2026 IEEE 26th International Conference on Communication Technology

OCTOBER 16-18, 2026 | **ZHUHAI, CHINA**

Special Session 2

AI-Driven Network Security and Intelligent Threat Detection

As communication networks evolve toward 6G, IoT, and cloud-native architectures, the attack surface expands dramatically, making traditional rule-based security mechanisms insufficient against sophisticated, adaptive threats. This special session focuses on cutting-edge research that leverages artificial intelligence to safeguard next-generation communication infrastructures. We invite original contributions on AI-driven intrusion detection, intelligent anomaly analysis, deep learning-based traffic classification, zero-day threat prediction, and autonomous defense mechanisms in mobile, wireless, and edge networks. Topics of interest also include trustworthy AI for security, adversarial robustness of detection models, federated learning for privacy-preserving threat intelligence, and real-time security orchestration in large-scale networks. By integrating advances from AI for communications and network security, this session aims to explore how intelligent threat detection can empower resilient, secure, and high-quality communication systems. We welcome theoretical breakthroughs, novel algorithms, system designs, and practical deployments that address the growing.

Peishun Yan
Nantong University, China

Yuhan Jiang
Nanjing University of Posts and Telecommunications, China

Yu Ding
Zhejiang University of Technology, China

Topic of Interest

- Deep learning-based network intrusion detection and attack classification in large-scale communication network
- Multi-agent reinforcement learning for automated security testing and vulnerability assessment
- Graph neural networks for attack graph analysis and threat propagation modeling
- Real-time anomaly detection in encrypted network traffic using unsupervised learning
- Large language models for automated vulnerability discovery and exploit generation
- Intelligent security orchestration and automated response in software-defined networks
- Adversarial machine learning attacks and defenses on network security systems
- AI-powered malware detection and analysis in IoT and edge computing environments
- Federated learning for collaborative threat intelligence sharing across networks
- Explainable AI methods for interpretable network security decision-making

Important Dates

Submission Due:	2026-July 1st
Notification Due:	2026-July 25
Camera-ready Due:	2026-August 10

Submission

Submission Link:
https://easychair.org/conferences/?conf=icct2026
(Please choose Special Session 2)

Sponsored by | Hosted by | Patrons