The 1st International Workshop on Networked Sensing Systems and Security (NSSS-2025)

To be held in conjunction with IEEE TrustCom-2025, 14-17 November, 2025, Guiyang China

Introduction

==========

With the rapid proliferation of Internet of Things (IoT), cyber-physical systems, and smart environments, networked sensing systems have become ubiquitous in our daily lives. These systems collect, process, and transmit vast amounts of data from physical environments to digital platforms, enabling applications ranging from smart cities and healthcare to industrial automation and environmental monitoring. The evolution of sensing technologies, communication protocols, and data processing techniques has created exciting opportunities for innovation while also introducing significant challenges in system design, deployment, and security.

Networked sensing systems encompass a wide range of technologies, architectures, and applications, from traditional wireless sensor networks to emerging distributed sensing paradigms. These systems face unique technical challenges related to energy efficiency, scalability, reliability, and interoperability. Additionally, they encounter security threats due to their physical exposure, resource constraints, diverse communication protocols, and integration with critical infrastructure. The security vulnerabilities in these systems can lead to severe consequences, including privacy breaches, data manipulation, service disruption, and even physical harm.

This workshop will address both the important advances in networked sensing systems design and implementation, as well as the critical security and privacy challenges that impact their effectiveness. By bringing together researchers and practitioners from academia and industry, we aim to facilitate the exchange of cutting-edge ideas and experiences across the full spectrum of sensing systems research. The workshop seeks to foster collaboration across multiple disciplines including computer science, electrical engineering, cybersecurity, and application domains, focusing on both fundamental technological advances and practical security solutions for real-world deployments.

Topics of Interest

Topics of interest include but are not limited to:

Networked Sensing Systems

- Novel architectures for networked sensing systems
- Energy-efficient sensing and communication techniques
- Distributed and collaborative sensing approaches
- Mobile and wearable sensing systems
- Underwater, underground, and aerial sensing networks
- Data fusion and aggregation in heterogeneous sensing systems
- Quality of service in networked sensing
- Fog/edge computing for networked sensing
- Machine learning and AI for sensing data analytics
- Time synchronization in distributed sensing systems
- Deployment strategies for networked sensors
- Self-organizing and autonomous sensing networks

- Sensing as a service (SaaS) platforms
- Emerging sensing technologies and applications
- Resource management in sensing networks
- Internet of Things (IoT) sensing infrastructures
- 5G/6G-enabled sensing systems
- Testbeds and experimental platforms for sensing research

Sensing Systems Security

- Security architectures for networked sensing systems
- Intrusion detection and prevention in sensing networks
- Trust management in collaborative sensing environments
- Privacy-preserving sensing and data collection
- Lightweight security protocols for resource-constrained sensing devices
- Physical layer security for sensing systems
- Side-channel attacks and defenses in sensing systems
- Hardware security for sensing devices
- Authentication and access control in distributed sensing
- Security for crowd-sensing and participatory sensing
- Resilience against denial of service attacks in sensing networks
- Energy-efficient security solutions for battery-powered sensing devices
- Secure firmware updates for sensing devices
- Privacy and security in environmental monitoring systems
- Security for vehicular sensing networks
- Sensing security for smart cities and intelligent transportation
- Standardization and compliance for secure sensing systems
- Blockchain and distributed ledger technologies for sensing security

Applications and Case Studies

- Smart cities and urban sensing
- Environmental and agricultural monitoring
- Healthcare and medical sensing applications
- Industrial sensing and IIoT applications
- Vehicular and transportation sensing systems
- Smart home and building management
- Underwater and maritime sensing applications
- Energy management and smart grid sensing
- Emergency response and disaster management
- Human activity recognition and context-aware sensing
- Case studies and real-world deployments of sensing systems

Important Dates

==========

- Submission Deadline: before **August 1st, 2025**
- Authors Notification: **October 1st, 2025**
- Camera-Ready Paper Due: **October 15th, 2025**
- Registration Due: **October 21st, 2025**

Paper Submission Guidelines

==========

Prospective authors are invited to submit manuscripts reporting original unpublished research and recent developments in the topics related to the workshop. The length of the papers should not exceed 6 pages + up to 2 pages for overlength charges (IEEE Computer Society Proceedings Manuscripts style: two columns, single-spaced, 10-point font), including figures and references.

The template files for LATEX or WORD can be downloaded: [IEEE Template Link]

Papers should be submitted through the conference submission system: [Submission Link TBD]

All papers will be peer-reviewed and the comments will be provided to the authors. Once accepted, the paper will be included in the IEEE conference proceedings published by IEEE Computer Society Press (indexed by EI).

Submission of a paper should be regarded as an undertaking that, should the paper be accepted, at least one of the authors will register for the conference and present the work.

Organizing Committee

==========

General Chair

Tianyue Zheng, Southern University of Science and Technology, China (zhengty@sustech.edu.cn)

Program Co-Chairs

Chao Cai, Huazhong University of Science and Technology, China (chriscai@hust.edu.cn)

Huangxun Chen, Hong Kong University of Science and Technology (Guangzhou), China (chen.huangxun.amy@gmail.com, huangxunchen@hkust-gz.edu.cn)

Jinyang Huang, Hefei University of Science and Technology, China (hjy@hfut.edu.cn)

Jingzhi Hu, Imperial College London, United Kingdom (jingzhi.hu@imperial.ac.uk)

Hong Jia, University of Melbourne, Australia (hong.jia@unimelb.edu.au)