TCSN Newsletter – Issue Eleven – April 2023
Social Networks Technical Committee
Editor: Prof. Claudio Marche

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 Eleven – April 2023
Social Networks Technical Committee
Editor: Prof. Claudio Marche

SOCIAL MEDIA AND CYBERSECURITY: THE HUMAN, AN ASSET TO BE EXPLOITED?

FLORENCE SÈDES
FULL PROFESSOR, IRIT LABORATORY
UNIVERSITY OF TOULOUSE, FRANCE

As a Online Social Network (OSN), Twitter has become the main target for spamming activities such as phishing legitimate users or spreading malicious software, which introduces new security issues and waste resources. Therefore, as many other researchers, we have developed various machine-learning algorithms to reveal Twitter spam. Another aspect of social media is the Social Internet of Things (SIoT), i.e. integrating the social component into Internet of Things (IoT), rising to compete to offer a variety of attractive services. Some of them resorting to malicious behaviour to spread poor-quality services, perform so-called trust-attacks: one of our proposal on trust management mechanisms is handled to counter these attacks and provide the user with an estimate of the trust.

More generally, many studies address the global cybersecurity ecosystem: geographical and temporal distribution of attacks, typology, data leakage,... OSINT, the Open Source INTelligence, focuses on gathering information from open access sources, blogs, social networks. The objective is to extract from broadcasting media, a cyber-awareness, to make the individual and the collective aware of cybersecurity. Addressing this facet of the human dimension of cyber security, our research focuses on the study of the potential role of the digital media in the propagation of cyberattacks, through mimicry, imitation or other mass effect.

The increase in the volume of cyberattacks is not surprising as more and more users and endpoints are connected to the internet, increasing both the attack surface and the potential victims. Current cybersecurity is mainly reactive, which means that the cybersecurity technologies deployed are designed to react as quickly as possible to a security incident which will happen sooner or later. The constant state of alert and the increase in the volume of cyberattacks create fatigue among cybersecurity operators in charge of monitoring and handling security incidents triggered by cyberattacks. In order to adopt a holistic approach, it is essential to invest in prevention, in addition to the “reactive” paradigm. There are several approaches, including increased training for users to increase their skills on the subject.

This investigation is based on our consolidated previous contributions on the vast area of media, OSN and SIoT. Based on these expertises, well aware of the essential steps of prevention, we focus on solutions to extend it to more traditional media. Indeed, training and prevention being the first step towards security awareness, we study various use cases to formalize it.

In order to comply with sustainable requirements and the 17 SDG of UN, among which gender equality, we aim at measuring the digital societal footprint of our research, i.e. access to knowledge for all, whatever the gender is, appropriation and awareness, providing measurement methods and tools, collaboration, transparency and equity in the entire ecosystem.

Taking these theoretical and operational limits into account, our research rely on the deployment of holistic analysis methodologies, the measurement of the impacts associated with assets, data sets and data storage, the definition of skills dedicated to measuring and understanding the societal and environmental impacts w.r.t. ethics.

As a data scientist, aware of the evidence that biases must be analysed, elicited and controlled, I aim to manage by certifying input and output data, complying with inclusiveness and gender equality. These requirements provide the basis of behavioral mining and discovery, associated with formal methodologies, based on the analysis of the good practices, associated with the creation of quality data sets, which are still lacking in this research area.

Malicious human behaviour prevention in information system is a key issue: how to strengthen security through education, training and awareness?

Florence Sedes,
florence.sedes@irit.fr

IEEE COMMUNICATIONS SOCIETY

TCSN Newsletter – Issue Eleven – April 2023

Social Networks Technical Committee

Editor: Prof. Claudio Marche

SMART CAMPUSES AS COMPLEX ADAPTIVE SYSTEMS TO ACHIEVE COMFORT AND ENERGY EFFICIENCY: A PROPOSAL

VÍCTOR CABALLERO

ASSOCIATE PROFESSOR, RESEARCH GROUP ON SMART SOCIETY

LA SALLE - UNIVERSITAT RAMON LLULL, BARCELONA, SPAIN

XAVI SOLÉ-BETETA

RESEARCHER, RESEARCH GROUP ON SMART SOCIETY

LA SALLE - UNIVERSITAT RAMON LLULL, BARCELONA, SPAIN

ANNA CARRERAS-COCH

ASSOCIATE PROFESSOR, RESEARCH GROUP ON SMART SOCIETY

LA SALLE - UNIVERSITAT RAMON LLULL, BARCELONA, SPAIN

JOAN NAVARRO

ASSOCIATE PROFESSOR, RESEARCH GROUP ON SMART SOCIETY

LA SALLE - UNIVERSITAT RAMON LLULL, BARCELONA, SPAIN

AGUSTÍN ZABALLOS

FULL PROFESSOR, RESEARCH GROUP ON SMART SOCIETY

LA SALLE - UNIVERSITAT RAMON LLULL, BARCELONA, SPAIN

Smart cities are complex systems. These complex systems are constituted by heterogeneous elements that interact with each other (endogenous to the system) and their environment (exogenous to the system). The level of complexity of smart cities and their ability to achieve urban sustainability has called for debate: complexity is hard to understand and manage, and adding smartness to complexity increases complexity and requires more energy. There is the acknowledgment that smart campuses are like small smart cities, which renders smart campuses plausible to be frame-reduced models to understand the complexity of smart cities.

Under the umbrella of complexity theory lies the framework of Complex Adaptive Systems (CAS). CAS refers to systems made up of many components, often termed agents, that interact, learn, and adapt. The agents in a Smart Campus (SC), such as the teaching and learning community, facility managers, and energy providers, are adaptive, and the system itself is a complex collectivity of self-similar, interactive, adaptive agents. Properties such as self-similarity, complexity, emergence, and self-organization make CAS an ideal framework for researching sustainable comfort in educational environments.

Some authors also view the Internet of Things (IoT), an enabling technology for SCs and smart cities, as a complex system. To illustrate our modeling approach for SCs, we consider increasing students' comfort and energy efficiency. We place an agent –responsible for sensing the different properties of students and classrooms through IoT sensors, gathering contextual information, and taking action to achieve the desired level of comfort and energy efficiency through IoT devices— in each space (e.g., classroom). This means that agents are allocated across the campus.

Agents in a multi-agent system cooperate to achieve a common goal and usually to optimize it. For instance, the agent in a classroom sets a goal of achieving a particular level of comfort and energy efficiency, given, for example, the number and preferences of students present. To reach this goal, the agent needs to take action. Additionally, the environment in which the agent is situated may be altered by other agents and exogenous factors. Alterations by other agents can be due to their operations in other areas (e.g., on the same floor or building), and changes by external factors can be due to weather conditions, for example.

To characterize the hierarchical structure of the system composed of IoT devices and agents (the latter, "guardians"), we include an additional higher-level module, the "wise module", providing a decision support system. This means that the IoT devices, the guardian modules, and the wise module have a hierarchical relationship; IoT devices situated at the bottom, the wise module at the top. IoT devices are deployed in a zone or section of a smart campus building, and the guardian uses these devices to perceive and act on the physical world. This creates a one-to-many relationship between the guardian and the IoT devices. Meanwhile, the wise module is connected to the guardians in a one-to-many relationship that communicate with the decision support system (in the wise module) to coordinate their actions and ensure they work together towards a common goal: increasing students' comfort and energy efficiency.

Application Of Social Internet Of Things As A Framework To Tackle Complexity

The Social Internet of Things (SIoT) enables a network structure that is both scalable and flexible and allows IoT devices to become part of a social network to find the necessary services to achieve their goal. The search is determined by the trust, both subjective and objective, assigned to each thing. In a SC, sensors and actuators may be placed in key locations such as classrooms. Following the SIoT relationships, sensors and actuators in a classroom form social connections with each other, either due to their location (co-location relationships) or because of their need to collaborate and work together towards a particular objective (co-work relationships). A hierarchical relationship is created by having an agent per classroom (the guardian), with the agent on top and the sensors and actuators (things) at the bottom.

The presence of mobile agents (e.g., students) should also be noted. Students' comfort preferences and profiles influence the energy efficiency and comfort goals of the classroom –they are considered

"new" agents that are part of the classroom. As expressed through their preference profiles for comfort, their preferences form a co-work relationship with the guardian and work together to achieve comfort and energy efficiency in the classroom.

So far, we have focused on students' comfort and only tackled energy efficiency sideways. Energy efficiency can be concretely measured via IoT devices and smart meters when understood as energy consumption of concrete appliances (e.g., HVAC or the electricity network covered by the smart meter). However, and as stated previously, achieving comfort and energy efficiency on precise locations may affect other locations, therefore the need for the wise module to understand and act upon such affects and effects. The flow of information is hierarchical, from IoT devices, to guardians, to the wise module.

Once the wise module "understands" these affects and effects (usually as correlations, but preferably as causations), the system (IoT devices, guardians and wise module) would be ready to create meaningful co-work relationships between agents that effect and affect each other. Then, the wise module would be able to offload its responsibility for optimizing comfort and energy efficiency to the guardians and the system would shift towards decentralisation.

Víctor Caballero,
victor.caballero@salle.url.edu
Xavi Solé-Beteta,
xavier.sole@salle.url.edu
Anna Carreras-Coch,
anna.carreras@salle.url.edu
Joan Navarro,
joan.navarro.caballero@salle.url.edu
Agustín Zaballos,
agustin.zaballos@salle.url.edu

TCSN Newsletter – Issue Eleven – April 2023
Social Networks Technical Committee
Editor: Prof. Claudio Marche

TOP EMERGING TECHNOLOGY TRENDS AND THEIR IMPACT IN OUR LIFE

FARHAN AMIN

ASSISTANT PROFESSOR, DEPARTMENT OF INFORMATION AND COMMUNICATION ENGINEERING
YEUNGNAM UNIVERSITY, GYEONGSAN, REPUBLIC OF KOREA

Emerging technologies are new and rapidly evolving technologies that have the potential to transform various aspects of our lives. The Internet of Things (IoT), Social Internet of Things (SIoT), and Big Data are key examples of emerging technologies that have been growing in popularity and importance in recent years.

IoT refers to the network of interconnected physical devices, vehicles, and other objects that are embedded with sensors, software, and network connectivity, allowing them to exchange data and be remotely monitored and controlled. This technology has the potential to transform various aspects of our daily lives, from home automation and transportation to healthcare and energy efficiency. The key concerns of IoT security, scalability, interoperability, and privacy.

SIoT refers to the integration of social networking technologies with IoT devices or it works as a cluster between IoT and social networks. SIoT is a new paradigm that enables IoT devices to share information and interact with users through social media channels. For example, Smart homes can use SIoT to automate various tasks, such as adjusting lighting and temperature based on user preferences, monitoring energy usage, and controlling security systems. Social networks can also be used to connect smart homes with other homes and devices, allowing users to share information and collaborate on tasks. The idea behind SIoT is to enhance the capabilities of IoT devices by leveraging social media and community interactions. This can lead to new and innovative ways of using IoT devices, as well as improved user experiences and engagement. However, there are also concerns around the privacy and security implications of integrating social media with IoT devices, as personal data may be shared more widely and potentially put users at risk. It is important to address these concerns in order to fully realize the potential of SIoT.

Big data is a term used to describe large and complex data sets that require advanced tools and techniques to analyze and process. While big data can offer valuable insights and opportunities for businesses and organizations, it also presents several issues and challenges. Here are some of the most common issues in big data:

1. Volume: Big data is characterized by its sheer volume, which can make it difficult to store, manage, and process. Traditional data management tools and techniques may not be sufficient to handle the volume of data, requiring specialized hardware and software.

2. Velocity: Big data is also characterized by its velocity or the speed at which it is generated and needs to be processed. Real-time data processing and analysis can be challenging, requiring advanced technologies and infrastructure.

3. Variety: Big data comes in various formats, including structured, semi-structured, and unstructured data. This variety can make it challenging to integrate and analyze data from multiple sources.

4. Veracity: Big data can also be characterized by its veracity, which refers to its accuracy and reliability. Incomplete or inaccurate data can lead to incorrect insights and decisions.

5. Privacy and Security: Big data can contain sensitive information, which can pose privacy and security risks. It's essential to implement robust security measures to protect data from unauthorized access or misuse.

6. Cost: The hardware, software, and infrastructure required to manage and analyze big data can be expensive, making it challenging for smaller organizations to invest in this technology.

Although these emerging technologies has pros and cons but these echnologies having a significant impact on our daily lives. Here are some examples:

1. IoT: Smart homes and smart cities are becoming more common with the use of IoT devices such as smart thermostats, lighting, and security systems. IoT is also being used in healthcare to monitor patients remotely, in agriculture to optimize crop yield and resource usage, and in transportation to improve efficiency and safety.
2. SIoT: SIoT is creating new opportunities for social interaction and collaboration through the shared use of IoT devices. For example, communities can use shared sensor networks to monitor air quality, noise levels, and traffic patterns, which can inform urban planning decisions and improve quality of life.
3. Big Data: Big data is being used in various industries to inform decision-making processes. In healthcare, big data is being used to develop personalized treatment plans and to identify disease patterns. In finance, big data is being used to identify investment opportunities and to detect fraud. In transportation, big data is being used to optimize routes and improve safety.

Overall, these emerging technologies are transforming the way we live and work, and are expected to continue shaping our lives in significant ways in the years to come. While these technologies offer many benefits, it is also important to address issues around privacy, security, and ethical implications to ensure that they are used responsibly and for the benefit of society as a whole.

Farhan Amin,

farhanamin10@hotmail.com