Security and Privacy for Internet of Drones (IoD-Security 2024)

in conjunction with IEEE IWCMC 2024

Website: http://iwcmc.org/2024/

Submission Link: **https://edas.info/newPaper.php?c=31475**

Technically sponsored by IEEE and IEEE Cyprus Section

May 27-31, 2024, Cyprus

Chairs

Houbing Song, University of Maryland, Baltimore County, USA
Constandinos Mavromoustakis, University of Nicosia, Cyprus
Jordi Mongay Batalla, Warsaw University of Technology

Scope

Unmanned Aerial Vehicles (UAVs), also termed drones, are extensively being adopted for a wide variety of applications such as traffic surveillance, disaster management, rescue operations, and environment monitoring. With the adoption of IoT, UAV networks are quickly transforming into the Internet of Drones (IoD) paradigm. This has opened up opportunities for the exploration of more sophisticated UAV applications. Yet, the success, prosperity, and advancement of IoD strongly depend on the security, privacy and trust of the IoD as well as the sensitive data being exchanged. While these technologies offer a lot of new possibilities, the increasing complexity of hardware and software as well as the worldwide access increase the vulnerability to security attacks. There is an urgent need to develop novel tools that will constitute the heart of a much-needed science of security for IoD and will assist in building resilient, secure, and dependable IoD. The goal of the IoD-Security 2024 workshop is to bring together internationally leading academic and industrial researchers in an effort to identify and discuss the major technical challenges and recent results aimed at addressing all aspects of security and privacy for IoD.

To ensure complete coverage of the advances in this field, the IoD-Security 2024 Workshop solicits original contributions in, but not limited to, the following topic areas:

- Security, Privacy and Trust for IoD Systems especially as applied to critical infrastructures like renewable energy, manufacturing, building energy systems, oil and gas, natural gas, water, etc.
- Secure IoD architectures, vulnerabilities in IoD systems, and data Security and Privacy in IoD
- Detecting and preventing attacks in IoD
- Evaluation of the Threats, Attacks and Risks in IoD
- Game theory for IoD security
- Security and Privacy in IoD applications and services (health care, smart cities, smart grid, safety and surveillance systems, connected car and transportation systems, etc.)
- Network-distributed signal processing for security solutions in IoD
- Joint security and privacy aware protocol design
- Test-bed and performance metrics of security solutions in IoD
- Deployment and performance studies of secure IoD
- Secure network control systems for IoD applications
- Secure implementation of IoD and architectures for secure hardware/software IoD systems.

Important Dates

The same deadlines as those of the main conference.

Note: Within this workshop, there will be a Best Paper Award.