ACM Journals

CALL FOR PAPERS

ACM Transactions on Sensor Networks

Special Issue on Resiliency for AI-enabled Smart Critical Infrastructures for 5G and Beyond

Guest Editors:

- **Prof. Laizhong Cui**, Shenzhen University, China, Email: cuilz@szu.edu.cn
- **Dr. Yulei Wu**, University of Exeter, UK, Email: Y.L.Wu@exeter.ac.uk
- **Prof. Ryan Ko,** University of Queensland, Australia, Email: ryan.ko@uq.edu.au
- **Alex Ladur,** CTEK – Combined Technologies Ltd, New Zealand, Email: Alex.Ladur@ctek.co.nz
- **Prof. Jianping Wu**, Tsinghua University, China, Email: jianping@cernet.edu.cn

Modern critical infrastructures are becoming more and more important to defense against extreme threats, such as extreme weather disasters or terrorist attacks. Protecting critical infrastructures and making them behave smartly resilient will play an essential role in our future ecosystems. However, smart critical infrastructures face many challenges, 1) thousands of devices are integrated, resulting in scalability issues; 2) various devices, e.g., machines, sensors, cameras and other Internet of Things (IoT) devices, are exposed to security risks; 3) infrastructure failures happen now and then, causing reliability problems; 4) IoT devices usually have limited battery life and low computing power.

5G and B5G (Beyond 5G) create opportunities for smart critical infrastructures. They will provide the necessary transmission speed, latency and connectivity to improve the scalability, security and reliability issues of existing infrastructures, and enable a new generation of applications for smart critical infrastructures. In addition, 5G/B5G supports emerging and advanced networking paradigms, e.g., software-defined network (SDN), network functions virtualization (NFV), network slicing and multi-access edge computing (MEC), which are potential techniques to improve the flexibility and performance of critical infrastructures. For example, SDN/NFV can be used to improve the reliability of critical infrastructures, and MEC can be adopted to reduce latency of critical applications.

However, the introduction of new technologies makes the system more complex to manage. For example, SDN/NFV collects massive information from the infrastructures and needs to manage an ascending order of magnitude of networking components, and MEC creates thousands of tiny datacenters at the edge, which are more difficult to manage. The complexity makes the existing infrastructure more difficult to manage, which also makes it more vulnerable. To solve the complexity problems and make critical infrastructures self-adaptive under dynamic environments, AI-enabled solutions point the way to future development. For example, AI-enabled solutions can schedule computing and slicing resources more intelligently, to improve network performance and user experience for critical applications.

Although introducing AI-enabled solutions into 5G and B5G improves the flexibility and performance of critical infrastructures, it brings more energy consumption. 5G will double or triple energy consumption for mobile operators, e.g., 5G base stations produce more energy consumption. The problem would get worse with the additional communications and computation for AI-enabled solutions. Given that IoT devices have limited battery life, AI-enabled solutions shall deeply take energy consumption factors into considerations. Improving energy efficiency is the one of the key factors for the success of AI-enabled smart critical infrastructures.
This special issue is devoted to the most recent developments and research outcomes addressing the related theoretical and practical aspects on resiliency for AI-enabled smart critical infrastructures. It also aims to provide worldwide researchers and practitioners an ideal platform to innovate new solutions targeting at the corresponding key challenges.

Topics

Suggested topics include, but are not limited to the following:

- 5G and B5G for resilient smart IoT critical infrastructures
- Network slicing for resilient smart IoT critical infrastructures in 5G and B5G
- Applications of AI and wireless communications in resilient smart critical infrastructures
- QoS-driven resilient smart critical infrastructures for 5G and B5G
- AI-enabled orchestration and control of network slicing for resilient smart critical infrastructures
- AI-enabled management and resource scheduling of MEC for resilient smart critical infrastructures
- Experiments and deployment of resilient smart critical infrastructures for 5G and B5G
- Trust, security and privacy of resilient smart critical infrastructures for 5G and B5G
- Digital twin environments and representative datasets for AI research in resilient smart critical infrastructures for 5G and B5G
- Ethical issues of resilient smart IoT critical infrastructures

Important Dates

- Submission deadline: 1 October 2021
- First-round review decisions: 1 January 2022
- Deadline for revision submissions: 1 March 2022
- Notification of final decisions: 1 May 2022
- Tentative publication: Third quarter, 2022

Submission Information

Submissions to the special issue will be screened by the Special Issue Editors to ensure that they conform to the quality standards of ACM Transactions on Sensor Networks (TOSN). Papers that do not pass this initial screening will be immediately returned to the authors. Reviewers will apply those standards in forming recommendations for acceptance, revision, or rejection. Papers should be formatted with TOSN style (https://dl.acm.org/journal/tosn/author-guidelines). The submission deadline is October 1, 2021. The prospective contributors should submit their papers directly to the online submission system (https://mc.manuscriptcentral.com/tosn). In addition, Authors please choose the Special Issue (Resiliency for AI-enabled Smart Critical Infrastructures for 5G and Beyond) in the online submission.

For questions and further information, please contact Prof. **Laizhong Cui, cuilz@szu.edu.cn**