Contagion Source Detection in Epidemic and Infodemic Outbreaks: Mathematical Analysis and Network Algorithms

Other titles in Foundations and Trends® in Networking

Distributed Coding in A Multiple Access Environment
Yanru Tang, Faeze Heydaryan and Jie Luo
ISBN: 978-1-68083-468-0

Age of Information: A New Concept, Metric, and Tool
Antzela Kosta, Nikolaos Pappas and Vangelis Angelakis
ISBN: 978-1-68083-360-7

Network and Protocol Architectures for Future Satellite Systems
Tomaso de Cola, Alberto Ginesi, Giovanni Giambene,
George C. Polyzos, Vasilios A. Siris, Nikos Fotiou and Yiannis Thomas
ISBN: 978-1-68083-334-8

Duality of the Max-Plus and Min-Plus Network Calculus
Jorg Liebeherr
ISBN: 978-1-68083-294-5

Contagion Source Detection in Epidemic and Infodemic Outbreaks: Mathematical Analysis and Network Algorithms

Chee Wei Tan
Nanyang Technological University
cheewei.tan@ntu.edu.sg

Pei-Duo Yu
Chung Yuan Christian University
peiduoyu@cycu.edu.tw

the essence of knowledge
Boston — Delft

Foundations and Trends® in Networking

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

C. W. Tan and P. D. Yu. *Contagion Source Detection in Epidemic and Infodemic Outbreaks: Mathematical Analysis and Network Algorithms*. Foundations and Trends® in Networking, vol. 13, no. 2-3, pp. 106–251, 2023.

ISBN: 978-1-63828-251-8

Foundations and Trends® in Networking
Volume 13, Issue 2-3, 2023

Editorial Scope

Topics

Foundations and Trends® in Networking publishes survey and tutorial articles in the following topics:

- Modeling and Analysis of:
  - Ad Hoc Wireless Networks
  - Sensor Networks
  - Optical Networks
  - Local Area Networks
  - Satellite and Hybrid Networks
  - Cellular Networks
  - Internet and Web Services
- Protocols and Cross-Layer Design
- Network Coding
- Energy-Efficiency Incentives/Pricing/Utility-based
- Games (co-operative or not)
- Security
- Scalability
- Topology
- Control/Graph-theoretic models
- Dynamics and Asymptotic Behavior of Networks

Information for Librarians

Foundations and Trends® in Networking, 2023, Volume 13, 4 issues. ISSN paper version 1554-057X. ISSN online version 1554-0588. Also available as a combined paper and online subscription.

Contents

Contagion Source Detection in Epidemic and Infodemic Outbreaks: Mathematical Analysis and Network Algorithms

Chee Wei Tan[1] and Pei-Duo Yu[2]

[1] *Nanyang Technological University, Singapore; cheewei.tan@ntu.edu.sg*
[2] *Chung Yuan Christian University, Taiwan; peiduoyu@cycu.edu.tw*

ABSTRACT

The rapid spread of infectious diseases and online rumors share similarities in terms of their speed, scale, and patterns of contagion. Although these two phenomena have historically been studied separately, the COVID-19 pandemic has highlighted the devastating consequences that simultaneous crises of epidemics and misinformation can have on the world. Soon after the outbreak of COVID-19, the World Health Organization launched a campaign against the COVID-19 Infodemic, which refers to the dissemination of pandemic-related false information online that causes widespread panic and hinders recovery efforts. Undoubtedly, *nothing spreads faster than fear.*

Networks serve as a crucial platform for viral spreading, as the actions of highly influential users can quickly render others susceptible to the same. The potential for contagion in epidemics and rumors hinges on the initial source, underscoring the need for rapid and efficient digital contact

Chee Wei Tan and Pei-Duo Yu (2023), "Contagion Source Detection in Epidemic and Infodemic Outbreaks: Mathematical Analysis and Network Algorithms", Foundations and Trends® in Networking: Vol. 13, No. 2-3, pp 107–251. DOI: 10.1561/1300000068.

tracing algorithms to identify superspreaders or Patient Zero. Similarly, detecting and removing rumor mongers is essential for preventing the proliferation of harmful information in online social networks. Identifying the source of large-scale contagions requires solving complex optimization problems on expansive graphs. Accurate source identification and understanding the dynamic spreading process requires a comprehensive understanding of surveillance in massive networks, including topological structures and spreading veracity. Ultimately, the efficacy of algorithms for digital contact tracing and rumor source detection relies on this understanding.

This monograph provides an overview of the mathematical theories and computational algorithm design for contagion source detection in large networks. By leveraging network centrality as a tool for statistical inference, we can accurately identify the source of contagions, trace their spread, and predict future trajectories. This approach provides fundamental insights into surveillance capability and asymptotic behavior of contagion spreading in networks. Mathematical theory and computational algorithms are vital to understanding contagion dynamics, improving surveillance capabilities, and developing effective strategies to prevent the spread of infectious diseases and misinformation.

1

Introduction

1.1 Epidemics and Rumors

The spreading of epidemics and rumors on networks share many important features [28], [29], [36], [58]. The underlying network interaction cannot be directly observed and often has to be implicitly inferred from macroscopic phenomenons. Driven by the same human collective crowd behavior, these network dynamics can lead to common network effects like the small-world phenomenon and percolation thresholds. The study of epidemics and rumor spreading is thus an important part of applied probability theory and graph theory related to the analysis of the evolution of large systems arising in networks. Even though the process of spreading information in online social networks differs from that of disease epidemics, the proliferation of fake news and recent disinformation campaigns in online social networks has emerged in recent years as a formidable cybersecurity threat that can have catastrophic real-world consequences like a pandemic [45], [92], [135], [149].

Though epidemics and rumor spreading have been separately studied in the past with a longer history for the stochastic theory of epidemic spreading, the COVID-19 pandemic has been the first of simultaneous global crises in which both the epidemic and overabundance of misinformation devastatingly wreak havoc on the world. The COVID-19 pandemic is the first pandemic in history in which humans rely heavily on the Internet and online social networks to stay connected amidst the prolonged lockdown and social distancing measures in place. It has also spawned an epidemic of online misinformation, undermining the efficacy of online social networks that humans crucially rely on and disrupting public health risk communications. Shortly after the COVID-19 pandemic started, the World Health Organization (WHO) declared war against the COVID-19 Infodemic, which is the viral spreading of pandemic-related misinformation or disinformation in social media [54].

Spreading processes are dynamic cascading phenomena where the action of some users increases the susceptibility of other users to the same; this results in the successive spread of a disease virus or rumor from an initial few users to a much larger set of users [28], [29], [36], [58]. When a new infectious virus spreads, public healthcare authorities want to identify persons who may have come into contact with an infected person and to trace close social contacts in order to stop ongoing transmission or reduce the spread of infection. When rumors like false treatment for the COVID-19 disease spread in online social networks, this can prevent humans from adopting the right behaviors to reduce the COVID-19 pandemic risk. Once misinformation morphed into disinformation attacks, it can be disruptive and deadly. These simultaneous crises require both public healthcare and cyber security experts to work together to fight infodemics by identifying sources of misinformation.

An objective of interests is to unravel the dynamical spreading process to root out the malicious source quickly, accurately, and reliably with only limited observation data of infected nodes in the network. Just like epidemic countermeasures like digital contact tracing and policies to identify *Patient Zero* in an outbreak,[1] building resilience to catastrophic viral misinformation is of huge importance to a safe and functioning cyberspace because of the highly-connected online social networks.

[1]Contact tracing apps based on the Bluetooth wireless radio standard are arguably one of the defining technologies for surveillance during the COVID-19 pandemic [65], [91].

To accurately detect or predict the causation of contagion in large networks, it is crucial to identify the superspreaders and the origin of disease viruses. Similarly, it is essential to determine who is spreading rumors and disinformation to cause division and influence decisions among users. This raises questions about the provenance of such information [92], [100], [150]. Additionally, the implications of network surveillance and the response to contain a contagion must be considered. With the emergence of new communication platforms, new avenues for spreading misinformation and disinformation arise. Identifying the source of contagion can have far-reaching consequences, such as timely responses to the next pandemic or promoting a safe cyberspace.

Numerous fundamental questions remain unanswered in the statistical inference of infection sources in networks. The theory of stochastic processes over large networks is still evolving, and the computational aspects of estimation and detection in networks have not yet been systematically examined, with source identification understood only in the simplest graph topology cases. It is remarkable that even though human social interaction or online social networks are not designed with the intention of spreading a payload (such as an infectious disease virus or rumor) as rapidly as possible, the process of viral spreading over large networks is not fully comprehended [92], [100], [150]. Are there specific network structures, quantifiable measures of user influence that promote viral spreading? If so, what particular features could aid in the development of better digital contact tracing strategies or interventions to counter the spread of malicious rumors?

As we strive to comprehend the spread of contagions across large networks, it is crucial to recognize the potential for cross-pollination of ideas between different types of networks, each with distinct interaction graph structures, initial nodes, and nature of user interactions [28], [29], [36], [58]. For instance, in [6], researchers proposed intervention strategies based on a generative model of viral misinformation spread using infectious disease spreading dynamics. Moreover, when network topology abstraction is sufficiently random, it may provide insights into network phenomena based on percolation theory, as noted in [38].

1.2 Propagated Epidemics and Contact Tracing

Tracing the origins of propagated epidemics can be traced back to the investigation of the 1854 London cholera epidemics by John Snow (1813–1858), who is widely recognized as a pioneer of modern epidemiology [5], [49], [50]. His work in tracking the source of the cholera outbreak was a significant breakthrough in epidemiological research. By creating detailed dot distribution maps of household deaths due to cholera, Snow was able to identify the source of the epidemic - a water pump located in Broad Street, Golden Square. Snow's methodical tracing effort was one of the earliest applications of inferential statistics to the study of epidemics [5], [49], [50]. Additionally, his heroic intervention in persuading the parish's vestrymen to remove the water pump symbolizes one of the earliest examples of public health action. It is important to note that Snow's contribution to epidemiology was not only a significant scientific achievement but also a landmark event in the history of public health. The removal of the water pump resulted in the rapid cessation of the cholera epidemic, saving countless lives and laying the foundation for modern epidemiological research.

Nowadays, epidemiologists agree that it is necessary to employ contact tracing to stop an infectious disease from spreading: Once a person has been diagnosed as infected, public health authorities fan out to trace the recent contacts of this person for the purpose of monitoring or quarantine. This process repeats if one of those contacts exhibits symptoms until all the contacts who have been exposed are out of circulation. Contact tracing can be effective in the early stage of an epidemic. However, the COVID-19 pandemic had revealed severe deficiencies in public health protection due to asymptomatic infections. Prior study [22] shows that asymptomatic infections need to be considered in analyzing the spread of the disease. The COVID-19 disease is highly contagious, wide-ranging with long incubation periods and transmissible within 6 feet. Its speed and scale of infection had overwhelmed most contact tracing capabilities which are labor-intensive, cost-inefficient and very slow [45], [86]. A new public health innovation, *digital contact tracing*, then came to the scene. Digital contact tracing leverages a plethora of mobile apps to contact trace people and to provide exposure notifications [8], [17], [46], [65], [82], [91], [94], [95].

Current contact tracing practices focus primarily on finding recent contacts of index cases, while overlooking the source of origin. In fact, source inference is an important factor that explains the initial success of backward contact tracing adopted by countries like Japan and Australia in the early days of the COVID-19 pandemic [12], [17], [86], showing that, whenever there is a sudden outbreak, tracing transmission events rather than infectious individuals can efficiently and effectively prevent infection waves.

There are several challenging unsolved problems in digital contact tracing [17], [81], [91], [139]. First, what is the fundamental relationship between infectiousness and the agility of contact tracing? Can contact tracing be faster than the spreading of an infectious disease? Second, how to quadruple the speed of contact tracing? Can backward contact tracing complement forward contact tracing to find Patient Zero or the superspreaders accurately? Third, can we design disease surveillance networks so as to provide timely prediction and early warning capability to automate digital contact tracing upon the arrival of future epidemics?

1.3 Disinformation and Rumor Source Detection

Online social networks like Twitter, Facebook, and YouTube are critical online platforms for spreading news and the diffusion of all kinds of information. They can however cause misinformation and disinformation to spread faster and more rampantly than the traditional "word-of-mouth" mechanism [3], [15], [52], [62], [92], [96], [98], [110], [135], [149], [159]. In fact, false news spreads faster than the truth in a Twitter network [150]. Misinformation is inaccurate or unreliable information that is spread regardless of an intent to mislead. On the other hand, disinformation is intentionally-fabricated misinformation (e.g., hoax news) that is spread with the intent to influence people to make certain decisions or to further an agenda. A malicious rumor monger can now "infect" people across geographical regions on a massive scale faster than ever before. Online rumors, misinformation, and disinformation can thus disrupt livelihood and have serious real-world repercussions.

Recent examples are political mobilization messages spreading in social media that sparked off waves of demonstrations and protests in the Middle East (dubbed the "Arab Spring" or the Twitter revolution) in 2010-2012. In 2013, a bogus Tweet that the White House was attacked went viral after it was sent out by the Associated Press Twitter account that was hacked [11]. This incident momentarily crashed the stock market, demonstrating how online disinformation can cause flash crash and allowing computer hackers to profiteer in the process. A similarly severe incident happened in 2020 when computer hackers seized control of dozens of Twitter accounts belonging to high-profile users like Barack Obama and Elon Musk to tweet out a "double your bitcoin" scam, which went viral quickly. Eventually, this cryptocurrency scam led to a theft of bitcoins worth more than US $110,000 before all the scam messages were removed. Such Internet frauds and cybersecurity threats will be more widespread, especially when bots are recruited to sow discord to amplify the spread of disinformation.

Nations worldwide now recognize that the spread of misinformation and disinformation is an imminent cybersecurity threat that should be seriously addressed by law enforcement agencies [130]. However, the distinction between harmless misinformation and disinformation is often blurred. Moreover, rapid advances in deepfake technologies can make hoax news look legitimate and further exacerbate the situation. Rooting out rumor mongers and dispelling disinformation of increased scale and impact will be part of a timely and practical defense strategy that can offer intellectually deep insight to the science of networks.

What can cause the viral spreading of rumors or disinformation? One factor is semantics [52], [101]. For example, hoaxes and prank threats such as bomb threats are considered more serious but are likely short-lived as they can be quickly debunked. On the other hand, some rumors might swirl longer in social media (e.g., workplace rumors like layoffs or the inefficacy of certain pandemic measures) [52], [101], [126], [147]. Another factor is the principle of homophily in which humans have a tendency to associate with similar others, leading to cognitive bias typically known as the "echo chamber" effect [56], [62], [159]. The element of surprise can also affect rumor viscosity as people will tend to spread the information.

1.4 Overview of the Monograph

This monograph provides an overview of the surveillance of contagion sources in networks that find applications in digital contact tracing and rumor source detection to combat epidemics and infodemics, respectively. Given data that embeds both network topological structure (e.g., knowing who is connected to whom) and relational patterns on how a disease virus or rumor propagates, the objective is to answer the fundamental question: *how to unravel stochastic spreading processes in the network to find the initial outbreak source quickly, accurately and reliably with high confidence by exploiting the topological and statistical properties of networks.*

The contagion source detection problem was first studied in the seminal work [131]–[133]. Mathematically, the problem is: Given a snapshot observation of the contagion graph (showing how "infected" users are connected), who is the contagion source of the spreading? This problem is formulated as a maximum likelihood estimation problem over graphs and then solved exactly for special cases of degree-regular trees with infinite underlying graphs using a new form of network centrality called rumor centrality. Since then, it has spawned a huge literature on contagion source detection with various extensions such as random trees in [37], [53], to multiple sources in [69], [70], [105], [106], [108], [109], [112], [144], [167], to probabilistic sampling in [77], [120] and detection with multiple observations in [35], [153], belief propagation [40], general graphs with irregularity [154], [155], [165] and the implication of probabilistic spreading models and different graph topological features on solving the contagion source detection problem [4], [40], [84], [103], [114], [127], [137], [155], [168].

Different types of network centrality defined on vertices can resolve different types of network problems. Rumor centrality [132] is designed to solve the contagion source detection problem on infinite-size regular tree networks optimally (cf. Section 3.2). The vertex with the maximum rumor centrality is called the rumor center of a tree graph, and the rumor center was proved to be the same as the distance center [131], and the graph centroid of the tree [142], [163], [164]. Furthermore, it was shown in [72], [73], [85] that the graph centroid is almost surely central in the limit of the random growth process of infection on an underlying infinite regular graph. Aside from the distance centrality, another distance-based centrality, the Jordan center, was proposed to solve the contagion source detection in different scenarios [111], [112]. Dynamic influence due to stochastic spreading and opinion dynamics in online social networks can be characterized by the harmonic influence centrality in [1], [148] and the Shapley centrality in [21]. The protection centrality in [2] and relative centrality in [18] measure how important a set of vertices in a network is with respect to other vertices at the gatekeeper level and community level respectively. Querying this contagion source in a large graph with cost constraints and query complexity has been analyzed in [25], [93], [127]. Centrality measures related to the eigenvectors of the network topology are also important in the study of stochastic processes over large graphs [31], [57], [76], [124].

The bibliography included in this monograph seeks to encompass as many contributions as possible, aiming to provide a balanced overview of the key results and methodologies. Although the monograph may not be a perfect summary of the state-of-the-art (see related surveys in [71], [160] before 2018), it aims to serve as an imperfect yet informative summary, providing a rough illustration of the existing literature in the last 15 years and with relevance to the COVID-19 pandemic and infodemic. We survey the various work in this field with a particular focus on the intricate interplay between contagion source detection and mathematical tools like graph theory, probability theory, combinatorics, and algorithm design for statistical inference in the context of large networks.

This monograph provides a comprehensive overview of contagion source detection problem along with a problem-solving approach called "*network centrality as statistical inference*" that expounds a systematic approach to analyze inferential statistical problems in networks with applications to digital contact tracing and rumor source detection. The framework presented in this work establishes a connection between network centrality and the solution of challenging optimization problems that involve complex combinatorial constraints arising from the interaction of a stochastic process with the underlying network. By leveraging an appropriate network centrality, which induces a metric on each graph node, it is possible to obtain compact measures that quantify the importance of nodes and accurately capture the optimality of stochastic optimization. This framework also enables the utilization of graph algorithm techniques to address these problems effectively [59], [145].

We will discuss how the "*network centrality as statistical inference*" approach can be useful to the graph algorithm design that comes with performance guarantees, computational complexity, detection accuracy, and to address the "big data" regime in which the contagion graph can be very large (as is the case in the COVID-19 pandemic and infodemic). Designing scalable algorithms that uncover the contagion source accurately by leveraging network science and mathematical tools will be important to prevent future pandemics (e.g., 'Disease X' pandemic and infodemic) given the enhanced human connectivity on a global scale. We will conclude with open issues and several promising research directions to address the challenges of surveillance of spreading in networks.

References

[1] D. Acemoglu, G. Como, F. Fagnani, and A. Ozdaglar, "Opinion fluctuations and disagreement in social networks," *Mathematics of Operations Research*, vol. 38, no. 1, 2013, pp. 1–27.

[2] D. Acemoglu, A. Malekian, and A. Ozdaglar, "Network security and contagion," *Journal of Economic Theory*, vol. 166, 2016, pp. 536–585.

[3] E. Adar and L. A. Adamic, "Tracking information epidemics in blogspace," in *Proceedings of IEEE/WIC/ACM International Conference on Web Intelligence*, ser. WI '05, pp. 207–214, Washington, DC, USA: IEEE Computer Society, 2005. DOI: 10.1109/WI.2005.151.

[4] R. Alexandru and P. L. Dragotti, "Rumour source detection in social networks using partial observations," in *Proceedings of IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pp. 730–734, 2018. DOI: 10.1109/GlobalSIP.2018.8646695.

[5] N. T. J. Bailey, *The Mathematical Theory of Infectious Diseases and its Applications*, Second. Griffin, 1975.

[6] J. Bak-Coleman, I. Kennedy, and M. Wack, "Combining interventions to reduce the spread of viral misinformation," *Nature Human Behavior*, vol. 6, 2022, pp. 1372–1380. URL: https://doi.org/10.1038/s41562-022-01388-6.

[7] J. Balogh and G. Pete, "Random disease on the square grid," *Random Structures and Algorithms*, vol. 13, no. 3–4, 1998, pp. 409–422.

[8] Y. Bengio, P. Gupta, T. Maharaj, N. Rahaman, M. Weiss, and et al, "Predicting infectiousness for proactive contact tracing," in *Proc. of Int. Conf. on Learning Representations*, 2021.

[9] F. Bergeron, P. Flajolet, and B. Salvy, "Varieties of increasing trees," in *CAAP '92*, J. .-. Raoult, Ed., pp. 24–48, Berlin, Heidelberg: Springer Berlin Heidelberg, 1992.

[10] S. Bikhchandani, D. Hirshleifer, and I. Welch, "A theory of fads, fashion, custom, and cultural change as informational cascades," *Journal of Political Economy*, vol. 100, no. 5, 1992, pp. 992–1026.

[11] Bloomberg Businessweek, *A Fake AP Tweet Sinks the Dow for an Instant*, 2013. URL: https://www.bloomberg.com/news/articles/2013-04-23/a-fake-ap-tweet-sinks-the-dow-for-an-instant.

[12] W. J. Bradshaw, E. C. Alley, J. H. Huggins, A. L. Lloyd, and K. M. Esvelt, "Bidirectional contact tracing could dramatically improve COVID-19 control," *Nature Communications*, vol. 12, no. 1, 2021, pp. 1–9.

[13] U. Brandes, "A faster algorithm for betweenness centrality," *Journal of Mathematical Sociology*, vol. 25, no. 2, 2001, pp. 163–177.

[14] G. Brightwell and P. Winkler, "Counting linear extensions," *Order*, vol. 8, no. 3, 1991, pp. 225–242. DOI: 10.1007/BF00383444.

[15] P. E. Brown and J. Feng, "Measuring user influence on Twitter using modified K-shell decomposition," in *Proceedings of AAAI Conference on Artificial Intelligence*, 2011.

[16] S. Bubeck, L. Devroye, and G. Lugosi, "Finding Adam in random growing trees," *Random Struct. Alg.*, vol. 50, 2017, pp. 158–172.

[17] G. Cencetti, G. Santin, A. Longa, E. Pigani, A. Barrat, C. Cattuto, S. Lehmann, M. Salathe, and B. Lepri, "Digital proximity tracing on empirical contact networks for pandemic control," *Nature Communications*, vol. 12, no. 1, 2021, pp. 1–12.

[18] C. S. Chang, C. J. Chang, W. T. Hsieh, and D. S. Lee, "Relative centrality and local community detection," *Network Science*, vol. 3, no. 4, 2015, pp. 445–479.

[19] C. Chen, H. Tong, B. A. Prakash, C. E. Tsourakakis, T. Eliassi-Rad, C. Faloutsos, and D. H. Chau, “Node immunization on large graphs: Theory and algorithms,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 28, no. 1, 2016, pp. 113–126.

[20] S. Chen, P. D. Yu, C. W. Tan, and H. V. Poor, “Identifying the superspreader in proactive backward contact tracing by deep learning,” in *Proceedings of the 52nd Annual Conference on Information Sciences and Systems (CISS)*, 2022. DOI: 10.1109/CISS53076.2022.9751196.

[21] W. Chen, S.-H. Teng, and H. Zhang, “A graph-theoretical basis of stochastic-cascading network influence: Characterizations of influence-based centrality,” *Theoretical Computer Science*, vol. 824-825, 2020, pp. 92–111.

[22] Y.-C. Chen, P.-E. Lu, C.-S. Chang, and T.-H. Liu, “A time-dependent SIR model for COVID-19 with undetectable infected persons,” *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 4, 2020, pp. 3279–3294. DOI: 10.1109/TNSE.2020.3024723.

[23] Y.-D. Chen, H.-C. Chen, and C.-C. King, “Social network analysis for contact tracing,” *Infectious Disease Informatics and Biosurveillance*, vol. 27, 2010, pp. 339–358. DOI: 10.1007/978-1-4419-6892-0_15.

[24] Z. Chen, K. Zhu, and L. Ying, “Detecting multiple information sources in networks under the SIR model,” *IEEE Transactions on Network Science and Engineering*, vol. 3, no. 1, 2016, pp. 17–31. DOI: 10.1109/TNSE.2016.2523804.

[25] J. Choi, S. Moon, J. Woo, K. Son, J. Shin, and Y. Yi, “Information source finding in networks: Querying with budgets,” *IEEE/ACM Transactions on Networking*, vol. 28, no. 5, 2020, pp. 2271–2284.

[26] F. Chung, P. Horn, and A. Tsiatas, “Distributing antidote using pagerank vectors,” *Internet Mathematics*, vol. 6, no. 2, 2009, pp. 237–254.

[27] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms 3th ed.* Cambridge, Massachusetts London, England: The MIT Press, 2009.

[28] D. J. Daley and D. G. Kendall, "Epidemics and rumours," *Nature*, vol. 204, no. 1118, 1964.

[29] D. J. Daley and D. G. Kendall, "Stochastic rumours," *IMA Journal of Applied Mathematics*, vol. 1, no. 1, 1965, pp. 42–55.

[30] Q. E. Dawkins, T. Li, and H. Xu, "Diffusion source identification on networks with statistical confidence," in *Proceedings of the 38th International Conference on Machine Learning (ICML)*, vol. 139, pp. 2500–2509, PMLR, 2021.

[31] J.-C. Delvenne and A.-S. Libert, "Centrality measures and thermodynamic formalism for complex networks," *Physical Review E*, vol. 83, no. 4, 2011, p. 046 117. DOI: 10.1103/PhysRevE.83.046117.

[32] N. Demiris and P. D. O'Neill, "Bayesian inference for epidemics with two levels of mixing," *Scandinavian Journal of Statistics*, vol. 32, no. 2, 2005, pp. 265–280. URL: http://www.jstor.org/stable/4616877.

[33] D. Domenico, G. Manlio, C. Granell, M. Porter, and A. Arenas, "The physics of spreading processes in multilayer networks," *Nature Physics*, vol. 12, 2016, pp. 901–906.

[34] M. D. Domenico, A. Lima, P. Mougel, and M. Musolesi, "The anatomy of a scientific rumor," *Scientific Reports*, vol. 3, no. 2980, 2013. DOI: 10.1038/srep02980.

[35] W. Dong, W. Zhang, and C. W. Tan, "Rooting out the rumor culprit from suspects," in *Proceedings of IEEE International Symposium on Information Theory*, pp. 2671–2675, 2013.

[36] M. Draief and L. Massoulié, *Epidemics and Rumors in Complex Networks*, First. Cambridge University Press, 2009.

[37] K. Durant and S. Wagner, "On the centroid of increasing trees," *Discrete Mathematics and Theoretical Computer Science*, vol. 21, no. 4, 2019.

[38] R. Durrett, "Some features of the spread of epidemics and information on a random graph," *The Proceedings of the National Academy of Sciences*, vol. 107, no. 10, 2010, pp. 4491–4498.

[39] H. E. Egilmez, E. Pavez, and A. Ortega, "Graph learning from filtered signals: Graph system and diffusion kernel identification," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 5, no. 2, 2019, pp. 360–374. DOI: 10.1109/TSIPN.2018.2872157.

[40] T. Fan and I. Wang, "Rumor source detection: A probabilistic perspective," in *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 4159–4163, 2018.

[41] G. Fanti, P. Kairouz, S. Oh, K. Ramchandran, and P. Viswanath, "Spy vs. spy: Rumor source obfuscation," in *Proceedings of ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems*, pp. 271–284, Portland, Oregon, USA: ACM, 2015. DOI: 10.1145/2745844.2745866.

[42] G. Fanti, P. Kairouz, S. Oh, K. Ramchandran, and P. Viswanath, "Metadata-conscious anonymous messaging," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 2, no. 4, 2016, pp. 582–594. DOI: 10.1109/TSIPN.2016.2605761.

[43] G. Fanti, P. Kairouz, S. Oh, K. Ramchandran, and P. Viswanath, "Rumor source obfuscation on irregular trees," in *Proceedings of ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Science*, pp. 153–164, New York, NY, USA: ACM, 2016. DOI: 10.1145/2896377.2901471.

[44] G. Fanti, P. Kairouz, S. Oh, K. Ramchandran, and P. Viswanath, "Hiding the rumor source," *IEEE Transactions on Information Theory*, vol. 63, no. 10, 2017, pp. 6679–6713. DOI: 10.1109/TIT.2017.2696960.

[45] Z. Fei, Y. Ryeznik, A. Sverdlov, C. W. Tan, and W. K. Wong, "An overview of healthcare data analytics with applications to the COVID-19 pandemic," *IEEE Transactions on Big Data*, vol. 8, no. 6, 2022, pp. 1463–1480.

[46] L. Ferretti, C. Wymant, M. Kendall, and et al, "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing," *Science*, vol. 368, no. 6491, 2020, pp. 316–329. DOI: 10.1126/science.abb6936.

[47] V. Fioriti and M. Chinnici, "Predicting the sources of an outbreak with a spectral technique," *Applied Mathematical Sciences*, vol. 8, no. 135, 2014.

[48] P. Flajolet and R. Sedgewick, *Analytic Combinatorics*. Cambridge University Press, 2009.

[49] D. A. Freedman, *Statistical Models: Theory and Practice*, 2nd. Cambridge, UK: Cambridge University Press, 2009.

[50] D. A. Freedman, *Statistical Models and Causal Inference: A Dialogue with the Social Sciences*, 1st. Cambridge, UK: Cambridge University Press, 2011.

[51] L. C. Freeman, "Centrality in social networks conceptual clarification," *Social Networks*, vol. 1, 1978-1979, pp. 215–239.

[52] A. Friggeri, L. A. Adamic, D. Eckles, and J. Cheng, "Rumor cascades," in *Proceedings of 8th International AAAI Conference on Weblogs and Social Media*, 2014.

[53] M. Fuchs and P. D. Yu, "Rumor source detection for rumor spreading on random increasing trees," *Electronic Communications in Probability*, vol. 20, no. 2, 2015.

[54] R. Gallotti, F. Valle, N. Castaldo, P. Sacco, and M. D. Domenico, "Assessing the risks of 'infodemics' in response to COVID-19 epidemics," *Nature Human Behaviour*, vol. 4, 2020, pp. 1285–1293.

[55] A. Ganesh, L. Massoulie, and D. Towsley, "The effect of network topology on the spread of epidemics," in *Proceedings of IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies.*, vol. 2, 1455–1466 vol. 2, 2005. DOI: 10.1109/INFCOM.2005.1498374.

[56] K. Garimella, G. G. F. Morales, A. Gionis, and M. Mathioudakis, "Political discourse on social media: Echo chambers, gatekeepers, and the price of bipartisanship," in *Proceedings of the World Wide Web Conference*, pp. 913–922, Lyon, France: International World Wide Web Conferences Steering Committee, 2018. DOI: 10.1145/3178876.3186139.

[57] D. F. Gleich, "Pagerank beyond the web," *SIAM Review*, vol. 57, no. 3, 2015, pp. 321–363.

[58] W. Goffman and V. A. Newill, "Generalization of epidemic theory: An application to the transmission of ideas," *Nature*, vol. 204, 1964, pp. 225–228.

[59] A. Goldenberg, A. X. Zheng, S. E. Fienberg, and E. M. Airoldi, "A survey of statistical network models," *Foundations and Trends in Machine Learning*, vol. 2, no. 2, 2010, pp. 129–233.

[60] A. J. Goldman, "Optimal center location in simple networks," *Transportation Science*, vol. 5, no. 2, 1971, pp. 212–221.

[61] M. Gomez-Rodriguez, J. Leskovec, and A. Krause, "Inferring networks of diffusion and influence," *ACM Trans. Knowl. Discov. Data*, vol. 5, no. 4, 2012, 21:1–21:37. DOI: 10.1145/2086737.2086741.

[62] N. Grinberg, K. Joseph, L. Friedland, B. Swire-Thompson, and D. Lazer, "Fake news on Twitter during the 2016 US presidential election," *Science*, vol. 363, no. 6425, 2019, pp. 374–378.

[63] Z. Guo, M. Schlichtkrull, and A. Vlachos, "A Survey on Automated Fact-Checking," *Transactions of the Association for Computational Linguistics*, vol. 10, 2022, pp. 178–206. DOI: 10.1162/tacl_a_00454.

[64] A. A. Hagberg, D. A. Schult, and P. J. Swart, "Exploring network structure, dynamics, and function using networkx," in *Proc. of the 7th Python in Science Conference*, pp. 11–15, 2008.

[65] C. N. Hang, Y. Z. Tsai, P. D. Yu, J. Chen, and C. W. Tan, "Privacy-enhancing digital contact tracing with machine learning for pandemic response: A comprehensive review," *Big Data and Cognitive Computing, Special issue on digital health and data analytics in public health, accepted and to appear*, 2023.

[66] C. N. Hang, P. D. Yu, S. Chen, C. W. Tan, and G. Chen, "Machine learning-enhanced graph analytics for infodemic risk management," *IEEE Journal of Biomedical and Health Informatics*, Preprint, Accepted with minor revision, 2023.

[67] W. Hu, W. P. Tay, A. Harilal, and G. Xiao, "Network infection source identification under the SIRI model," in *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 1712–1716, 2015.

[68] F. Ji, W. Tang, and W. P. Tay, "On the properties of gromov matrices and their applications in network inference," *IEEE Transactions on Signal Processing*, vol. 67, no. 10, 2019, pp. 2624–2638.

[69] F. Ji and W. P. Tay, "An algorithmic framework for estimating rumor sources with different start times," *IEEE Transactions on Signal Processing*, vol. 65, no. 10, 2017, pp. 2517–2530.

[70] F. Ji, W. P. Tay, and L. R. Varshney, "Estimating the number of infection sources in a tree," in *Proceedings of IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pp. 380–384, 2016. DOI: 10.1109/GlobalSIP.2016.7905868.

[71] J. Jiang, S. Wen, S. Yu, Y. Xiang, and W. Zhou, "Identifying propagation sources in networks: State-of-the-art and comparative studies," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, 2017, pp. 465–481.

[72] V. Jog and P. Loh, "Analysis of centrality in sublinear preferential attachment trees via the Crump-Mode-Jagers branching process," *IEEE Transactions on Network Science and Engineering*, vol. 4, no. 1, 2017, pp. 1–12. DOI: 10.1109/TNSE.2016.2622923.

[73] V. Jog and P. Loh, "Persistence of centrality in random growing trees," *Random Structures & Algorithms*, vol. 52, no. 1, 2018, pp. 136–157.

[74] N. L. Johnson and S. Kotz, *Urn models and their application: An approach to modern discrete probability theory*. Wiley, 1977.

[75] A. Kalvit, V. S. Borkar, and N. Karamchandani, "Stochastic approximation algorithms for rumor source inference on graphs," *Performance Evaluation*, vol. 132, 2019, pp. 1–20.

[76] U. Kang, S. Papadimitriou, J. Sun, and H. Tong, "Centralities in large networks: Algorithms and observations," in *Proceedings of the 2011 SIAM international conference on data mining*, pp. 119–130, 2011.

[77] N. Karamchandani and M. Franceschetti, "Rumor source detection under probabilistic sampling," in *Proceedings of IEEE International Symposium on Information Theory*, pp. 2184–2188, 2013.

[78] N. D. Kazarinoff, *Geometric Inequalities*. American Mathematical Society, 1975.

[79] D. Kempe, J. Kleinberg, and E. Tardos, "Maximizing the spread of influence through a social network," *Proc. ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2003, pp. 137–146.

[80] D. Kempe, J. Kleinberg, and E. Tardos, "Influential nodes in a diffusion model for social networks," in *Proceedings of the International Colloquium on Automata, Languages, and Programming (ICALP)*, pp. 1127–1138, 2005.

[81] J. T. Kemper, "On the identification of superspreaders for infectious disease," *Mathematical Biosciences*, vol. 48, no. 1-2, 1980, pp. 111–127.

[82] L. Kennedy-Shaffer, M. Baym, and W. P. Hanage, "Perfect as the enemy of good: Tracing transmission with low-sensitivity tests to mitigate SARS-CoV-2 outbreaks," *Lancet Microbe*, vol. 2, 2021, pp. 219–224.

[83] W. O. Kermack and A. G. McKendrick, "A contribution to the mathematical theory of epidemics," *Proc. R. Soc. Lond. A*, vol. 115, no. 772, 1972, pp. 700–721. DOI: 10.1098/rspa.1927.0118.

[84] H. Kesavareddigari, S. Spencer, A. Eryilmaz, and R. Srikant, "Identification and asymptotic localization of rumor sources using the method of types," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 3, 2019, pp. 1145–1157. DOI: 10.1109/TNSE.2019.2911275.

[85] J. Khim and P. Loh, "Confidence sets for the source of a diffusion in regular trees," *IEEE Trans. Network Science and Engineering*, vol. 4, no. 1, 2017, pp. 27–40.

[86] S. Kojaku, L. Hébert-Dufresne, E. Mones, S. Lehmann, and Y.-Y. Ahn, "The effectiveness of backward contact tracing in networks," *Nature Physics*, vol. 17, no. 5, 2021, pp. 652–658.

[87] D. Koller and N. Friedman, *Probabilistic Graphical Models: Principles and Techniques*. Cambridge, MA: The MIT Press, 2009.

[88] F. Krzakala, "Belief propagation for the (physicist) layman," Lecture Notes, 2011.

[89] A. Kumar, V. S. Borkar, and N. Karamchandani, "Temporally agnostic rumor-source detection," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 3, no. 2, 2017, pp. 316–329.

[90] J. Kunegis, "KONECT – The Koblenz Network Collection," in *Proc. Int. Conf. on World Wide Web Companion*, pp. 1343–1350, 2013.

[91] S. Landau, *People Count: Contact-Tracing Apps and Public Health*. MIT Press, 2021.

[92] D. M. J. Lazer, M. A. Baum, Y. Benkler, A. J. Berinsky, K. M. Greenhill, F. Menczer, M. J. Metzger, B. Nyhan, G. Pennycook, J. L. Zittrain, and et al, "The science of fake news," *Science*, vol. 359, no. 6380, 2018, pp. 1094–1096. DOI: 10.1126/science.aao2998.

[93] V. Lecomte, G. Ódor, and P. Thiran, "The power of adaptivity in source identification with time queries on the path," *Theoretical Computer Science*, vol. 911, 2022, pp. 92–123. DOI: 10.1016/j.tcs.2021.09.034.

[94] D. Leith and S. Farrell, "A measurement-based study of the privacy of Europe's COVID-19 contact tracing apps," in *Proceedings of IEEE International Conference on Computer Communications*, 2021.

[95] D. J. Leith and S. Farrell, "Coronavirus contact tracing: Evaluating the potential of using bluetooth received signal strength for proximity detection," *ACM SIGCOMM Computer Communication Review*, vol. 50, no. 4, 2020, pp. 66–74.

[96] K. Lerman and R. Ghosh, "Information contagion: Empirical study of the spread of news on Digg and Twitter social networks," in *Proceedings of 4th International AAAI Conference on Weblogs and Social Media*, 2010.

[97] J. Leskovec and A. Krevl, *SNAP Datasets: Stanford large network dataset collection*, 2014. URL: http://snap.stanford.edu/data.

[98] J. Leskovec, M. McGlohon, C. Faloutsos, N. Glance, and M. Hurst, "Patterns of cascading behavior in large blog graphs," in *Proceedings of SIAM International Conference on Data Mining*, pp. 551–556, 2007. DOI: 10.1137/1.9781611972771.60.

[99] Y. Lim, A. Ozdaglar, and A. Teytelboym, "Competitive rumor spread in social networks," *SIGMETRICS Perform. Eval. Rev.*, vol. 44, no. 3, 2017, pp. 7–14. DOI: 10.1145/3040230.3040233.

[100] S. van der Linden, "Misinformation: Susceptibility, spread, and interventions to immunize the public," *Nature Medicine*, vol. 28, 2022, pp. 460–467.

[101] X. Liu, A. Nourbakhsh, Q. Li, R. Fang, and S. Shah, "Real-time rumor debunking on Twitter," in *Proceedings of the 24th ACM International on Conference on Information and Knowledge Management*, ser. CIKM '15, pp. 1867–1870, Melbourne, Australia, 2015. DOI: 10.1145/2806416.2806651.

[102] A. Y. Lokhov, M. Mézard, H. Ohta, and L. Zdeborová, "Inferring the origin of an epidemic with a dynamic message-passing algorithm," *Phys. Rev. E*, vol. 90, 1 2014.

[103] A. Louni and K. P. Subbalakshmi, "Who spread that rumor: Finding the source of information in large online social networks with probabilistically varying internode relationship strengths," *IEEE Transactions on Computational Social Systems*, vol. 5, no. 2, 2018, pp. 335–343.

[104] L. Lovász, "Random walks on graphs: A survey," *Combinatorics*, vol. 2, 1993, pp. 1–46.

[105] W. Luo and W. P. Tay, "Identifying infection sources in large tree networks," in *Proceedings of the 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, pp. 281–289, 2012. DOI: 10.1109/SECON.2012.6275788.

[106] W. Luo and W. P. Tay, "Estimating infection sources in a network with incomplete observations," in *Proceedings of IEEE Global Conference on Signal and Information Processing*, pp. 301–304, 2013.

[107] W. Luo and W. P. Tay, "Finding an infection source under the SIS model," in *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 2930–2934, 2013.

[108] W. Luo, W. P. Tay, and M. Leng, "Identifying infection sources and regions in large networks," *IEEE Trans. Signal Processing*, vol. 61, no. 11, 2013, pp. 2850–2865.

[109] W. Luo, W. P. Tay, and M. Leng, "How to identify an infection source with limited observations," *IEEE Journal of Selected Topics in Signal Processing*, vol. 8, no. 4, 2014, pp. 586–597. DOI: 10.1109/JSTSP.2014.2315533.

[110] W. Luo, W. P. Tay, and M. Leng, "Rumor spreading maximization and source identification in a social network," in *Proceedings of IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, pp. 186–193, 2015.

[111] W. Luo, W. P. Tay, and M. Leng, "Infection spreading and source identification: A hide and seek game," *IEEE Transactions on Signal Processing*, vol. 64, no. 16, 2016, pp. 4228–4243.

[112] W. Luo, W. P. Tay, M. Leng, and M. K. Guevara, "On the universality of the Jordan center for estimating the rumor source in a social network," in *Proceedings of IEEE International Conference on Digital Signal Processing (DSP)*, pp. 760–764, 2015.

[113] D. J. C. Mackay, *Information Theory, Inference and Learning Algorithms*, First. Cambridge University Press, 2003.

[114] T. Matsuta and T. Uyematsu, "Probability distributions of the distance between the rumor source and its estimation on regular trees," in *Proceedings of the 37th Symposium on Information Theory and its Applications (ISTIA)*, pp. 605–610, 2014.

[115] N. Megiddo, "An $O(nlog_2n)$ algorithm for the kth longest path in a tree with applications to location problems," *SIAM Journal on Computing*, vol. 10, no. 2, 1979, pp. 328–337.

[116] E. Meirom, C. Milling, C. Caramanis, S. Mannor, A. Orda, and S. Shakkottai, "Localized epidemic detection in networks with overwhelming noise," *ACM SIGMETRICS Performance Evaluation Review*, vol. 43, 2014. DOI: 10.1145/2796314.2745883.

[117] E. A. Meirom, C. Caramanis, S. Mannor, A. Orda, and S. Shakkottai, "Detecting cascades from weak signatures," *IEEE Transactions on Network Science and Engineering*, vol. 5, no. 4, 2018, pp. 313–325. DOI: 10.1109/TNSE.2017.2764444.

[118] M. Meister and J. Kleinberg, "Optimizing the order of actions in a model of contact tracing," *The Proceedings of the National Academy of Sciences (PNAS) Nexus*, vol. 2, no. 3, 2023.

[119] C. Milling, C. Caramanis, S. Mannor, and S. Shakkottai, "Network forensics: Random infection vs spreading epidemic," *ACM SIGMETRICS Performance Evaluation Review*, vol. 40, no. 1, 2012, pp. 223–234. DOI: 10.1145/2318857.2254784.

[120] S. Negahban, S. Oh, and D. Shah, "Rank centrality: Ranking from pairwise comparisons," *Operations Research*, vol. 65, no. 1, 2016.

[121] M. E. J. Newman, "The spread of epidemic disease on networks," *Physical Review E*, vol. 66, 2002, p. 016 128.

[122] P. D. O'Neill, "A tutorial introduction to Bayesian inference for stochastic epidemic models using Markov chain Monte Carlo methods," *Mathematical Biosciences*, vol. 180, no. 1, 2002, pp. 103–114. DOI: https://doi.org/10.1016/S0025-5564(02)00109-8.

[123] A. Ortega, P. Frossard, J. Kovacevic, J. M. F. Moura, and P. Vandergheynst, "Graph signal processing: Overview, challenges, and applications," *Proceedings of the IEEE*, vol. 106, no. 5, 2018, pp. 808–828. DOI: 10.1109/JPROC.2018.2820126.

[124] L. Page, S. Brin, R. Motwani, and T. Winograd, *The pagerank citation ranking: Bringing order to the web*, 1998.

[125] R. Pastor-Satorras and A. Vespignani, "Immunization of complex networks," *Physical Review E*, vol. 65, 2002.

[126] B. Pittel, "On spreading a rumor," *SIAM J. Appl. Math.*, vol. 47, no. 1, 1987, pp. 213–223. DOI: 10.1137/0147013.

[127] B. A. Prakash, J. Vreeken, and C. Faloutsos, "Efficiently spotting the starting points of an epidemic in a large graph," *Knowledge and Information Systems*, vol. 38, no. 1, 2014, pp. 35–39.

[128] V. M. Preciado, M.Zargham, C. Enyioha, A. Jadbabaie, and G. J. Pappas, "Optimal resource allocation for network protection against spreading processes," *IEEE Trans. Control of Network Systems*, vol. 1, no. 1, 2014, pp. 99–108.

[129] M. Z. Rácz and J. Richey, "Rumor source detection with multiple observations under adaptive diffusions," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 1, 2021, pp. 2–12. DOI: 10.1109/TNSE.2020.3022621.

[130] R. Richardson and C. Director, "CSI computer crime and security survey," *Computer Security Institute*, vol. 1, 2008, pp. 1–30.

[131] D. Shah and T. Zaman, "Detecting sources of computer viruses in networks: Theory and experiment," *Proc. of ACM SIGMETRICS*, 2010.

[132] D. Shah and T. Zaman, "Rumors in a network: Whos's the culprit?" *IEEE Transactions on Information Theory*, vol. 57, 2011, pp. 5163–5181.

[133] D. Shah and T. Zaman, "Rumor centrality: A universal source detector," *Proc. of ACM SIGMETRICS*, 2012.

[134] Singapore Ministry of Health, "News highlights in March and April 2021," 2021. URL: https://www.moh.gov.sg/news-highlights/details/23-more-cases-discharged-120-new-cases-of-covid-19-infection-confirmed.

[135] S. T. Smith, E. K. Kao, E. D. Mackin, D. C. Shah, O. Simek, and D. B. Rubin, "Automatic detection of influential actors in disinformation networks," *The Proceedings of the National Academy of Sciences*, vol. 118, no. 4, 2021, pp. 1–10.

[136] S. T. Smith, E. K. Kao, K. D. Senne, G. Bernstein, and S. Philips, "Bayesian discovery of threat networks," *IEEE Transactions on Signal Processing*, vol. 62, no. 20, 2014, pp. 5324–5338.

[137] S. Spencer and R. Srikant, "Maximum likelihood rumor source detection in a star network," in *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 2199–2203, 2016. DOI: 10.1109/ICASSP.2016.7472067.

[138] A. Sridhar and H. V. Poor, "Quickest inference of network cascades with noisy information," *IEEE Transactions on Information Theory*, vol. 69, no. 4, 2023, pp. 2494–2522.

[139] R. A. Stein, "Super-spreaders in infectious diseases," *International Journal of Infectious Diseases*, vol. 15, no. 8, 2011, e510–e513.

[140] G. Streftaris and G. J. Gibson, "Statistical inference for stochastic epidemic models," in *Proceedings of International Workshop on Statistical Modelling*, pp. 609–616, 2002.

[141] Taiwan Centers for Disease Control, "Press releases from February 2021 to May 2021," 2021. URL: https://www.cdc.gov.tw/En/Bulletin/Detail/PbMrcxQ2bO7H2cdN2_JUEw?typeid=158.

[142] C. W. Tan, P. Yu, C. Lai, W. Zhang, and H. Fu, "Optimal detection of influential spreaders in online social networks," in *Proceedings of the Conference on Information Science and Systems (CISS)*, pp. 145–150, 2016. DOI: 10.1109/CISS.2016.7460492.

[143] C. W. Tan, P. D. Yu, S. Chen, and H. V. Poor, "DeepTrace: Learning to optimize contact tracing in epidemic networks with graph neural networks," *CoRR*, vol. abs/2211.00880, 2022. URL: https://arxiv.org/abs/2211.00880.

[144] W. Tang, F. Ji, and W. P. Tay, "Estimating infection sources in networks using partial timestamps," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 12, 2018, pp. 3035–3049. DOI: 10.1109/TIFS.2018.2837655.

[145] S.-H. Teng, "Scalable algorithms for data and network analysis," *Foundations and Trends in Computer Science*, vol. 12, no. 1-2, 2016, pp. 1–274.

[146] T. Uno and H. Satoh, "An efficient algorithm for enumerating chordless cycles and chordless paths," *Proceedings of the International Conference on Discovery Science*, 2014, pp. 313–324.

[147] P. Van Mieghem, J. Omic, and R. Kooij, "Virus spread in networks," *IEEE/ACM Transactions on Networking*, vol. 17, no. 1, 2009, pp. 1–14. DOI: 10.1109/TNET.2008.925623.

[148] L. Vassio, F. Fagnani, P. Frasca, and A. Ozdaglar, "Message passing optimization of harmonic influence centrality," *IEEE Trans. Control of Network Systems*, vol. 1, no. 1, 2014, pp. 109–120.

[149] M. D. Vicario, A. Bessib, F. Zollo, and et al, "The spreading of misinformation online," *The Proceedings of the National Academy of Sciences*, vol. 113, no. 3, 2016, pp. 554–559.

[150] S. Vosoughi, D. Roy, and S. Aral, "The spread of true and false news online," in *Science*, ser. Vol. 359, Issue 6380, pp. 1146–1151, American Association for the Advancement of Science, 2018. DOI: 10.1126/science.aap9559.

[151] C. Wan, W. Chen, and Y. Wang, "Scalable influence maximization for independent cascade model in large-scale social networks," *Data Mining and Knowledge Discovery*, vol. 25, 2012, pp. 545–576.

[152] B. Wang, G. Chen, L. Fu, L. Song, and X. Wang, "DRIMUX: Dynamic rumor influence minimization with user experience in social networks," *IEEE Transactions on Knowledge and Data Engineering*, vol. 29, no. 10, 2017, pp. 2168–2181.

[153] Z. Wang, W. Dong, W. Zhang, and C. W. Tan, "Rumor source detection with multiple observations: Fundamental limits and algorithms," in *Proceedings of ACM International Conference on Measurement and Modeling of Computer Systems*, pp. 1–13, Austin, Texas, USA: ACM, 2014. DOI: 10.1145/2591971.2591993.

[154] Z. Wang, W. Dong, W. Zhang, and C. W. Tan, "Rooting out rumor sources in online social networks: The value of diversity from multiple observations," *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, no. 4, 2015, pp. 663–677.

[155] Z. Wang, W. Zhang, and C. W. Tan, "On inferring rumor source for SIS model under multiple observations," in *Proceedings of the IEEE International Conference on Digital Signal Processing (DSP)*, pp. 755–759, 2015.

[156] J. Waring, C. Lindvall, and R. Umeton, "Automated machine learning: Review of the state-of-the-art and opportunities for healthcare," *Artificial Intelligence in Medicine*, vol. 104:101822, 2020.

[157] K. Wasa, Y. Kaneta, T. Uno, and H. Arimura, "Constant time enumeration of bounded-size subtrees in trees and its application," *Proc. International Computing and Combinatorics Conference*, 2012.

[158] D. B. West, *Introduction to Graph Theory*. Englewood Cliffs, New Jersey: Prentice Hall, 1996.

[159] F. M. F. Wong, C. W. Tan, S. Sen, and M. Chiang, "Quantifying political leaning from tweets, retweets and retweeters," *IEEE Transactions on Knowledge and Data Engineering*, vol. 28, no. 8, 2016, pp. 2158–2172.

[160] L. Ying and K. Zhu, *Diffusion Source Localization in Large Networks*, ser. Synthesis Lectures on Communication Networks. Morgan & Claypool Publishers, 2018.

[161] P. D. Yu, C. W. Tan, and H. Fu, "Rumor source detection in finite graphs with boundary effects by message-passing algorithms," in *Proceedings of IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, pp. 86–90, Sydney, Australia: ACM, 2017. DOI: 10.1145/3110025.3110028.

[162] P. D. Yu, C. W. Tan, and H. Fu, "Rumor source detection in unicyclic graphs," in *Proceedings of IEEE Information Theory Workshop (ITW)*, pp. 439–443, 2017. DOI: 10.1109/ITW.2017.8277993.

[163] P. D. Yu, C. W. Tan, and H. Fu, "Averting cascading failures in networked infrastructures: Poset-constrained graph algorithms," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 4, 2018, pp. 733–748. DOI: 10.1109/JSTSP.2018.2844813.

[164] P. D. Yu, C. W. Tan, and H. Fu, "Graph algorithms for preventing cascading failures in networks," in *Proceedings of the 52nd Annual Conference on Information Sciences and Systems (CISS)*, pp. 1–6, 2018. DOI: 10.1109/CISS.2018.8362273.

[165] P. D. Yu, C. W. Tan, and H. Fu, "Epidemic source detection in contact tracing networks: Epidemic centrality in graphs and message-passing algorithms.," *IEEE Journal of Selected Topics in Signal Processing*, vol. 16, no. 2, 2022, pp. 234–249. DOI: 10.1109/JSTSP.2022.3153168.

[166] T. Zaman, "Information extraction with network centralities: Finding rumor sources, measuring influence, and learning community structure," *Ph.D. Thesis, Massachusetts Institute of Technology*, 2011.

[167] Z. Zhang, W. Xu, W. Wu, and D. Du, "A novel approach for detecting multiple rumor sources in networks with partial observations," *Journal of Combinatorial Optimization*, vol. 33, no. 1, 2017, pp. 132–146.

[168] L. Zheng and C. W. Tan, "A probabilistic characterization of the rumor graph boundary in rumor source detection," in *Proceedings of IEEE International Conference on Digital Signal Processing (DSP)*, pp. 765–769, 2015.

[169] K. Zhu and L. Ying, "Information source detection in networks: Possibility and impossibility results," in *Proceedings of The 35th Annual IEEE International Conference on Computer Communications (INFOCOM)*, pp. 1–9, 2016.

[170] K. Zhu and L. Ying, "Information source detection in the SIR model: A sample-path-based approach," *IEEE/ACM Trans. Networking*, vol. 24, no. 1, 2016, pp. 408–421.