Sustainable Communications for Renaissance

Call for Papers

2nd International Workshop on CyberNet: Cyber-Physical Security in Mission-Critical Tactical Networks

SCOPE

Over the past few decades, evolving information and communications technology has been crucial for military operations. It is now possible to gather, transmit, store, analyze, and distribute data more quickly and efficiently due to the advancements in the field of sensors, computers, and wireless communications. As a result, command and control, intelligence, targeting, and logistical capabilities have all been enhanced and expanded. Thus, the current communication infrastructures are mostly getting replaced with rapidly deployable tactical networks (TN).In addition to being rapidly deployable and dependable, the ideal tactical network of the future should enable militaries to have access to state-of-the-art applications. With the 3GPP-specified 5G and beyond, TN gives access to applications such as remote controlled devices, video-based group communications, augmented situational awareness and unmanned vehicles. These applications are expected to be enabled by edge computing, a technology that will function with the TN to deliver compute, caching, sensing, and control services to a huge number of Internet of Things (IoT) and Internet of Battlefield Things (IoBT) devices in addition to traditional communication services. However, due to the increasing interdependencies and complexity of networked systems, the enormous amounts of data that are generated continuously, changing non-technical requirements, and evolving adversary threats, maintaining cyber security in command and control systems of TN is a challenging task. Additionally, the number of possible threat actors grows as TN are linked to commercial networks, connect heterogeneous IoT devices, and facilitate collaboration across various authority bodies. To counter cybersecurity risks, a number of Artificial Intelligence (AI)-based detection methods have been developed. Although AI-based cybersecurity systems have shown good results when applied to traditional enterprise networks, there is still a sizable gap in their dependability and resilience when it comes to the capability of attack detection in TN. In addition, AI-based systems are vulnerable to a variety of attacks and threats, including adversarial and backdoor attacks, on both the data and model levels, according to recent studies. These results point to a pressing need for pertinent research on dependability and resilience of AI-based cybersecurity solutions in TN. Finally, TN are vulnerable to supply-chain attacks, electro-magnetic cyber-attacks, and security breaches. Thus, designing and creating intelligent cybersecurity systems for TN becomes important. The proposed workshop is dedicated to the most current advancements and research findings on cybersecurity for mission-critical TN. It also seeks to give scholars and practitioners from all over the world a perfect platform to develop fresh approaches that specifically address the relevant major concerns.

TOPICS OF INTEREST

We seek original completed and unpublished work not currently under review by any other journal/ magazine/conference. Topics of interest include, but are not limited to:

- New Architecture, Design and Implementation for Cybersecurity in TN
- Network Science for Embedding Cybersecurity in Mission-Critical TN
- Security and Information Assurance in Mission-Critical TN
- Artificial Intelligence for Cybersecurity Provisioning in Mission-Critical TN
- Cybersecurity for software defined TN
- Cross-layer security architectures/technologies for Mission-Critical TN
- Game-theoretic security approaches for Mission-Critical TN
- Public key infrastructure, Trust and authentication for Mission-Critical TN
- Blockchain based security and privacy applications for Mission-Critical TN
- Cyber deterrence strategies for Mission-Critical TN
- Intrusion detection, prevention, and response for Mission-Critical TN
- Named Data Networking for Cybersecurity in Mission-Critical TN
- Cross-layer Optimizations for Cybersecurity Provisioning in Mission-Critical TN
- Knowledge Fusion for Cybersecurity in Mission-Critical TN
- Multi-agent and Distributed System for Cybersecurity in Mission-Critical TN
- Cognitive Modelling for Cybersecurity provisioning in Mission-Critical TN
- Other Smart Applications for Cybersecurity in Mission-Critical TN

PAPER SUBMISSION

All papers for Workshops should be submitted via EDAS.
Full instructions on how to submit papers are provided on the IEEE ICC 2023 website: https://icc2023.ieee-icc.org/

WORKSHOP CO-CHAIRS

Sahil Garg
Ultra I&C Communications, Montreal
Email: Sahil.Garg@ultra-tcs.com

Susan Watson
Defence R&D Canada, Ottawa
Email: susan.watson@forces.ga.ca

Satinder Singh
Ultra I&C Communications, Montreal
Email: Satinder.Singh@ultra-tcs.com

Fabrizio Granelli
University of Trento, Italy
Email: fabrizio.granelli@unitn.it

PUBLICITY CHAIRS

Kuljeet Kaur
École de Technologie Supérieure,
Montreal, Canada
Email: kuljeet.kaur@ieee.org

Georges Kaddoum
École de Technologie Supérieure
Montreal, Canada
Email: Georges.Kaddoum@etsmtl.ca

MAIN CONTACT

Sahil Garg
Ultra I&C Communications, Montreal
Email: Sahil.Garg@ultra-tcs.com

IMPORTANT DATES

Paper Submission Deadline:
20 January 2023
Paper Acceptance Notification:
6 March 2023
Camera Ready and Registration for accepted papers:
15 March 2023

WEBPAGE LINK

icc2023.ieee-icc.org