ACM Journals

CALL FOR PAPERS

ACM Transactions on Sensor Networks

Special Issue on Cyber-Physical Security and Zero-Trust

Guest Editors:

- **Fangyu Li**, Beijing University of Technology, fangyu.li@bjut.edu.cn.
- **WenZhan Song**, University of Georgia, wsong@uga.edu.
- **Xiaohua Xu**, University of Science and Technology of China, xiaohuaxu@ustc.edu.cn

The proliferation of smart sensing, pervasive computing, fog/cloud computing, sensor networks has promoted the development of Cyber-Physical Systems (CPS). However, in the meanwhile, the cyberattack risks are significant and real. Security and risk management have become major concerns for the critical infrastructure. Trust and related topics, such as privacy, security situational awareness, access control, identity authentication, access behavior analysis, etc., are being discussed. The crux of the problem is that traditional network-centric, point solution security tools are no longer sufficient to combat the speed and complexity of today's cyberattacks. In order to coordinate and incentivize the long tail of computing, service, data and content providers of the all kinds of distributed applications, zero-trust and permissionless networks should be identified as a primary kind of security solution for operations in future CPS systems. This paradigm has led to moving network security solutions beyond a perimeter or firewall to approaches that prevent unauthorized access to data and services through enforcing an advanced access control.

In the process of building a trust-based sensor network model, huge amounts of complex and multi-featured data and flexible data sharing enabling zero-trust data management through its life-cycle, from data collection, storage, to computing, bring great challenges. In summary, gathering novel research works related to emerging theories, techniques, and algorithms in trust mechanism within CPS security monitoring is the main purpose of this special issue. We encourage the submissions with new mechanisms, protocols, methods, infrastructures, results, applications and solutions in multiple related disciplines, such as secure and reliable CPS structure, privacy-aware distributed algorithms, distributed heterogeneous data analytics, distributed optimization, sensor networks, end-edge-cloud architecture, to support the trust implementation and cybersecurity in the CPS systems.

Topics

This special issue aims to bring researchers and practitioners in academia and industry together to present their cutting-edge research and engineering findings with emphasis on novel techniques to ensure the CPS security and implement zero-trust paradigm. Topics of interest include, but not limited to:

- CPS Security Architectures and Platforms
- Secured CPS Systems and Case Studies
- Real-Time CPS Security Analytics
- Zero-trust Network Models and Paradigms
- Optimization Algorithms for Secured CPS Systems
- CPS Security Solutions in Edge Computing
- Security and Privacy Threats to CPS Applications
- Accountability and Trust in CPS Applications
- Communication-Efficient Distributed AI Algorithms

- Efficient Privacy-Preserving & Secure AI Algorithms
- Applications of Zero-Trust in Ubiquitous Computing
- Applications of Zero-Trust in Health-care
- Applications of Zero-Trust in Finance & E-commence
- Applications of Zero-Trust in Distributed Sensor Networks

Important Dates

- Submissions Open: May 15, 2022
- Submissions deadline: August 31, 2022
- First-round review decisions: October 31, 2022
- Deadline for revision submissions: December 31, 2022
- Notification of final decisions: February 28, 2023
- Tentative publication: Middle 2023

Submission Information

For questions and further information, please contact **Fangyu Li at fangyu.li@bjut.edu.cn.**