “Media Convergence of Fake News: An Exploring on Taiwan Election in 2018,” *Mass Communication Research*, vol. 142, no. 1, pp. 111-153, 2020.
- [7] S. Vosoughi, D. Roy, and S. Aral, “The spread of true and false news online,” *Science*, vol. 359, no. 6380, pp. 1146-1151, 2018.
- [8] K.-Y. IP, “The Spread and Solution of Fake News on Social Media—a Case Study of Covid-19,” Master’s Thesis, Shih Hsin University, Taipei, Taiwan, 2021.
- [9] W.-C. Fu and S.-P. Tao, “Analysis of the Misinformation of Internet-Meme Communication Patterns,” *Chinese Journal of Communication Research*, no. 33, pp. 99-135, 2018.
- [10] L. Shifman, “Memes in a digital world: Reconciling with a conceptual troublemaker,” *Journal of Computer-Mediated Communication*, vol. 18, no. 3, pp. 362-377, 2013.
- [11] Y.-C. Cheng, “Exploring the Emerging Logic of Social Media Events: An Approach Integrating STS and Communication Research,” *Chinese Journal of Communication Research*, no. 32, pp. 129-164, 2017.
- [12] Y.-C. Cheng, “Exploring the Operation Modes of Disinformation on Social Media: Two Political Disinformation Cases in Taiwan,” *Chinese Journal of Communication Research*, no. 39, pp. 3-41, 2021.
- [13] L. Wu, and H. Liu, “Tracing Fake-News Footprints: Characterizing Social Media Messages by How They Propagate,” *Proceedings of the Eleventh ACM International Conference on Web Search and Data Mining (WSDM 2018)*, pp. 637-645, Marina Del Rey, CA, USA, February, 2018.
- [14] Y. Dou, K. Shu, C. Xia, P. S. Yu, and L. Sun, “User Preference-aware Fake News Detection,” *Proceedings of the 44th International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR 21)*, Online, July, 2021.
- [15] K. Shu, D. Mahudeswaran, S. Wang, D. Lee, and H. Liu, “FakeNewsNet: A Data Repository with News Content, Social Context and Dynamic Information for Studying Fake News on Social Media,” *Big Data*, vol. 8, no. 3, pp. 171-188, 2020.
- [16] A. E. Marwick, “Why do people share fake news? A sociotechnical model of media effects,” *Georgetown Law Technology Review*, vol. 2, no. 2, pp. 474-512, 2018.
- [17] G. Pennycook, T. D. Cannon, and D. G. Rand, “Prior exposure increases perceived accuracy of fake news,” *Journal of Experimental Psychology: General*, vol. 147, no. 12, pp. 1865-1880, 2018.
- [18] A. Dechêne, C. Stahl, J. Hansen, and M. Wänke, “The Truth About the Truth: A Meta-Analytic Review of the Truth Effect,” *Personality and Social Psychology Review*, vol. 14, no. 2, pp. 238-257, 2010.
- [19] E. J. Newman, M. C. Jalbert, N. Schwarz, and D. P. Ly, “Truthiness, the illusory truth effect, and the role of need for cognition,” *Consciousness and Cognition*, vol. 78, pp. 102866, 2020.
- [20] M. D. Vicario, A. Bessi, F. Zollo, F. Petroni, A. Scala, G. Caldarelli, H. E. Stanley, and W. Quattrociocchi, “The spreading of misinformation online,” *Proceedings of the National Academy of Sciences*, vol. 113, no. 3, pp. 554-559, 2016.
- [21] Y. Ishida and S. Kuraya, “Fake News and its Credibility Evaluation by Dynamic Relational Networks: A Bottom up Approach,” *Procedia Computer Science*, vol. 126, pp. 2228-2237, 2018.
- [22] S. Kumar and N. Shah, “False Information on Web and Social Media: A Survey,” *arxiv*, 2018.
- [23] 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, no. 1, pp. 22-36, 2017.
- [24] X. Zhang and A. A. Ghorbani, “An overview of online fake news: Characterization, detection, and discussion,” *Information Processing & Management*, vol. 57, no. 2, pp. 102025, 2020.
- [25] X. Zhou and R. Zafarani, “A Survey of Fake News: Fundamental Theories, Detection Methods, and Opportunities,” *ACM Computing Surveys*, vol. 53, no. 5, pp. pp. 1-40, 2021.



C.-H. Chen received the PhD degree in computer science and information engineering from National Taiwan Normal University, Taipei, Taiwan in 2021. Now he is a postdoctoral researcher at the Department of Computer Science and Information Engineering, National Taiwan Normal University. His research interests include computer games and artificial intelligence.



Y. Ma is an assistant professor in National Taiwan University of Science and Technology. He received the PhD degree in the Department of Engineering Science at National Cheng Kung University, Tainan, Taiwan. His research interests include internet of things, cloud computing, future network and ubiquitous computing.



Y. H. Lai received the PhD Degree in National Cheng Kung University, Tainan, Taiwan, in 2013. He serves associate professor of the Department of Computer Science and Information Engineering at National Taitung University. His research interests include STEAM education, AIOts applications, and Multicultural education.



W.-T. Chang is currently acting as technology director in CyberSecurity Technology Institute (CSTI) at Institute for Information Industry (III), Taiwan. He received his B.S, M.S, and PhD degrees in Computer Science from National Chiao-Tung University, Taiwan, in 1989, 1991 and 1995, respectively. His research interests are Object-Oriented design and programming, performance evaluation, distributed systems and media processing on wireless and embedded systems.

Currently his major research focuses on Artificial Intelligence, FinTech/Credit Scoring,RPA (Robotic Process Automation),Big Data Analytics,Smart Tourism, IIoT Cybersecurity Analytics, Media Forensics, and leads the teams to develop core data analysis technologies and services on the related application domains.



S.-C. Yang is currently acting as section manager in CyberSecurity Technology Institute(CSTI) at Institute for Information Industry (III). He received his B.S. degree in Computer Science from National Chiao-Tung University, MS. degree in Electrical Engineering from National Taiwan University, in 2004 and 2008. Currently his major research focuses on Influence Operation, Open Source Intelligence, and Fake Accounts Detection on Social Media.