

2026年第16届通信与网络安全国际会议



2026年12月19-21日 中国·哈尔滨



Chair

涂山山

北京工业大学

专题1: 物联网与空间计算安全

随着物联网终端大规模部署，空间计算技术快速赋能元宇宙、增强现实、室内外高精度定位、数字孪生等场景，物理世界与数字空间深度交融，也催生大量新型安全威胁。异构物联网设备资源受限、空间感知数据泄露、定位欺骗、三维场景篡改、虚实融合系统攻防等问题日益突出，传统网络安全方案难以完全适配此类复杂场景。本专题聚焦物联网与空间计算交叉领域的安全挑战，征集相关理论、算法、系统实现与实测案例，涵盖感知安全、定位抗欺骗、空间数据隐私保护、虚实融合系统攻防、轻量级安全防护等方向。旨在汇聚学界与产业界研究人员，分享前沿成果，促进技术交流与跨领域合作。

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"



Chair

宁振虎

北京工业大学

主题

征稿主题包括但不限于:

- 物联网感知层安全、可信数据采集与异常检测
- AR/VR、元宇宙及数字孪生环境下的安全与隐私保护
- 安全高精度定位、仿真检测与抗干扰技术
- 空间感知、轨迹、点云及三维场景数据的隐私保护
- 三维地图、数字资产和空间内容的完整性与真实性保护
- 智能物理空间系统的攻击建模、威胁检测与协同防御
- 物联网设备的轻量级认证、密钥管理、访问控制与远程可信验证
- 边缘、雾计算与云-边缘设备协同计算的安全保障
- 基于AI的安全分析与空间计算中的对抗鲁棒性

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

Sponsored by



Organized by



Co-organized by



THE 16TH INTERNATIONAL CONFERENCE ON COMMUNICATION AND NETWORK SECURITY



December 19–21, 2026 Harbin, China



Chair

Shanshan Tu

Beijing University of Technology, China

Special Session 1

IoT and Spatial Computing Security

With the large-scale deployment of IoT devices, spatial computing has empowered metaverse, AR/VR, high-precision positioning and digital twin applications. The deep integration of physical and digital spaces brings substantial new security threats. Resource-constrained heterogeneous IoT terminals, spatial-aware data leakage, location spoofing, 3D-scene tampering and attacks on virtual-physical fusion systems cannot be fully addressed by conventional cybersecurity solutions. This special session targets security challenges at the intersection of IoT and spatial computing. We welcome original theoretical research, algorithms, system implementations and practical case studies, including sensing security, anti-spoofing for positioning, spatial data privacy preservation, virtual-physical system attack-defense technologies, and lightweight security mechanisms. It aims to bring together academic and industrial researchers to share cutting-edge progress and foster cross-domain collaboration.

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>

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



Chair

Zhenhu Ning

Beijing University of Technology, China

TOPICS

- IoT sensing-layer security, trustworthy data acquisition, and anomaly detection
- Security and privacy for AR/VR, metaverse, and digital-twin environments
- Secure high-precision positioning, spoofing detection, and anti-jamming technologies
- Privacy preservation for spatial sensing, trajectory, point-cloud, and 3D-scene data
- Integrity and authenticity protection for 3D maps, digital assets, and spatial content
- Attack modeling, threat detection, and collaborative defense for cyber-physical-spatial systems
- Lightweight authentication, key management, access control, and remote attestation for IoT devices
- Security for edge, fog, and cloud-edge-device collaborative computing
- AI-enabled security analytics and adversarial robustness for spatial computing

Sponsored by



Organized by



Co-organized by

