

2026年第16届通信与网络安全国际会议



ICCN5

Communication and Network Security

2026年12月19-21日 中国·哈尔滨



Chair

于尧

东北大学

专题2

6G 通信安全与下一代可信系统

6G 通信网络面向全域感知、泛在连接、通感一体、算力互联等全新能力，在带来超高带宽、极低时延与全域智能服务的同时，也面临复杂的安全与可信挑战。网络异构接入、通感融合带来的隐私泄露、AI 赋能通信带来的算法安全、分布式可信架构、跨域身份认证、内生安全机制等关键问题亟待解决。本专题聚焦 6G 通信安全与下一代可信系统，征集相关理论模型、关键算法、原型系统与实践方案，涵盖 6G 内生安全、通感一体化安全、AI-enabled 通信安全、分布式可信架构、隐私保护、抗攻击技术等方向。旨在汇聚国内外学者，交流前沿研究成果，推动 6G 安全技术的发展与落地。

投稿

投稿网址: <https://www.zmeeting.org/submission/iccns2026>

官方咨询邮箱: iccns_secretary@young.ac.cn

※模板下载

- 论文模板:

Word 版: https://iccns.org/acm_template.docx

LaTeX 版: <https://iccns.org/LaTeX-Templates.zip>

- 摘要模板: https://iccns.org/abstract_template.docx

如需了解完整投稿细则，请访问页面: <https://iccns.org/sub.html>

联系方式

联络人: 雷女士

邮箱: iccns_secretary@young.ac.cn

电话: +86-18010667294

微信: 添加账号 iconf-cs-2, 发送 "ICCN5 2026"

主题

征稿主题包括但不限于:

1. 内生安全架构与零信任机制
2. 通感一体化 (ISAC) 安全与隐私保护
3. AI 赋能通信中的算法安全与对抗防御
4. 算力网络与云边协同中的可信计算
5. 空地海一体化网络中的接入认证与信任管理
6. 面向泛在连接的轻量级安全与物理层防护
7. 区块链与分布式账本技术在可信系统中的应用
8. 智能安全感知与自动化响应技术
9. 抗量子密码体制与未来密码迁移策略
10. 数据面与智能面安全及跨域数据治理

重要时间

投稿截止时间: 2026 年 10 月 25 日

录用结果通知: 2026 年 11 月 20 日

终稿提交 / 会议注册截止: 2026 年 12 月 01 日

THE 16TH INTERNATIONAL CONFERENCE ON COMMUNICATION AND NETWORK SECURITY



Communication and Network Security

December 19–21, 2026 Harbin, China



Chair

Yao Yu

Northeastern University, China

Special Session 2

6G Communication Security and Next-Generation Trusted Systems

Introduction: 6G networks deliver brand-new capabilities including ubiquitous sensing, pervasive connectivity, integrated communication-sensing and cross-domain computing services. While offering high-throughput, ultra-low-latency and intelligent applications, 6G also introduces unprecedented security and trust challenges. Critical open issues such as privacy leakage in heterogeneous access and communication-sensing integration, algorithm-level risks from AI-empowered communications, distributed trusted frameworks, cross-domain authentication and intrinsic security mechanisms remain to be addressed. This special session focuses on 6G communication security and next-generation trusted systems. We welcome theoretical models, key algorithms, prototype implementations and practical solutions, covering 6G intrinsic security, communication-sensing integrated security, AI-enabled communication security, distributed trusted architecture, privacy preservation and anti-attack technologies. It aims to gather worldwide researchers to exchange cutting-edge findings and advance the development and deployment of 6G security technologies.

SUBMISSION

→Submission System: <https://www.zmeeting.org/submission/iccns2026>
→Email Submission Address: iccns_secretary@young.ac.cn
*Full Paper Template: https://iccns.org/acm_template.docx;
<https://iccns.org/LaTeX-Templates.zip>
*Abstract Template: https://iccns.org/abstract_template.docx

For more details about submission, please visit <https://iccns.org/sub.html>

TOPICS

- Native Security Architecture and Zero Trust Mechanisms
- Security and Privacy in Integrated Sensing and Communication (ISAC)
- Algorithmic Security and Adversarial Defense in AI Empowered Communications
- Trusted Computing for Computing Power Networks and Cloud Edge Collaboration
- Access Authentication and Trust Management in Space Air Ground Sea Integrated Networks
- Lightweight Security and Physical Layer Protection for Ubiquitous Connectivity
- Blockchain and Distributed Ledger Technologies for Trusted Systems
- Intelligent Security Awareness and Automated Response Technologies
- Post-Quantum Cryptography and Future Cryptographic Migration Strategies
- Data Plane and Intelligent Plane Security with Cross-Domain Data Governance

IMPORTANT DATE

Submission Deadline: October 25, 2026
Notification Deadline: November 20, 2026
Registration Deadline: December 01, 2026

CONTACT

Ms. Lesley Lei (Conference Secretary)
E-mail: iccns_secretary@young.ac.cn
Tel: +86-18010667294 | +86-28-86527868
WeChat: Add iconf-cs-2 and send the keyword ICCNS 2026

Sponsored by



Organized by



Co-organized by

