



CALL FOR WORKSHOP

IEEE 36th International Telecommunication Networks and Applications Conference (ITNAC)

November 25-27, 2026, | Melbourne, Australia

WORKSHOP TITLE

Autonomous Security Optimization and Reinforcement Learning in Distributed 5G/6G Cloud-Edge Continuums

SCOPE AND OVERVIEW

As cloud-native environments rapidly transition toward highly distributed architectures spanning public clouds, edge clusters, and upcoming 6G networks, protecting these setups becomes incredibly complex. Traditional position-agnostic security platforms introduce massive operational overhead and communication delays, allowing fast-evolving threats to propagate across multi-tenant boundaries.

This workshop focuses on the convergence of cybersecurity, mathematical optimization, and machine learning to build self-healing, zero-touch network architectures. We invite technical papers exploring how network topology, multi-domain latency, trust dynamics, and computational capacity can transform security orchestration from rigid, centralized workflows into highly dynamic, localized defense mechanisms.

TOPICS OF INTEREST

We welcome submissions addressing theoretical frameworks, algorithmic designs, and real-world implementations, particularly (but not limited to) the following:

- Multi-objective optimization formulations for localized threat containment
- Deep Reinforcement Learning (DQN, PPO) for real-time security steering and mitigation placement
- Context-aware security in softwarized network slicing, NFV MANO, and SDN infrastructures
- Graph-based attack propagation models and real-world testbed evaluations
- Bio-inspired approaches (e.g., L-Systems) and game-theoretic models for anomaly detection

- Topological signal processing and advanced mathematical frameworks for cloud security
- Spatially Aware Game-Theoretic Defense (SA-GTD) models for strategic resource deployment against adaptive attackers
- Intent-based automated mitigation systems for intent-driven security orchestration in virtualized environments
- Lightweight edge-compute security stacks designed for low-overhead deployment in resource-constrained edge nodes
- Adaptive Topological Resonance Transform (TRTA) applications for high-performance anomaly and cyber-attack detection
- AI-assisted zero-trust architectures utilizing real-time mathematical validation for secure network slicing

SUBMISSION GUIDELINES

The length of the paper should be maximum 4 pages including references. Papers must be formatted according to the IEEE conference proceedings manuscript guidelines. Submitted papers must be unpublished and not currently under review elsewhere. All accepted and presented papers will be published in the ITNAC 2026 Workshop Proceedings and submitted to IEEE Xplore.

IMPORTANT DATES

- Workshop Paper Submission: September 10, 2026
- Notification of Acceptance: October 1, 2026
- Camera-Ready Paper Due: October 20, 2026
- Workshop Date: November 25, 2026

WORKSHOP CHAIR

Prof. Alessandro Carrega
University of Genoa & CNIT, Italy
Contact: alessandro.carrega@unige.it