Quality Engineering

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/lqen20

Broader impacts of network monitoring: Its role in government, industry, technology, and beyond

Nathaniel T. Stevens, James D. Wilson, Anne R. Driscoll, Ian McCulloh, George Michailidis, Cecile Paris, Kamran Paynabar, Marcus B. Perry, Mostafa Reisi-Gahrooei, Srijan Sengupta & Ross Sparks

To cite this article: Nathaniel T. Stevens, James D. Wilson, Anne R. Driscoll, Ian McCulloh, George Michailidis, Cecile Paris, Kamran Paynabar, Marcus B. Perry, Mostafa Reisi-Gahrooei, Srijan Sengupta & Ross Sparks (2021) Broader impacts of network monitoring: Its role in government, industry, technology, and beyond, Quality Engineering, 33:4, 749-757, DOI: 10.1080/08982112.2021.1974036

To link to this article: https://doi.org/10.1080/08982112.2021.1974036

Published online: 14 Oct 2021.

QUALITY ENGINEERING
2021, VOL. 33, NO. 4, 749–757
https://doi.org/10.1080/08982112.2021.1974036

Taylor & Francis
Taylor & Francis Group

THE PAST, PRESENT, AND FUTURE OF NETWORK MONITORING: A PANEL DISCUSSION

Broader impacts of network monitoring: Its role in government, industry, technology, and beyond

Nathaniel T. Stevens[a*], James D. Wilson[b*], Anne R. Driscoll[c**], Ian McCulloh[d,e**], George Michailidis[f**], Cecile Paris[g**], Kamran Paynabar[h**], Marcus B. Perry[i**], Mostafa Reisi-Gahrooei[f**], Srijan Sengupta[j**], and Ross Sparks[g**]

[a]University of Waterloo, Waterloo, Ontario, Canada; [b]University of Pittsburgh, Pittsburgh, Pennsylvania, USA; [c]Virginia Polytechnic Institute and State University, Blacksburg, Virginia; [d]Accenture Federal Services, Washington, District of Columbia; [e]Johns Hopkins University, Baltimore, Maryland; [f]University of Florida, Gainesville, Florida; [g]CSIRO, Sydney, NSW, Australia; [h]Georgia Institute of Technology, Atlanta, Georgia; [i]University of Alabama, Tuscaloosa, Alabama; [j]North Carolina State University, Raleigh, North Carolina

ABSTRACT

The study and use of network monitoring methodology is informed by its need in government, industry, and technology. Here, the panelists discuss the broader impacts of network monitoring in these sectors, how the use and development of new methods is influenced by these institutions, and what challenges need to be addressed in the next 5 to 10 years. There is a strong consensus that these sectors each play an important role in the innovation of network monitoring techniques. Applications to cyber security, transportation, infectious disease monitoring, engineering, and artificial intelligence are discussed.

KEYWORDS

graphs; network monitoring; network science; statistical process monitoring; surveillance

Question

Researchers, particularly those in quality engineering, are often inspired by real-world problems that occur in industry. How do you see industry helping spur innovative research in network monitoring? On the other hand, what role does network monitoring play in the challenges and broader field of quality engineering?

Reisi and Paynabar

A wide variety of industry sectors including manufacturing, construction, and transportation have shifted toward designing interconnected systems with physical and cyber components (Agostinelli et al. 2021; Gokhale et al. 2010). For example, in transportation, roads constitute a physical layer that are connected through a cyber layer for information transmission. Although such a shift created opportunities for designing smarter and more efficient systems, it simultaneously introduced a significant vulnerability due to the interconnected nature of these systems. One major challenge is that a fault or a cyberattack can be propagated to other regions of the networked system and cause harm beyond what would have been traditionally imaginable (Li et al. 2021). Therefore, traditional techniques in SPM for systems monitoring and root-cause analysis that do not consider the inter-connectedness of a system may fall short in addressing these new challenges.

Network monitoring research should be advanced by establishing techniques appropriate for detection and localization of the faults caused in such complex interconnected systems. Such advancement requires collaboration with industry experts to leverage their domain knowledge and incorporate it in data-driven modeling for developing more effective network monitoring methods. On the other hand, the advancement in the knowledge base of network monitoring allows industry to design more complex systems to achieve higher efficiencies. For example, with access to a complex detection framework that can quickly localize faults and attacks, a networked mechanism to optimally control and adjust traffic lights at the intersections can be designed without the concern of possible

CONTACT Nathaniel T. Stevens nstevens@uwaterloo.ca University of Waterloo, Waterloo, Ontario, Canada; James D. Wilson wilsonj41@upmc.edu University of Pittsburgh, Pittsburgh, Pennsylvania, USA.
*Discussion Editors.
**Discussion Panelists.

faults that may propagate and generate transportation disruptions.

Perry

In my view, it is extremely important for researchers in statistical network monitoring to collaborate with practitioners working in today's industry. Such collaborative efforts can lead to new or improved problem definitions and a thorough problem understanding. The increased connectivity and interactions between systems, humans and machines in Industry 4.0 is likely to spur a plethora of research opportunities for the modern statistical process monitoring (SPM) researcher. For example, given the rise of cyber-attacks in manufacturing (e.g., see Elhabashy, Wells, and Camelio 2020; Elhabashy et al. 2021), the need for sophisticated statistical network monitoring schemes to detect and deter cyber-physical attacks on Industry 4.0 systems and processes seems ever increasing. I believe the role of statistical network monitoring in the future could be sizable if the nature and structure of the connections between vertices in a network are of interest. For example, one can distinguish between statistical network monitoring and the monitoring of, e.g., a sensor network. That is, in the former, one is typically interested in monitoring the interaction or pattern frequency between network vertices, e.g., see Sparks (2015); Perry (2020), while the latter aims to detect changes in the measurements observed at the vertices. Consequently, monitoring a sensor network is more in line with what quality engineers typically refer to as multivariate statistical process monitoring. The key point here is that statistical network monitoring is often concerned with monitoring the connections or interactions between vertices, and not necessarily the measurements taken at the vertices themselves.

McCulloh

The rise of big data and the increase in artificial intelligence (AI) consulting has marked a significant change in industry. Big data and AI create greater complexity and with it network dependence. As industry leaders explore how to integrate new machines with humans in hybrid processes, more and more network applications emerge. These industrial changes create new problems for academics to explore. Quality engineering must keep pace with changes in industry. As manufacturing processes and industries are increasingly replaced by information related industries such as cloud computing, data-driven consulting, and advanced robotics, quality engineers must discover how to ensure quality and efficiency for these new applications. Rather than modeling how widgets move through a manufacturing process, they may need to model how data moves through an enterprise IT architecture. Due to the ease of replicating data compared to a single physical entity, network dependence is more common and provides a powerful analytic frame. Not only must quality engineers discover new ways to support big data, statistical network monitoring becomes even more useful.

Michailidis

Complex engineered systems filling a specific function can give rise to novel problems in network monitoring. However, these systems obey either physical laws or engineering design principles and hence both the underlying network topologies and flows may exhibit special characteristics. For example, power transmission networks usually have mesh topologies for enhanced reliability, whereas their distribution relies on radial topologies due to cost benefits. Similarly, electricity flows on power networks obey specific physical laws (Ohm's, Kirchhoff's) and hence the data produced come with certain characteristics. Hence, a monitoring problem for power networks has additional structure that needs to be incorporated in its formulation and can be communicated and explained by industry domain experts. Analogous examples arise for many other types of networks related to engineered systems, but also from other physical or biological systems (e.g., protein interaction or metabolic networks).

In the other direction, novel network monitoring strategies and change point detection algorithms can inform industry researchers of computational and technical advances that would enable them to address larger scale problems in their domain, or existing problems more efficiently. Network monitoring, like all other science and engineering problems, requires a two way communication process between practitioners and methods developers to address its numerous novel challenges.

Driscoll

While working at Virginia Tech, I had the pleasure of serving as the chair of our Corporate Partners program. This program is a cooperative outreach venture

to solidify the mutually beneficial ties that have been built by the Virginia Tech Department of Statistics with industry, business, and government over the past 50 years. The program has been very successful in matching undergraduate students and graduate students with internships and full-time employment. The relationships that we have created with the companies have in many cases resulted from alumni returning to recruit from their alma mater.

Another objective of the program is to strengthen the relationships between faculty and company representatives. We encourage sharing of research ideas and collaboration. We ask our partners if there are problems that have come up where they could use statistical help but they just don't have the time to tackle them. While these opportunities are at times hard to find and you have to have the right people to match to make this work, the results from these projects can be extremely valuable and satisfying for both the faculty member and the company. One example was a project where one of our corporate partners needed help on a reliability project. We had an early career faculty member who is an expert in reliability who received a grant from the company to do research on this project. He was able to publish portions of his work, which helped with his promotion in our field. This is one example of where a problem from industry led to real advances in reliability research.

I encourage other colleges and universities to consider creating a program like our Corporate Partners program that can foster these types of relationships and help with the logistics of creating the partnerships between faculty and companies. In order for industry to help spur innovative research really in any field, we as faculty members have to be open to adapting our research agendas to address the research topics presented like those in network monitoring.

Sengupta

Many industrial systems have complex interconnectedness, where a network monitoring framework could be highly relevant. Examples include logistics chains and coordination networks between teams. Infrastructural networks such as traffic networks and power grid networks are important components in the success of many industrial processes, and network monitoring could play a valuable role in analyzing the dynamics of such systems as well.

Sparks and Paris

We think the challenge will be in assessing the right set of skills that can make a valuable contribution to future social networks analysis. Sales networks are currently exploited by Amazon and similar companies that sell to the public. They identify what people purchase, and then offer people similar items that people may want to buy based on their purchasing habits. Online advertising has been revolutionized in part with people marketing their skills and offerings, which has been made easier with the digital economy. Also, companies are able to market themselves and core activities on the Internet. Establishing communities around products and services has been a well-known method of building brand loyalty, establishing exit barriers, and facilitating viral marketing through self-emergent customer testimonials (Assaad and Gómez 2011; Yu et al. 2021). We feel that warranty claims for a complex product could be monitored using time to event data analysis. Anomalies in their frequencies could provide useful information. These are already mature areas of services that are offered to the network of customers.

Online shopping offers a different experience to customers compared to shopping centers. They often appeal to different customers that want different experiences. These differences need to be examined for their understanding. Supermarkets have all but taken over the grocery shopping marketshare with the disappearance of most corner stores. However, these simple networks of customers are relatively easy to please because supermarkets offer convenience shopping with most of the purchasing needs in one location. Inventory control at shopping centers and online stores are another challenging area ripe for monitoring. The past selling history and stock history could be used for controlling inventory to ensure products are always available when they are needed.

Editors' comments

There is a strong consensus among the panelists that industry, technology, and government sectors each play an important role in the innovation of network monitoring techniques. On the other hand, it is also agreed that network monitoring provides an important set of techniques that can help answer significant challenges in these sectors. Industries in artificial intelligence, Industry 4.0, e-commerce, and engineering bring with them complex interconnected (network) data for which traditional quality engineering strategies are not directly appropriate. Although there

are commonalities, the challenges for network monitoring are often industry-specific and not only require special methodological considerations, but also interdisciplinary expertise. The relationship between network monitoring and the discussed applications introduces rich opportunities for innovation and development in the field of network monitoring.

Question

What broader impacts do you see network monitoring playing in the next decade? In particular, comment on what impact network monitoring strategies will have on technology, government, and academia. In the context of these broader institutions, what are some of the challenges that need to be addressed within the next 5 to 10 years?

Sengupta

Networks are ubiquitous in today's world, and most real-world networks vary over time. Network monitoring plays a key role in such settings. For example, the ongoing COVID-19 pandemic has underscored that social contact networks change over time, due to seasons, weekly and daily cycles, as well as behavioral patterns. The time-varying behavior of social contact networks plays a critical role in determining whether or how fast an infectious disease will spread through a population (Prakash et al. 2010; Leitch, Alexander, and Sengupta 2019; Holme and Saramäki 2012). Thus, network monitoring can be a key component of public health policy.

In my view, the future of network monitoring is very bright and promising, and I see three challenges that need to be addressed:

- We need to develop statistically rigorous network monitoring methods that allow flexible dependence patterns between networks observed at successive time points.
- We need to formulate computationally efficient algorithms to implement these methods for large-scale networks.
- We need to actively collaborate with network scientists from different disciplinary domains to understand unique challenges in their fields and to ensure swift adaptation of statistical methods in network science research.

Reisi and Paynabar

The broader impact of network monitoring should be viewed in the context of its wider application areas. One emerging application of network monitoring is in security of cyber-physical systems that are transforming a wide range of engineering, technology, and government strategies. Applications of cyber-physical systems in which IOT devices are interconnected is significant in the future of manufacturing, healthcare, transportation, and construction industries (Devi and Rukmini 2016; Mourtzis, Vlachou, and Milas 2016; Kodali, Swamy, and Lakshmi 2015). Nevertheless, these systems come with security and reliability risks that should be addressed. Due to the interconnected nature of cyber-physical systems, intrusions and faults propagate and cause malfunctions or security risks at distant devices or locations. Network monitoring plays a significant role in modeling, monitoring, and diagnosis of IOT frameworks to achieve more efficient, reliable, and secure systems. Recent cybersecurity breaches indicate how cyber-attacks can impact the physical systems such as supply chain networks (Pandey et al. 2020). Advances in network monitoring for fast detection and isolation of faults or intrusion will have significant impact on the society by enhancing national security and resiliency.

Another major impact of network monitoring is on social network monitoring and analysis. Social networks have been shown to be very effective in the creation of social movements and spread of fake news (Farajtabar et al. 2017). Network monitoring is a crucial component of early detection of malicious social movements caused by the spread of fake news and identification of its sources. These studies have important implications both in theoretical social sciences and in government policy making. One major challenge, besides the technical challenges mentioned previously, is data accessibility. Because of privacy concerns and proprietary reasons, IOT and social media data are not accessible to academics for research purposes. This hinders the development of more effective and realistic network monitoring methods by researchers.

Michailidis

As outlined in this brief discussion, network monitoring has introduced new exciting problems that require strongly interdisciplinary approaches and a good understanding of domain knowledge for addressing them. Hence, it has led to new fruitful collaborations between various academic fields, and interactions

between academia, government organizations and industry in the form of formulating new problems, making network data publicly available for experimentation and implementing new techniques in software tools deployed on networks, just to name a few.

An ongoing challenge is that network monitoring acts as an input to control systems for physical and engineered systems. Hence, detection of network change points in real time can trigger various forms of corrective actions, ranging from traffic rerouting, to shutdown of parts or even the entire system. However, detection of a change point may be the result of injection of false data. An obvious mitigation strategy would be to harden the security of measurement devices on such systems. Nevertheless, it should be complemented by deploying network monitoring algorithms that exhibit a certain degree of robustness to false data injections. Such algorithms may be easier to develop in application areas wherein the underlying data obey certain physical laws or engineering principles. The topic has attracted attention in the context of monitoring power networks (smart grids). However, given the ever increasing importance of cyber-physical systems in our daily lives, this problem merits additional study in the context of network monitoring.

Driscoll

A major contribution statisticians have had on network analyses and especially network monitoring is the need to not only look at how methods perform using case study data, but to actually simulate network data and study the properties of these monitoring methods. Yu et al. (2021) acts as a great resource to encourage comparative studies. These types of studies are critical for developing methods that help answer the research questions related to network data analysis and will allow our work to have an impact in the next decade.

While simulation studies are very important, we also must not lose sight of the power of case studies and example datasets that help show how our methods can tackle current problems that we face in society. If we do this, we will keep people excited about network monitoring research and we can continue to have an impact on areas like technology and government. It would be very beneficial for us to acquire datasets or be part of collaborations that focus on applications in the area of cyber security, (biological) neural networks and the study of the spread of infectious diseases. These are all areas that represent some of the challenges that need to be addressed within the next 5 to 10 years and as a result could lead to many funding opportunities.

There are also many open areas of research that can all have impacts on technology, government and academia. One way to expedite this impact is to make code-sharing common practice. This allows the community to easily simulate network type data and evaluate network monitoring methods. In order for practitioners to use our methods, they must have the infrastructure in place to implement our techniques. An important indicator of success in our field would be if some of the main statistical software companies begin implementing our network monitoring methods from the literature in the next 5 to 10 years. That being said, we also have opportunities to use other technologies to create graphical user interfaces so that practitioners can more readily use our methods. In conclusion, there are a lot of open questions that are waiting to be answered in network monitoring and network science in general that will make for a fun ride in the next 5 to 10 years!

Sparks and Paris

In many transaction-based applications, such as eBay, trust is a core component of the fact that sellers are going to trust that the product is genuine, and that the purchaser is going to pay for the product and its postage. A major challenge with social media is the amount of misinformation that is disseminated, and to think about how to combat this so as to protect those most vulnerable (Gong et al. 2020; Kauffmann et al. 2020; Amoruso et al. 2020; Guo, Chen, and Wu 2020; Dhillon, Breuer, and Hirst 2020; Sahoo and Gupta 2021; Gentina, Chen, and Yang 2021). Cheong and Babcock (2021) considered misleading and contentious tweets during a natural hazard. Do we have a responsibility to protect individuals from such misinformation? And what do we do about the individuals that have a right to freedom of speech? These are the types of questions that will need to be considered as social media monitoring enters into the mainstream.

New applications of the research and technology are emerging. We name a few here: understanding employment opportunities, crisis management, sentiment/emotion/opinion mining for a whole range of applications, the agrifood sector and tourism. There is evidence that one's network is likely to determine one's future employment prospects, because of the fundamental role that social networks play in shaping human activity (Jackson 2011). With the creation of

an application like CrowdHelp, we are stepping into the next stage of crowdsourced information for crisis management (Besaleva and Weaver 2013; Jin, Liu, and Austin 2014; Kim and Hastak 2018; Kankanamge et al. 2019; Saroj and Pal 2020; Yin et al. 2015). All that is needed is a smartphone in our pocket for providing a faster and more accurate model of a situation's current state. "Social networks are still growing while relevant threats are increasing. We should pay more attention to the safety of social networks" stated by Luo et al. (2009). In their work, Devece, Palacios, and Ribeiro-Navarrete (2019) used crowdsourcing for online social networks to improve organizational performance. On the whole, Italian agrifood companies have lately understood the opportunities offered the social media (Sturiale and Scuderi 2013; Scuderi and Sturiale 2014) in order to refer directly to final consumers who are here involved actively by including the "experience sharing" in contexts of food related products.

A sustainable tourism study on the Gili Islands in Indonesia highlights the contribution that social media can play in supporting tourism (Partelow and Nelson 2020). We have been approached by tourism emeritus Professor Roy Ballantyne to carry out a similar study while tourism was allowed in Australia. Yet other applications covered in the literature are: methods of rumor blocking are outlined by Guo, Chen, and Wu (2020) and Zhu, Ghosh, and Wu (2021). López-Vizcaíno et al. (2021) examined early detection of cyberbullying on social media networks.

Finally, in our own work, we have considered drought assessment in Australia using real-time social media data, and this could be expanded to animal diseases with farmers sharing their diseased history with the local farmers in a way that could track the progression of animal diseases particularly for those domestic animals. Tracking the advances and movement of a recent mice plague in Australia could have been handled in this way. Fauna and flora diseases could be geographically tracked using similar techniques. Albizua et al. (2021) used social networks to influence farming practices and agrarian sustainability. The role of farmers' social networks in the implementation on farming practices as explored by Skaalsveen, Ingram, and Urquhart (2020); Pratiwi and Suzuki (2017); Maertens and Barrett (2013) deserves further attention.

Perry

As indicated earlier, I believe the broader impacts of network monitoring will be prevalent in Industry 4.0 processes, perhaps in the context of detecting or preventing cyber-physical attacks on modern manufacturing systems. This can impact technology by enabling more stable and secure smart systems in a world of ever-increasing cyber threats. Furthermore, this can impact governments as ransomware attacks are on the rise and capable of causing significant harm at the local, national, and global levels (as was recently witnessed with the Colonial Pipeline ransomware attack). However, social network monitoring is also an area where I feel statistical network monitoring will have significant future impact. Some particular areas to consider include the detection of shifts in population sentiment using online social networks, crisis detection in organizations using email networks, and monitoring for changes in the rate of propagation of information or disease using contact networks. Another potential application might involve cryptocurrency networks, e.g., monitoring the emotional sentiment of the investor community to gain potential insights into future price swings.

There are a number of challenges that I feel need to be addressed in the near future. Most typically, statistical network monitoring should permit the effective monitoring of network-based systems where the resulting anomaly signals are interpretable. Since there are many facets of networks that can change, interpreting control chart signals can become more arduous when monitoring network-based systems. Consequently, charting statistics should seek to capture the change phenomena of interest without being overly affected by uninteresting or natural changes to the network under study. Furthermore, monitoring methods should be developed so that false alarm rates can be adequately controlled, since the added expense of too many false signals can render a method infeasible. Lastly, given that most methods developed are data-based, data quality is an immediate concern, particularly when extracting data from online social networks or clandestine networks. In my view, it seems nearly impossible to obtain an unbiased sample and so novel strategies for dealing with sampling bias should also be considered.

McCulloh

The growth of artificial intelligence (AI) creates two key opportunities for network monitoring. Unsupervised AI relies heavily on clustering methods and relational data, which provides opportunities for statistical network monitoring. As AI technologies grow, engineers must integrate these new advances

into the manufacturing and service industries. How do humans interact with machines? What new roles are created? How do those roles, skills, tasks and resources interact and do they change over time?

Cyber networks are becoming increasingly important as we progress further into the information age. Cyber networks consist of many different types of relational data, generating interesting networks. Statistical network monitoring methods offer a promising approach to identifying threats in zero-trust environments. Monitoring may also alert administrators to changes in system performance that will improve overall quality.

Critical infrastructure such as power/electric, transportation, and communication are increasingly network problems. Applications of statistical network monitoring will provide important methods for understanding vulnerabilities and change over time. As more and more industry practitioners learn about and use network methods, the need for all network methods, process monitoring or otherwise will increase.

Editors' comments

The velocity, volume, and complexity of interconnected (network) data is rapidly increasing, and these data introduce new challenges in network monitoring. One such challenge that was mentioned several times was the need for scalable monitoring algorithms. Not only do we agree that there is a need for scalable network monitoring methods, we also agree with Dr. Perry's advocation for *interpretable* methods. These two interests are sometimes at odds with one another when it comes to model development. Statisticians and quality engineers are well-suited for developing interpretable methods; yet their algorithms are often not scalable. Computer scientists and other computational scientists are well-suited for developing scalable algorithms but often sacrifice interpretability. Thus we want to emphasize that future work should focus jointly on statistical and computational innovation.

In this discussion, it was also pointed out that there is often a need for methods that are ethical and respect privacy. This is particularly important in the context of monitoring social interactions, crowds, and information dissemination. There has been a major focus in the technology sector in the last few years to ensure what is called ethical artificial intelligence. We believe that researchers should take lessons from this area to ensure ethical network monitoring techniques as well. Finally, we were excited to see that this discussion pointed to a large variety of applications in which network monitoring will play a role - applications ranging from cyber security, to infectious disease monitoring, and from engineering to artificial intelligence. It is clear from this discussion that network monitoring is an important discipline and will remain so for the next decade.

ORCID

Nathaniel T. Stevens http://orcid.org/0000-0001-6149-5797
James D. Wilson http://orcid.org/0000-0002-2354-935X
Ian McCulloh http://orcid.org/0000-0003-2916-3914
George Michailidis http://orcid.org/0000-0002-3676-1739
Kamran Paynabar http://orcid.org/0000-0002-6906-3611
Srijan Sengupta http://orcid.org/0000-0001-6889-8599
Ross Sparks http://orcid.org/0000-0001-5852-5334

References

Agostinelli, S., F. Cumo, G. Guidi, and C. Tomazzoli. 2021. Cyber-physical systems improving building energy management: Digital twin and artificial intelligence. *Energies* 14 (8):2338. doi:10.3390/en14082338.

Albizua, A., E. M. Bennett, G. Larocque, R. W. Krause, and U. Pascual. 2021. Social networks influence farming practices and agrarian sustainability. *PloS One* 16 (1): e0244619. doi:10.1371/journal.pone.0244619.

Amoruso, M., D. Anello, V. Auletta, R. Cerulli, D. Ferraioli, and A. Raiconi. 2020. Contrasting the spread of misinformation in online social networks. *Journal of Artificial Intelligence Research* 69:847–79. doi:10.1613/jair.1.11509.

Assaad, W., and J. M. Gómez. 2011. Social network in marketing (social media marketing) opportunities and risks. *International Journal of Managing Public Sector Information and Communication Technologies* 2 (1):13.

Besaleva, L. I., and A. C. Weaver. 2013. Applications of social networks and crowdsourcing for disaster management improvement. In 2013 International Conference on Social Computing, pp. 213–219. IEEE.

Cheong, S.-M., and M. Babcock. 2021. Attention to misleading and contentious tweets in the case of hurricane harvey. *Natural Hazards* 105 (3):2883–906. doi:10.1007/s11069-020-04430-w.

Devece, C., D. Palacios, and B. Ribeiro-Navarrete. 2019. The effectiveness of crowdsourcing in knowledge-based industries: The moderating role of transformational leadership and organisational learning. *Economic research-Ekonomska Istraživanja* 32 (1):335–51. doi:10.1080/1331677X.2018.1547204.

Devi, Y. U., and M. Rukmini. 2016. Iot in connected vehicles: Challenges and issues—a review. In 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), pp. 1864–1867. IEEE. doi:10.1109/SCOPES.2016.7955769.

Dhillon, P., M. Breuer, and N. Hirst. 2020. Covid-19 breakthroughs: Separating fact from fiction. *The FEBS Journal* 287 (17):3612–32. doi:10.1111/febs.15442.

Elhabashy, A. E., R. Dastoorian, L. J. Wells, and J. A. Camelio. 2021. Random sampling strategies for multivariate statistical process control to detect cyber-physical manufacturing attacks. *Quality Engineering* 33 (2):300–17. doi:10.1080/08982112.2020.1838541.

Elhabashy, A. E., L. J. Wells, and J. A. Camelio. 2020. Cyber-physical attack vulnerabilities in manufacturing quality control tools. *Quality Engineering* 32 (4):676–92. doi:10.1080/08982112.2020.1737115.

Farajtabar, M., J. Yang, X. Ye, H. Xu, R. Trivedi, E. Khalil, S. Li, L. Song, and H. Zha. 2017. Fake news mitigation via point process based intervention. In International Conference on Machine Learning, pp. 1097–1106. PMLR.

Gentina, E., R. Chen, and Z. Yang. 2021. Development of theory of mind on online social networks: Evidence from facebook, twitter, instagram, and snapchat. *Journal of Business Research* 124:652–66. doi:10.1016/j.jbusres.2020.03.001.

Gokhale, A., M. P. McDonald, S. Drager, and W. McKeever. 2010. A cyber physical systems perspective on the real-time and reliable dissemination of information in intelligent transportation systems. Technical report, Air Force Research Lab Rome NY.

Gong, Z., H. Wang, W. Guo, Z. Gong, and G. Wei. 2020. Measuring trust in social networks based on linear uncertainty theory. *Information Sciences* 508:154–72. doi:10.1016/j.ins.2019.08.055.

Guo, J., T. Chen, and W. Wu. 2020. A multi-feature diffusion model: Rumor blocking in social networks. *IEEE/ACM Transactions on Networking* 29 (1):1–397. doi:10.1109/TNET.2020.3032893.

Holme, P., and J. Saramäki. 2012. Temporal networks. *Physics Reports* 519 (3):97–125. doi:10.1016/j.physrep.2012.03.001.

Jackson, M. O. 2011. An overview of social networks and economic applications. *Handbook of Social Economics* 1:511–85.

Jin, Y., B. F. Liu, and L. L. Austin. 2014. Examining the role of social media in effective crisis management: The effects of crisis origin, information form, and source on publics' crisis responses. *Communication Research* 41 (1):74–94. doi:10.1177/0093650211423918.

Kankanamge, N., T. Yigitcanlar, A. Goonetilleke, and M. Kamruzzaman. 2019. Can volunteer crowdsourcing reduce disaster risk? a systematic review of the literature. *International Journal of Disaster Risk Reduction* 35:101097. doi:10.1016/j.ijdrr.2019.101097.

Kauffmann, E., J. Peral, D. Gil, A. Ferrández, R. Sellers, and H. Mora. 2020. A framework for big data analytics in commercial social networks: A case study on sentiment analysis and fake review detection for marketing decision-making. *Industrial Marketing Management* 90:523–37. doi:10.1016/j.indmarman.2019.08.003.

Kim, J., and M. Hastak. 2018. Social network analysis: Characteristics of online social networks after a disaster. *International Journal of Information Management* 38 (1):86–96. doi:10.1016/j.ijinfomgt.2017.08.003.

Kodali, R. K., G. Swamy, and B. Lakshmi. 2015. An implementation of iot for healthcare. In 2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS), pp. 411–416. IEEE. doi:10.1109/RAICS.2015.7488451.

Leitch, J., K. A. Alexander, and S. Sengupta. 2019. Toward epidemic thresholds on temporal networks: A review and open questions. *Applied Network Science* 4 (1):1–21. doi:10.1007/s41109-019-0230-4.

Li, D., N. Gebraeel, K. Paynabar, and A. Meliopoulos. 2021. An online approach to cyberattack detection and localization in smart grid. *arXiv Preprint arXiv:2102.11401*

López-Vizcaíno, M. F., F. J. Nóvoa, V. Carneiro, and F. Cacheda. 2021. Early detection of cyberbullying on social media networks. *Future Generation Computer Systems* 118:219–29. doi:10.1016/j.future.2021.01.006.

Luo, W., J. Liu, J. Liu, and C. Fan. 2009. An analysis of security in social networks. In 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, pp. 648–651. IEEE.

Maertens, A., and C. B. Barrett. 2013. Measuring social networks' effects on agricultural technology adoption. *American Journal of Agricultural Economics* 95 (2):353–9. doi:10.1093/ajae/aas049.

Mourtzis, D., E. Vlachou, and N. Milas. 2016. Industrial big data as a result of iot adoption in manufacturing. *Procedia Cirp* 55:290–5. doi:10.1016/j.procir.2016.07.038.

Pandey, S., R. K. Singh, A. Gunasekaran, and A. Kaushik. 2020. Cyber security risks in globalized supply chains: Conceptual framework. *Journal of Global Operations and Strategic Sourcing* 13 (1):103–28.

Partelow, S., and K. Nelson. 2020. Social networks, collective action and the evolution of governance for sustainable tourism on the gili islands, indonesia. *Marine Policy* 112:1–12. doi:10.1016/j.marpol.2018.08.004.

Perry, M. B. 2020. An ewma control chart for categorical processes with applications to social network monitoring. *Journal of Quality Technology* 52 (2):182–97. doi:10.1080/00224065.2019.1571343.

Prakash, B. A., D. Chakrabarti, M. Faloutsos, N. Valler, and C. Faloutsos. 2010. Got the flu (or mumps)? check the eigenvalue!. *arXiv Preprint arXiv:1004.0060*.

Pratiwi, A., and A. Suzuki. 2017. Effects of farmers' social networks on knowledge acquisition: Lessons from agricultural training in rural indonesia. *Journal of Economic Structures* 6 (1):1–23. doi:10.1186/s40008-017-0069-8.

Sahoo, S. R., and B. B. Gupta. 2021. Multiple features based approach for automatic fake news detection on social networks using deep learning. *Applied Soft Computing* 100:106983. doi:10.1016/j.asoc.2020.106983.

Saroj, A., and S. Pal. 2020. Use of social media in crisis management: A survey. *International Journal of Disaster Risk Reduction* 48:101584. doi:10.1016/j.ijdrr.2020.101584.

Scuderi, A., and L. Sturiale. 2014. Analysis of social network applications for organic agrifood products. *International Journal of Agricultural Resources, Governance and Ecology* 10 (2):176–89. doi:10.1504/IJARGE.2014.063583.

Skaalsveen, K., J. Ingram, and J. Urquhart. 2020. The role of farmers' social networks in the implementation of no-till farming practices. *Agricultural Systems* 181:102824. doi:10.1016/j.agsy.2020.102824.

Sparks, R. 2015. Social network monitoring: Aiming to identify periods of unusually increased communications between parties of interest. In *Frontiers in statistical quality control*, eds. S. Knoth and W. Schmid, Vol. 11, 3–13. Cham: Springer.

Sturiale, L., and A. Scuderi. 2013. Evaluation of social media actions for the agrifood system. *Procedia Technology* 8: 200–8. doi:10.1016/j.protcy.2013.11.028.

Yin, J., S. Karimi, A. Lampert, M. Cameron, B. Robinson, and R. Power. 2015. Using social media to enhance emergency situation awareness. In Twenty-fourth international joint conference on artificial intelligence.

Yu, L., I. M. Zwetsloot, N. T. Stevens, J. D. Wilson, and K. L. Tsui. 2021. Monitoring dynamic networks: A simulation- based strategy for comparing monitoring methods and a comparative study. *Quality and Reliability Engineering*. doi:https://doi.org/10.1002/qre.2944

Yu, X., C. Yuan, J. Kim, and S. Wang. 2021. A new form of brand experience in online social networks: An empirical analysis. *Journal of Business Research* 130:426–35. doi:10.1016/j.jbusres.2020.02.011.

Zhu, J., S. Ghosh, and W. Wu. 2021. Robust rumor blocking problem with uncertain rumor sources in social networks. *World Wide Web* 24 (1):229–47. doi:10.1007/s11280-020-00841-8.