TCSN Newsletter – Issue Twelve – December 2023

Social Networks Technical Committee

Editor: Prof. De-Nian Yang, Prof. Damla Turgut, and Prof. Burak Kantarci

TC website	https://sn.committees.comsoc.org/
TC officers	Chair: Prof. Damla Turgut
	Vice-Chair: Prof. De-Nian Yang
	Secretary: Prof. Burak Kantarci
Newsletter Editor	Dr. Claudio Marche

For information about the newsletter, please contact claudio.marche@unica.it

CHAIR’S MESSAGE

When social media dominates the traffic over the Internet and mobile communication networks, there are further insights and engineering that could be developed based on understanding social networks in depth. Such interplay between technological networks and social networks has so many different aspects to inspire IEEE Communications Society members toward the further frontier of communication technology and benefits of human society. Under such background, Technical Committee on Social Networks (TCSN) is established in 2016, after incubation as a sub-committee in Emerging Technology. We believe that the TCSN newsletters allow us a more fluent exchange of vision, ideas, and technological opportunities, in addition to the website and social media platforms. We greatly appreciate all the members who have contributed to this issue of the newsletter. Last, but not least, we wish TCSN newsletters serve as an effective means for this exciting multi-disciplinary knowledge on social networks to blend humanity and technology in an even better way. Most important, please welcome you to actively participate or initiate more volunteer services to TCSN and IEEE Communications Society.

Best wishes,

Damla Turgut, Chair, TCSN, 2022-2023

UPCOMING CONFERENCES & CFP FOR SOCIAL NETWORKS TRACK

IEEE ICC 2023: May 28 – June 1, Rome, Italy
IEEE Globecom 2023: December 4 – December 8, Kuala Lumpur, Malaysia
IEEE ICC 2024: June 9 – June 13, 2024, Denver, USA

Social networks have become prevalent forms of communication and interaction on the Internet and contribute to an increase in network traffic. As a result, social networks have attracted significant research interests in many related areas. Social networks have traditionally been studied outside of the technological domains; however, the focus is now changing towards networking challenges such as cloud, privacy, data analytics, and so on while still keeping the social perspective such as focusing on improving quality of life. The interplay between social networks and technological networks such as mobile networks and mobile computing is becoming still strong and many areas are still to be exploited.

TCSN Newsletter – Issue Twelve – December 2023
Social Networks Technical Committee
Editor: Prof. De-Nian Yang, Prof. Damla Turgut, and Prof. Burak Kantarci

CONTAGION SOURCE DETECTION IN ONLINE SOCIAL NETWORKS: FROM COVID-19 INFODEMICS TO GEN-AI BASED DISINFORMATION SPREADING

CHEE WEI TAN

ASSOCIATE PROFESSOR, SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

NANYANG TECHNOLOGICAL UNIVERSITY, SINGAPORE

Introduction

Online social networks like X (formerly Twitter), Facebook, and Telegram serve as critical platforms for spreading news and various types of information. However, they also possess the potential to propagate misinformation and disinformation at an alarming rate, surpassing traditional word-of-mouth channels. It is widely believed that false information tends to spread more swiftly than verifiable truths within an online social network. Misinformation pertains to inaccurate or unreliable information disseminated without necessarily intending to mislead. Conversely, disinformation encompasses deliberately fabricated misinformation (e.g., false news) circulated with the purpose of influencing decision-making or advancing a particular agenda. With the unprecedented reach of online platforms, malicious actors can now disseminate information across vast geographical regions faster than ever before. Consequently, online rumors, misinformation, and disinformation have the potential to disrupt livelihoods and yield substantial real-world consequences.

Notable instances include the dissemination of politically charged messages on social media, which ignited waves of protests and demonstrations during the "Arab Spring" in 2010-2012. Additionally, in 2013, a fabricated tweet claiming an attack on the White House went viral after being posted by the hacked Associated Press Twitter account. This incident briefly triggered a stock market crash, demonstrating the capacity of online disinformation to prompt sudden market fluctuations and enable cybercriminals to profit in the process. A similarly grave incident occurred in 2020 when hackers gained control of numerous high-profile Twitter accounts, including those of Barack Obama and Elon Musk, to promote a "double your bitcoin" scam that rapidly gained traction. Ultimately, this cryptocurrency scam resulted in the theft of over $110,000 worth of bitcoins before the fraudulent messages were removed. Such instances of internet fraud and cybersecurity threats are anticipated to become more prevalent, particularly as bots are enlisted to sow discord and amplify the dissemination of disinformation.

Governments worldwide now acknowledge that the proliferation of misinformation and disinformation poses a significant cybersecurity threat that warrants serious attention from law enforcement agencies. However, distinguishing between benign misinformation and intentional disinformation can often be challenging. Furthermore, rapid advancements in deepfake technology have the potential to make fabricated news appear authentic, further exacerbating the issue. Identifying and countering rumor mongers, along with dispelling disinformation on an amplified scale, will constitute a timely and practical defence strategy that can offer profound insights into the science of networks.

The emergence of generative artificial intelligence (Gen-AI), particularly ChatGPT in late November 2022, has revolutionized the creation and dissemination of information, enabling unprecedented amount of information propagating at scale across the globe. However, this newfound tool has also paved the way for the rapid spread of rumors, misinformation, and disinformation. There is now a complex interplay between Gen-AI, online social networks, and critical societal issues that affect mankind worldwide. In the October 2023 edition of the Communications of the ACM, Vint Cerf highlighted that addressing the scale of information entails utilizing AI filters and consumer-driven curation. However, the emergence of deep fakes adds complexity to the situation. Although transparency and source verification can mitigate disinformation, they are not infallible. Promoting critical thinking is crucial but demands active engagement. A strong demand for reliable information could play a significant role in finding a solution. We briefly examine some of threats of rumor spreading in online social networks and discuss open questions in the following.

Rumors as Catalysts for COVID-19 Infodemics

The COVID-19 pandemic ushered in not just a global health emergency, but also an unprecedented surge in misinformation, leading to what the World Health Organization termed as an "infodemic". The World Health Organization's declaration of a "COVID-19 Infodemic" emphasized the seriousness of the issue. As communities grappled with an unfamiliar and potentially life-threatening virus, online social networks became fertile ground for the spread of false information. This misinformation ranged from baseless treatment claims to elaborate conspiracy theories, not only hindering effective pandemic response but also posing a significant threat to public health. The COVID-19 pandemic has underscored the far-reaching consequences of misinformation on public health. Much like identifying patient zero in an epidemic outbreak, the crucial question becomes: who is the rumor monger? Another critical aspect of this endeavor involves proactively verifying and disseminating accurate information. What is the science of fact-checking?

The inherent ability of rumors to go viral is amplified by human curiosity, fear, and the desire for novelty. Analogous to the dynamics of epidemic spread, the mechanisms driving rumors reveal compelling parallels, emphasizing the need for a multidisciplinary approach to address this phenomenon. Identifying the origins of rumors and understanding the network structures that facilitate their rapid dissemination is crucial in devising effective countermeasures. Fact-checking organizations and health authorities have collaborated with social media platforms to promptly identify and flag misleading or false information related to COVID-19. By implementing networking algorithms and fact-checking systems, online social networks can swiftly detect and remove such content, reducing its reach and potential harm.

Additionally, accurate and reliable sources of information, such as official health organizations and reputable news outlets, are promoted to ensure users have access to trustworthy updates. A vital strategy is the promotion of health literacy and digital media literacy. Intelligent online social networks can be leveraged as essential tools for information-seeking during crises, making it imperative for users to discern reliable sources from misinformation. Similar to how the TCP/IP protocol facilitates user coordination for network resource utilization to mitigate congestion, we will require dependable information processing protocols disseminated through online platforms to combat misinformation. These protocols aim to equip individuals with the ability to critically evaluate information. By fostering a culture of discernment and skepticism, users are better prepared to navigate the influx of information and make informed decisions. Stakeholders of online social networks will need to share insights, data, and work together to develop and implement innovative strategies. This collaborative approach can led to the creation of tools like chatbots and information hubs that provide accurate and up-to-date information directly within social media platforms. Such initiatives enhance accessibility to reliable information, reducing reliance on potentially misleading sources. Algorithms are designed to prioritize content from trusted sources, ensuring that users are exposed to accurate information. Additionally, contagion source detection algorithms can be deployed to issue warnings to content that may contain misinformation, providing users with the context of provenance and directing them to verified sources. These measures collectively serve to create an environment where accurate information is more prominently featured, mitigating the impact of misinformation.

By employing a multi-faceted approach that encompasses fact-checking, collaborative network algorithms, and real-time interventions, we can effectively combat the spread of misinformation. As we navigate future health crises such as that posed by Disease X outbreaks, it is imperative that we continue to prioritize the responsible use of online social networks in disseminating accurate and timely information to safeguard public health and emphasizing the need for proactive strategies in mitigating misinformation spreading.

Combatting Generative-AI Disinformation: The Urgent Imperative

Generative AI, exemplified by large language models like OpenAI GPT series (e.g., ChatGPT and Codex), has the potential to both exacerbate and mitigate the issue of disinformation in online social networks. On one hand, these models are incredibly powerful at generating human-like text, which can be exploited to create and disseminate false or misleading information at an unprecedented scale. This raises concerns about the proliferation of misinformation, as AI-generated content can be used to amplify conspiracy theories, false claims, and divisive narratives. However, on the other hand, Generative AI also offers a powerful tool for combating disinformation.

Large language models can potentially be harnessed to develop advanced fact-checking and content moderation systems. By training AI models to recognize patterns indicative of misinformation, platforms can automate the process of flagging and removing false content. Additionally, Gen-AI can be used to generate accurate and informative content, providing users with reliable information and countering the spread of falsehoods.

In particular, Gen-AI driven conversational agents (e.g., WHO launched a chatbot to combat COVID-19 Infodemic) can assist to disseminate the right kind of information through online social networks to reach a wide audience, empowering users to navigate the digital landscape with greater confidence. Human users can crowdsource and, together with Gen-AI conversational agents, co-participate in the creation of educational resources and campaigns aimed at promoting critical thinking as well as generating content that highlights the importance of verifying information from reputable sources. In addition, Gen-AI agents can play a role in sentiment analysis and trend detection. For example, by analyzing online discourses, AI models can identify emerging topics and sentiments, providing early warning signs of potential infodemics. This enables authorities to respond swiftly and implement targeted interventions to curb the spread of misinformation. We list below several pressing open problems that warrant attention:

1. Dynamic Modeling of Gen-AI Disinformation Spreading: Developing sophisticated models capable of predicting the propagation of Gen-AI driven disinformation in real-time, accounting for evolving network structures and user behaviour.
2. Source Identification with Limited Data: Enhancing techniques for identifying the origins of misinformation swiftly, accurately, and reliably with minimal observation data, particularly in large-scale networks. Identifying bots or human individuals with outsized influence in misinformation spreading allows for targeted interventions.
3. Cross-Network Pollination: Understanding the mechanisms by which ideas and misinformation traverse diverse networks with distinct bot and human interaction patterns, and devising Gen-AI based strategies to understand cross-pollination.
4. Gen-AI Countermeasures: Harnessing advanced technologies to automate the detection and mitigation of disinformation, while taking into account potential biases and ethical concerns surrounding Gen-AI driven interventions aimed at curbing misinformation, ensuring transparency, data privacy, and accountability.
5. Intervention Strategies for Rapid Response: Designing intervention strategies that can be promptly deployed to curb the rapid dissemination of disinformation. Investigating Gen-AI strategies to promote lasting behavioural changes in information consumption and sharing habits, bolstering resilience against disinformation in the long run.

Conclusion

The parallels between epidemic spreading and the dissemination of rumors and misinformation highlight the urgency for multidisciplinary approaches in tackling these issues. Leveraging advanced technologies and refining information verification protocols are essential steps towards countering the rapid spread of falsehoods. It is imperative that we continue to develop innovative strategies to identify and mitigate contagion sources. By doing so, we can fortify our defenses against infodemics. The impact of Gen-AI on online social networks is dual-faceted. While it poses challenges in terms of generating and disseminating false information, it also offers powerful solutions in the form of automated fact-checking, educational initiatives, and trend analysis. By leveraging Gen-AI responsibly and in conjunction with other AI ethic compliance measures, Gen-AI models can contribute to building a more discerning and informed online community.

Chee Wei Tan,
cheewei.tan@ntu.edu.sg

TRUSTED DATA OFFLOADING IN VEHICULAR NETWORKS BY EXPLOITING SOCIAL INTERNET OF VEHICLES AND REINFORCEMENT LEARNING

Yasir Saleem

Lecturer In Computer Science

Aberystwyth University, United Kingdom

Kok-Lim Alvin Yau

Professor

Universiti Tunku Abdul Rahman (UTAR), Malaysia

Nathalie Mitton

Senior Researcher

Inria Lille – Nord Europe, France

The Social Internet of Vehicles (SIoV) is a combination of two key technologies, namely Social Internet of Things (SIoT) and Internet of Vehicles (IoV). SIoT infuses IoT with the concept of social networking to establish social relationships, which facilitate autonomous collaboration without human intervention, among smart objects/ things connected to the Internet. IoV enhances connectivities between vehicles, and between vehicles and roadside units (RSUs), to enhance network performance (e.g., a shorter end-to-end delay) in vehicular networks. SIoV brings together the benefits of SIoT and IoV, enabling vehicles and RSUs to establish social relationships and collaborations among themselves to further enhance network performance.

Data offloading transfers data gathered or generated at a vehicle to complementary network infrastructure, particularly the RSUs, to process a large number of data received from the vehicles. In SIoV, vehicles collect different types of data (e.g., accident, emergency, advertisement, and backup data) mostly through sensors deployed on vehicles and offload the collected data in the upstream direction to RSUs for relevant departments to get notified of incidents and take appropriate actions (e.g., emergency services to send a rescue team in case of accidents). Data is offloaded to RSUs by vehicles either directly (if RSU is inside the communication range) or indirectly by relaying through other vehicles (if RSU is outside the communication range) by autonomously collaborating and establishing social relationships among vehicles and RSUs.

In this scenario of data offloading in SIoV, trust management is an important process to be considered because individuals or groups of malicious vehicles (or entities) may perform various types of attacks for their own benefits. As an example, if a malicious vehicle is not in the communication range of an RSU but is in the communication range of other vehicles, it requests other vehicles to offload its own data toward an RSU. However, upon request from the requested vehicles in a symmetric way, it simply declines to offload with fake reasons, such as a lack of capacity while offloading data to other vehicles although there is sufficient capacity. Consequently, the malicious vehicle takes advantage of other vehicles without offering its own resources in return, creating an unfair environment. As another example, a group of malicious vehicles offload each other's data and request other vehicles to offload their data. But when other vehicles request one of these malicious vehicles to offload their data, even though they might have the capacity to do it, they decline. Moreover, a group of malicious vehicles can jam the network through a denial of service (DoS) attack by colluding and flooding the network with fake data offloading.

SIoV can help in the trust management of data offloading. RSUs are connected with each other, and they regularly exchange messages with vehicles. Therefore, trust management can be handled by RSUs. Since vehicles regularly communicate with other vehicles and RSUs, the RSUs receive information from vehicles about themselves and their neighboring vehicles. Subsequently, RSUs calculate the reputation of each vehicle and periodically disseminate the reputation of vehicles to other RSUs and vehicles. In this manner, RSUs and vehicles have up-to-date reputations of vehicles in the network. Since vehicles are not necessarily connected with RSUs all the time, the vehicles having the updated vehicles' reputations can share them with their neighboring vehicles that are not in the communication range of RSUs in a collaborative manner to equip them with up-to-date vehicles' reputations, thanks to the social aspect of SIoV. In this manner, vehicles can be cautious about malicious vehicles while granting/ sending data offloading requests to/from other vehicles.

Let's consider an example. An individual or a group of malicious vehicles act in a selfish manner by offloading their data to RSUs with the help of other vehicles, however, when they are requested to offload data of other vehicles, they deny the requests with a false reason that their capacity is full. Each vehicle records request acceptance/ decline responses of their requesting vehicles and shares this information periodically with RSUs directly if it is located inside the communication range and using the store-carry-forward mechanism if RSU is located outside the communication range. RSUs receive this information and their trust management systems reduce the reputations of such malicious vehicles, and disseminate the updated vehicles' reputations in the network. This penalizes such malicious vehicles in a way that other vehicles will not collaborate with malicious vehicles to offload their data to RSUs leading to losing the social relationship of malicious vehicles with other vehicles.

When it comes to trust management systems, reinforcement learning (RL) is a potential candidate for evaluating the trust scores of vehicles. RL is an artificial intelligence (AI) approach that enables a decision maker (vehicle/RSU) to observe the environment (the state and the reward), and subsequently take action to improve the state and reward in the next time instance. Initially, all vehicles have the same reputation. Then, based on the interactions and decisions made on data offloading requests between vehicles, RL can update each vehicle's reputation (reward) based on its current capacity to offload (state) and the decisions of accepting/ declining the request (action). This creates an opportunity for malicious vehicles to repent in a way that their reputations improve when they act benevolently in the current interaction.

New approaches, such as generative adversarial network (GAN), which is a generative AI approach, can be incorporated into RL. Real-world datasets comprised of positive and negative samples are used in transfer learning to pre-train RL algorithms. While positive samples without attacks are easy to collect, the opposite is true for negative samples with attacks, causing an imbalanced dataset and overfitting. This issue is compounded by the fact that there is a diverse range of attacks. GAN-enabled RL can be applied to generate synthetic yet high-quality negative samples for transfer training in RL. The pre-trained RL algorithm applied to real operating environments can be applied to increase the convergence rate to optimal actions, hence reducing the learning time.

To conclude, SIoV and RL can be beneficial for trusted data offloading in vehicular networks by providing social relationships and learning through interactions with the operating environment.

Yasir Saleem,
yasir.saleem@aber.ac.uk
Kok-Lim Alvin Yau,
yaukl@utar.edu.my
Nathalie Mitton,
nathalie.mitton@inria.fr

TCSN Newsletter – Issue Twelve – December 2023
Social Networks Technical Committee
Editor: Prof. De-Nian Yang, Prof. Damla Turgut, and Prof. Burak Kantarci

AN EVALUATION OF SERVICE DISCOVERY MECHANISMS FOR A NETWORK OF SOCIAL DIGITAL TWINS

SARA RANJBARAN

DOCTORAL RESEARCHER, DEPARTMENT OF COMPUTER SCIENCE

AALTO UNIVERSITY, FINLAND

CLAUDIO MARCHE

ASSISTANT PROFESSOR, DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING

UNIVERSITY OF CAGLIARI, ITALY

The Internet of Things (IoT) is a global network of interconnected physical devices, set to reach over 125 billion devices by 2030, or about 15 devices per person. The proliferation of IoT devices has resulted in a surge in network traffic, driven by the diverse range of services they offer. One of the core challenges within the IoT landscape is effective service discovery. While applications may know their service needs, they often lack knowledge about which devices can fulfill those needs. This necessitates the development of effective strategies to manage network traffic diversity and volume.

Addressing these challenges, the research community is promoting Digital Twin (DT) technology. DTs create virtual representations of physical systems, predicting their future status and capabilities. Effective service discovery plays a vital role in this context, allowing the network to locate the appropriate DTs offering desired services. Challenges persist due to the vast search space and the high volume of network traffic generated by IoT devices.

Moreover, recently, the concept of Social IoT (SIoT) has emerged as a solution to these issues. SIoT envisions each IoT node forming social relationships with other DTs, improving service discovery, selection, and composition. The idea is that devices can form relationships, much like people, which can improve the discovery, selection, and composition of services. Several SIoT models have been proposed in recent years, defining various forms of socialization among objects, such as Parental Object Relationships (POR), Co-location or Co-work Object Relationships (CLOR and CWOR), Ownership Object Relationships (OOR), and Social Object Relationships (SOR). However, the parameters for selecting the right "friend" in the social network are still a subject of exploration.

This scenario, building upon the concept of DTs in IoT as entities that both create and consume services, can leverage the benefits of the SIoT, where entities, namely Social DTs (SDTs), establish friendship links among each other to create a social network of “friends”. Whenever an SDT receives a new query, it checks if its friends are able to perform it; otherwise, it evaluates which is the best one to forward it to.

The service discovery mechanism plays a crucial role in determining which SDTs among the requester's friends are best suited to forward the query. The discovery process begins when the application layer initiates processing that requires the search for other services, leading to the generation of a relevant query. The SDT of the device triggering the process takes charge of the query and must select the most appropriate friend for each of the services required by the application. This mechanism relies on several parameters, allowing each SDT to make its selection based on its own local information.

The routing process assumes that each SDT has knowledge of the local social network topology and possesses information about its friends, including the services they offer, the number of relationships they maintain, and more. Each node forwards the query for the required services to the friend with the highest likelihood of satisfying them. Several essential parameters are considered in the service discovery mechanism, including:

- Degree Centrality: This parameter represents the number of relationships an SDT has in the social network. A higher degree of centrality implies a better chance of resolving the query and finding the desired service.
- Relationship Factor: This parameter reflects the strength of the relationship between nodes and aids the requester in navigating the network for specific services.
- Space Requirement: This parameter considers the spatial aspects by evaluating the distance between friends' positions and the location specified in the query.
- Time Requirement: This parameter addresses the temporal aspect by indicating the frequency of data updates for a friend's SDT.
- Additionally, parameters related to similarity are introduced to select friends with more similar characteristics as potential next-hops.
- Service Similarity: This parameter measures the similarity between the requested service and the services a friend can provide. It helps expedite service discovery by connecting nodes with high service similarity.
- Application Similarity: SDTs running similar applications are more likely to be interested in similar services. This parameter considers the similarity between applications run by SDTs.

Each SDT involved in a query can take all these parameters into account to select the next friend in the network and forward the query. The importance of these parameters varies depending on the specific service being sought. These parameters are commonly used for service discovery in SIoT, and further research is needed to fine-tune and test them with real SIoT data to develop an efficient service discovery mechanism.

Sara Ranjbaran,
sara.ranjbaran@aalto.fi
Claudio Marche,
claudio.marche@unica.it