CONFERENCE PROGRAM

2025 15th International Conference on Communication and Network Security (ICCNS 2025)

2025 年第 15 届通信与网络安全国际会议

December 19-21, 2025 | Jilin, China

2025 年 12 月 19 日- 21 日 | 中国吉林

Sponsored by

东北电力大学
NORTHEAST ELECTRIC POWER UNIVERSITY

Organized by

计算机学院
School of Computer Science

Table of Content

Organizing Committee

▶ Advisory Committees
Shigang Chen, IEEE Fellow, University of Florida, USA
Hui Tian, Huaqiao University, China

▶ Conference Chairs
Haizhou Li, The Chinese University of Hong Kong (Shenzhen) & National University of Singapore
Jianpo Li, Northeast Electric Power University, China
Xianhua Niu, Xihua University, China

▶ Conference Co-chairs
Masahiro Fujita, University of Tokyo & National Institute of Advanced Industrial Science and Technology, Japan
Tao Lu, Wuhan University of Technology, China

▶ Program Committee Co-chairs
Krzysztof Szczypiorski Warsaw University of Technology, Poland
Huifang Chen, Zhejiang University, China
Qiushi Zhang, Northeast Electric Power University, China

▶ Program Committee Vice-chairs
Pascal Lorenz, University of Haute Alsace, France
Hongye Zhang, Northeast Electric Power University, China
Zhenrong Zhang, Guangxi University, China

▶ Publicity Co-chairs
Chao Cheng, Changchun University of Technology, China
Arash Habibi Lashkari, York University, Canada
Bobby Barua, Ahsanullah University of Science and Technology, Bangladesh

▶ Track Chairs
Shaoshuai Gao, University of Chinese Academy of Sciences, China
Yanping Zhang, Gonzaga University, USA
Nan Zhao, Dalian University of Technology, China
Yu-Beng Leau, Universiti Malaysia Sabah, Malaysia
Thuan Yew Edward Chuah, University of Aberdeen, UK
Xuru Li, Shanghai Maritime University, China
Mi Wen, Shanghai University of Electric Power, China
Min Luo, Wuhan University, China
Hui Zhu, Xidian University, China
Lijun Zhang, E-surfing Vision Technology Co., Ltd, China Telecom, China

▶ Technical Committees
Paulo Batista, University of Évora, Portugal
KHALDI Amine, Universite Kasdi Merbah Ouargla, Algeria
Qian Lin, Qinghai Minzu University, China
Shaoshuai Gao, University of Chinese Academy of Sciences, China
Qingshui Xue, Shanghai Institute of Technology, China
Gerardo Pelosi, Politecnico di Milano, Italy
Sujata Mohanty, NIT, Rourkela, India
George C. Polyzos, The Chinese University of Hong Kong, China
Chenyuan Feng, University of Exeter, U.K.

Ming Wan, Liaoning University, China
Zhongyuan Qin, Southeast University, China
Zhang Lijun, E-surfing Vision Technology Co., Ltd, China Telecom, China
Gang Liu, Taishan University, China
Jain-Shing Liu, Providence University
Thien Wan Au, Universiti Teknologi Brunei, Brunei Darussalam
Riktesh Srivastava, City University Ajman, UAE
Hui Peng, The Fifth Electronic Research Institute of MIIT, China
E. Prince Edward, Sri Krishna Polytechnic College, India
Yanping Zhang, Gonzaga University, USA
Li Tan, Beijing Technology and Business University, China
Yong Wee Sek, Universiti Teknikal Malaysia Melaka, Malaysia
Peixian Zhuang, University of Science and Technology Beijing, China
Yu-Beng Leau, Universiti Malaysia Sabah, Malaysia
Kocsis Gergely, University of Debrecen, Hungary
Ghada Abdelhady, October University for Modern Sciences and Arts (MSA University), Egypt
Kai Zhou, China Unicom Digital Technology co., Ltd., China
Khondker Shajadul Hasan, University of Houston-Clear Lake, USA
Thuan Yew Edward Chuah, University of Aberdeen, UK
N.Ch.SrimanNarayanaIyengar, Sreenidhi Institute of Science and Technology(SNIST),India
Xuru Li, Shanghai Maritime University, China
Mehmet Hakan Karaata, Kuwait University, Kuwait
Fernanda Otilia Figueiredo, University of Porto, Portugal
Pascal Lorenz, University of Haute Alsace, France
Nahla EL ZANT, CS department at UFAZ university Baku, France
Weiru Wang, Beijing University of Technology, China
Yu-Che Huang, Chaoyang University of Technology
Ljiljana Trajkovic, Simon Fraser University, Canada
Valentina Emilia Balas, University of Arad, Romania
Jonilyn Dabalos, Davao del Norte State College, Philippines
Nimsuk Nitikarn Nimsuk, Thammasat University, Thailand
D.P. Sharma, MAISM under Rajasthan Technical University, India
Homero Toral Cruz, University of Quintana Roo, Mexico
Muhammad Rizwan, University of Derby, UK
Wei Peng, National University of Defense Technology, China
Muhammad Imran Aslam, NED University of Engineering and Technology, Pakistan
Rushit Dave, Minnesota State University, USA
Mehdi Gheisari, Shenzhen BKD Co.LTD, China
Francesco Zirilli, Universita di Roma La Sapienza, Italy
Nikola Ivkovic, University of Zagreb, Croatia
Suwat Pattaramalai, King Mongkut's University of Technology Thonburi, Thailand
Ioan Stefan Sacala, National University for Science and Technology Politehnica Bucharest, Romania
Madihah Mohd Saudi, Universiti Sains Islam Malaysia, Malaysia
June Tay, Singapore University of Social Sciences, Singapore
Mohd Nazri Ismail, National Defence University of Malaysia, Malaysia
Akharin Khunkitti, King Mongkut's Institute of Technology Ladkrabang, Thailand
Saeid Pourroostaei, University of Lincoln, UK
Koorosh Gharehbaghi, RMIT University, Australia
Tse Guan Tan, Universiti Malaysia Kelantan, Malaysia
Ping Guo, University of Illinois at Springfield, USA
Eunice B. Custodio, Bulacan State University, Philippines
Javier Gozalvez, Universidad Miguel Hernandez de Elche (UMH), Spain

Welcome Message

On behalf of the Conference Committees, we welcome you to attend the 2025 15th International Conference on Communication and Network Security (ICCNS 2025), which will be held in Jilin, China during December 19-21, 2025, sponsored by Northeast Electric Power University, China.

ICCNS 2025 welcomes submissions of papers by authors from all branches of communication and network security, as well as their applications and related research areas. The areas covered include, but are not limited to: communication and information engineering, information and network security, data security, privacy protection, etc.

The conference aims to provide an interactive communication platform for practitioners to learn about the most cutting-edge academic and industrial application trends, to share the latest scientific research and technological achievements, innovative ideas and scientific methods in the field of communication and network security, to improve the level of academic research and industrial application in the field of communication, so as to serve the global strategic deployment of the conversion of new and old kinetic energy, and promote technology research, development, and application at home and abroad.

We feel deeply grateful to all who have contributed to making this event possible: authors, the conference steering committee, the conference speakers, and the peer reviewers. Appreciations are also extended to the conference administrative committee and the supporters for their tireless efforts throughout the preparation and organization of the conference.

We hope that all participants benefit from the conference. Your contributions are vital in advancing the frontiers of knowledge and technology.

Welcome to Jilin—enjoy ICCNS 2025!

ICCNS Conference Organizing Committee

December, 2025

Onsite Conference Information

Conference Venue 会址

Northeast Electric Power University 东北电力大学

Address: Northeast Electric Power University, No. 169 Changchun Road, Chuanying District, Jilin, China

地址：吉林市船营区长春路169号东北电力大学

Oral Presentation Tips

- ✓ The duration of a presentation slot is 15 minutes. Please prepare your presentation for about 12 minutes plus about 3 minutes for questions from the audience;
- ✓ An LCD projector & computer will be available in every session room for regular presentations;
- ✓ Presentations MUST be uploaded at the computer at least 15 minutes before the session start.

Dress Code

- ✓ All participants are kindly requested to dress formally, as casual wear is discouraged.
- ✓ National formal dress is welcome.

Attention Please

- ✓ Please ensure the safety of your belongings in public areas. For personal and property security, delegates are advised to wear their identification badges during the conference and refrain from lending them to unauthorized individuals. The conference cannot be held responsible for the loss of personal items.

Emergency Call:

Police: 110

Ambulance: 120

Fire: 119

Average Temperature During the Conference

-11℃ ~ - 2℃

Transportation 交通

From Changchun Longjia International Airport

从长春龙嘉国际机场出发

✓ High-speed Train + Taxi / Bus (1 hour 30 mins, about 50-60 RMB)

✓ 动车 + 出租车 / 公交（1 小时 30 分钟，约 50-60 元）

Walk from Changchun Longjia International Airport to Longjia Railway Station (about 5 mins on foot), take a high-speed train to Jilin Railway Station (30 mins journey, second-class seat 22.5 RMB). Upon arrival at Jilin Railway Station, you can choose:

Taxi: Take a taxi from Jilin Railway Station West Square to Northeast Electric Power University (15 mins, 15-20 RMB).

从长春龙嘉国际机场步行至龙嘉站（步行约 5 分钟），乘坐动车前往吉林站（车程 30 分钟，二等座 22.5 元）。抵达吉林站后，可选择：

出租车：从吉林站西广场打车至东北电力大学（15 分钟，15-20 元）。

From Jilin Railway Station
从吉林站出发

✓ By Taxi (15 mins, 15-20RMB)
✓ 出租车（15 分钟，15-20 元）

Take a taxi from Jilin Railway Station (West Square Exit) to Northeast Electric Power University. The distance is about 6km, the fare is 15-20RMB, and the journey takes 15-20 minutes, avoiding peak hours for faster travel.
从吉林站（西广场出口）乘坐出租车前往东北电力大学。全程约 6 公里，费用 15-20 元，行程时间 15-20 分钟，避开高峰时段可更快到达。

Online Conference Information

Zoom information
ZOOM ID: 82313016185 **ZOOM Link: https://us02web.zoom.us/j/82313016185** **Passcode: 121921**

Time Zone

- ✓ Beijing Standard Time, UTC/GMT+8
- ✓ Please ensure your computer's time zone (and clock) is set to Beijing standard time.

Sign in and Join

- ✓ Join a meeting without signing in: A Zoom account is not required if you join a meeting as a participant, but you cannot change the virtual background or edit the profile picture.
- ✓ Sign in with a Zoom account: All the functions are available.

Additional Suggestions

- ✓ A computer with an internet connection (wired connection recommended)
- ✓ USB plug-in headset with a microphone (recommended for optimal audio quality)
- ✓ Webcam (optional): built-in or USB plug-in
- ✓ Quiet environment
- ✓ Proper lighting

Presentation Tips

Each presentation slot is 15 minutes. Please prepare to speak for around 12 minutes, allowing 3 minutes for audience questions.

Join the meeting room at least 15 minutes before the session begins.

Daily Schedule

December 19, 2025 | Friday

For Onsite Participants	
Venue: Experts' Guest House, Northeast Electric Power University | IF **会址：东北电力大学专家招待所 | 1楼**	
14:00-17:00	Sign in and Collect Conference Materials 签到及领取会议资料

For Online Participants	
ZOOM ID:82313016185 ZOOM Link: https://us02web.zoom.us/j/82313016185 Passcode: 121921	
14:00-17:00	ZOOM Test for Online (Presenters / Session Chairs / Committees) 作者及专家线上测试

Daily Schedule

December 20, 2025 | Saturday

Venue: Hall of the Academic Center, West Campus, Northeast Electric Power University | 1F **会址：东北电力大学校园西区学术中心大厅 | 1楼** **ZOOM ID: 82313016185 | Passcode: 121921**	
08:30-09:00	Sign In & Morning Reception 会议签到
Opening Ceremony	
Host: Prof. Jianpo Li, Northeast Electric Power University, China	
08:30-08:35	**Opening Remarks** **Prof. Dongfeng Yang,** Northeast Electric Power University, China
08:35-09:15	***Keynote Speech I: Intelligent Trust Provisioning and Collaborative Task Completion in the Era of 6G and Generative AI*** **Prof. Xianbin Wang,** Western University, Canada
09:15-09:40	**Coffee Break & Group Photo**
09:40-10:20	***Keynote Speech II: Bio-inspired Converged Network*** **Prof. Yao Yu,** Northeastern University, China
10:20-11:00	***Keynote Speech III: Theory and Methods for Low-Altitude Covert Communication*** **Prof. Nan Zhao,** Dalian University of Technology, China
11:00-11:40	***Keynote Speech IV: Power System Control Driven by Reinforcement Learning*** **Prof. Meng Zhang,** Xi'an Jiaotong University, China
11:40-14:00	**Lunch | Experts' Guest House, Northeast Electric Power University | IF** **午餐：东北电力大学专家招待所 | 1楼**

Author Presentation Sessions		
Venue: Academic Conference Center, West Campus, Northeast Electric Power University | 1F **地址：东北电力大学校园西区学术会议中心 | 1楼**		
14:00-15:30	**Onsite Oral Session 1** **Communication and Information Engineering & Privacy Protection** Session Chair: Prof. Jianxun Lou, Northeast Electric Power University, China CN3037, CN4054, CN4046, CN3040, CN4055, CN4053	**Meeting Room 3 | 1F** **三会议室 | 1楼** **ZOOM ID: 82313016185** **Passcode: 121921**
15:30-15:50	**Coffee Break**	
15:50-17:20	**Onsite Oral Session 2** **Information and Network Security & Privacy Protection** Session Chair: Assoc. Prof. Thien Wan Au, Universiti Teknologi Brunei, Brunei CN1006, CN2018, CN1005, CN2017, CN3044, CN3036	**Meeting Room 3 | 1F** **三会议室 | 1楼**
18:00-20:00	**Dinner | Experts' Guest House, Northeast Electric Power University | IF** **晚餐：东北电力大学专家招待所 | 1 楼**	

Daily Schedule

December 21, 2025 | Sunday

Online Presentation Session		
10:00-11:45	**Online Oral Session 1** **Information and Network Security-1** Session Chair: Assoc. Prof. Zhongyuan Qin, Southeast University, China CN1002, CN2012, CN3034, CN3033, CN4052, CN3035, CN2020	**ZOOM ID: 82313016185** **Passcode: 121921**
11:45-14:00	**Lunch Time**	
14:00-15:30	**Online Oral Session 2** **Information and Network Security-2** Session Chair: Assis. Prof. Muhammad Rizwan, University of Derby, UK CN4047, CN2021, CN3030, CN3042, CN3043, CN2023	**ZOOM ID: 82313016185** **Passcode: 121921**
15:30-15:50	**Break Time**	
15:50-17:20	**Online Oral Session 3** **Communication and Information Engineering, Data Security & Privacy Protection** Session Chair: Prof. Lijun Zhang, E-surfing Vision Technology Co., Ltd, China Telecom, China CN2016, CN2007-A, CN4050, CN4049, CN3029, CN4048	**ZOOM ID: 82313016185** **Passcode: 121921**

Keynote Speaker

Prof. Xianbin Wang,
IEEE Fellow
Fellow of Canadian Academy of Engineering
Western University, Canada

Speech Time: 08:35 - 09:15
(Online) ZOOM ID: 82313016185
Password: 121921
(Onsite) Hall of the Academic Center, West Campus, Northeast Electric Power University | 1F
东北电力大学校园西区学术会议中心大厅 | 1 楼

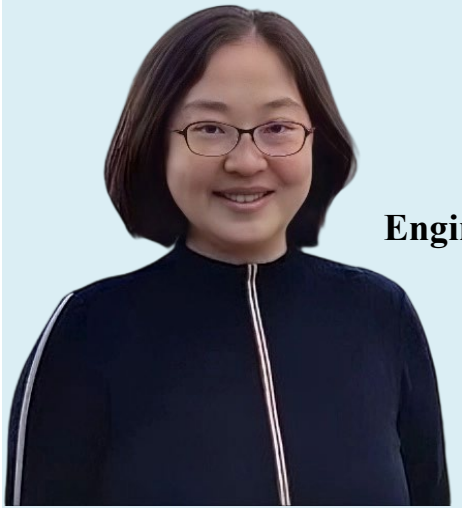
Speech Title: Intelligent Trust Provisioning and Collaborative Task Completion in the Era of 6G and Generative AI

Abstract: The rapid evolution of digital technologies from 1G to 6G, coupled proliferation networked system, has given rise to a wide variety of complex tasks that can only be executed by distributed devices collaboratively. In effectively completing such complex tasks, a core challenge lies in dynamically aligning diverse task-specific requirements with the capabilities, reliability and conditions of potential collaborators through intelligent trust evaluation. This keynote will explore the critical aspects of intelligent trust evaluation and collaborator selection for collaborative task completion. Specifically, this presentation will cover: i) Evolving challenges in trusted collaboration in networked systems, including diverse task requirements, task-specific definitions of trust, and their impact on effective task completion. ii) Key enabling technologies and mathematical frameworks for task-specific trust evaluation, trusted collaborator selection, and effective task completion. iii) Generative AI-driven autonomous trust orchestration, based on a new concept of semantic chain-of-trust. Agentic AI and hypergraph models will be discussed as tools to establish, maintain, and adapt spatiotemporal trust relationships among devices for effective collaboration and task completion.

Bio: Dr. Xianbin Wang is a Distinguished University Professor and a Tier-1 Canada Research Chair in Trusted Communications and Computing with Western University, Canada. His current research interests include 5G/6G technologies, Internet of Things, machine learning, communications security, and intelligent communications. He has over 700 highly cited journals and conference papers, in addition to over 30 granted and pending patents and several standard contributions. Dr. Wang is a Fellow of IEEE, a Fellow of the Canadian Academy of Engineering and a Fellow of the Engineering Institute of Canada. He has received many prestigious awards and recognitions, including the IEEE Canada R. A. Fessenden Award, Canada Research Chair, Engineering Research Excellence Award at Western University, Canadian Federal Government Public Service Award, Ontario Early Researcher Award, and 10 Best Paper Awards. He is currently a member of the Senate, Senate Committee on

Academic Policy and Senate Committee on University Planning at Western. He has been involved in many flagship conferences, including GLOBECOM, ICC, VTC, PIMRC, WCNC, CCECE, and ICNC, in different roles, such as General Chair, TPC Chair, Symposium Chair, Tutorial Instructor, Track Chair, Session Chair, and Keynote Speaker. He serves/has served as the Editor-in-Chief, Associate Editor-in-Chief, and editor/associate editor for over ten journals. He has served on the IEEE Fellow Committee and the Fellow Committee of IEEE Communications Society. He was the Chair of the IEEE ComSoc Signal Processing and Computing for Communications (SPCC) Technical Committee and is currently serving as the Central Area Chair of IEEE Canada.

Keynote Speaker



Prof. Yao Yu,
Northeastern University, China
Director,
Department of Communication and Electronic Engineering, School of Computer Science and Engineering

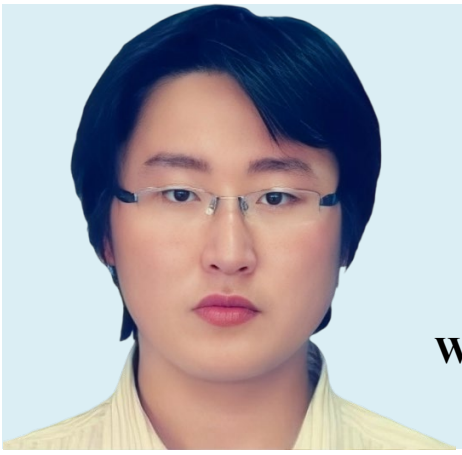
Speech Time: 09:40 - 10:20
Venue: Hall of the Academic Center, West Campus, Northeast Electric Power University | 1F
东北电力大学校园西区学术会议中心大厅 | 1 楼

Speech Title: Bio-inspired Converged Network

Abstract: Future autonomous swarm networks are rapidly evolving toward heterogeneity, intelligence, and large-scale collaboration. However, existing centralized and homogeneous architectures struggle to support cross-domain, cross-platform cooperation under highly dynamic and resource-constrained environments. To address these challenges, we introduce the Bio-inspired Converged Networks (BiCN). This unified framework draws inspiration from the structural, functional, and behavioral mechanisms of biological systems, particularly the immune system's surveillance, response, recognition, and memory processes. BiCN aims to integrate heterogeneous unmanned systems into a collaborative network capable of self-organizing sensing, self-adaptive communication, and self-evolving decision-making. We present three major research directions: the multi-source cooperative sensing for diversified information, the high-efficiency adaptive communication for dynamic environments, and the intelligent consistent decision-making across heterogeneous agents. We further propose immune-inspired approaches for cooperative sensing, efficient communication, and intelligent decision-making, thereby enhancing collaboration among heterogeneous networks. Overall, BiCN provides a bio-inspired framework for building resilient, autonomous, and evolvable networks, supporting future 6G, computing-driven infrastructures, and integrated space–air–ground–sea systems.

Bio: Yao Yu (Senior Member, IEEE) received the B.S. degree in communication engineering and the Ph.D. degree in communication and information system from Northeastern University, Shenyang, China, in 2005 and 2010, respectively. From 2010 to 2011, she was a Postdoctoral Fellow with the Department of Computing, Hong Kong Polytechnic University, Hong Kong, China. She was also a Visiting Scholar with The University of Sydney, Sydney, NSW, Australia, from 2019 to 2020. She is currently a Professor with the School of Computer Science and Engineering, Northeastern University. Her current research interest is intelligent wireless communications.

Keynote Speaker



Prof. Nan Zhao,
Dalian University of Technology, China
Young Changjiang Scholar

Speech Time: 10:20 - 11:00
Venue: Hall of the Academic Center, West Campus, Northeast Electric Power University | 1F
东北电力大学校园西区学术会议中心大厅 | 1 楼

Speech Title: Theory and Methods for Low-Altitude Covert Communication

Abstract: The low-altitude economy is developing rapidly. However, the low-altitude communication environment is complex and variable, facing severe challenges such as co-channel interference, malicious jamming, and risks of unintended detection or intentional interception. Traditional communication technologies, focused primarily on ensuring reliable transmission, struggle to meet the urgent modern low-altitude application demands for being "invisible yet transmitting flawlessly." This presentation will focus on the frontier field of low-altitude covert communication, systematically elaborating on its core theories and key technologies. Building on this foundation, it will provide detailed introductions to key research directions, including air-ground coordination, intelligent reflecting surfaces, integrated sensing and communication, and artificial intelligence for low-altitude covert communication. Finally, the application prospects and development trends of low-altitude covert communication technologies will be discussed.

Bio: Nan Zhao, Professor at Dalian University of Technology, Young Changjiang Scholar of the Ministry of Education, specializing in wireless communication and networks. He has been recognized as a Highly Cited Researcher globally, received the IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award, the Youth Science and Technology Award of the China Institute of Communications, the Liaoning Natural Science Award, and the Technological Invention Award of the China Institute of Communications. His Google Scholar citations exceed 21,000. He has led numerous research projects, including key topics under the National Key R&D Program and the National Natural Science Foundation Regional Joint Key Fund. He has served as an editorial board member for over 10 prestigious international and domestic journals, such as IEEE Communications Surveys & Tutorials.

Keynote Speaker

Prof. Meng Zhang,
Xi' an Jiaotong University, China
National-level Young Talent

Speech Time: 11:00 - 11:40
Venue: Hall of the Academic Center, West Campus, Northeast Electric Power University | 1F
东北电力大学校园西区学术会议中心大厅 | 1 楼

Speech Title: Power System Control Driven by Reinforcement Learning

Abstract: As the complexity of power systems continues to increase, purely model-based control methods struggle to effectively address the control challenges of complex power systems. Therefore, reinforcement learning, as one of the promising data-driven approaches, has been extensively studied and applied to solve these problems. This report first introduces how to leverage Lyapunov theory and stable deep dynamic models to ensure the stability of the system's equilibrium points, and optimizes the model through a deep reinforcement learning architecture to enhance the control performance of grid-forming and grid-connected inverters. Next, a multi-agent deep reinforcement learning framework combining offline training and online learning is designed, a model-free power system control method is proposed, and adaptive multi-area power system cooperative control is realized to address system uncertainties caused by renewable energy sources and other factors. Finally, experimental results demonstrate that the reinforcement learning-driven control method can achieve superior control performance compared with traditional methods under various power grid conditions and disturbances.

Bio: Meng Zhang is a professor and doctoral supervisor at Xi'an Jiaotong University, a Chief Scientist of the National Key R&D Program and young Changjiang Scholar from the Ministry of Education. Meng Zhang obtained his Ph.D degree from the school of control science and engineering of zhejiang university. Meng Zhang has received honors such as the First Prize for Excellent Achievements in Science and Technology Research at Shaanxi Higher Education Institutions, the First Prize for Natural Science at the Chinese Association of Automation, the Outstanding Youth Award for Artificial Intelligence of Wu Wenjun. Meng Zhang has published more than80 papers in journals such as Automatica Full Paper, IEEE TAC Full Paper, IEEE TASE, etc. Meng Zhang serves as an associate editor of IEEE Transactions on Cybernetics, IEEE Transactions on Automation Science and Engineering and the chairman of IEEE IESONCON and other conference industrial forums. Meng Zhang's research directions include intelligent control and optimization with applications to robotics and smart grids.

Onsite Oral Session 1

Communication and Information Engineering & Privacy Protection

- **Session Chair:** Prof. Jianxun Lou, Northeast Electric Power University, China
- **Time:** 14:00-15:30, December 20, 2025 | GMT+8 (Beijing Time)
- **Venue:** Meeting Room 3 | 1F
- **ZOOM ID:** 82313016185| **Password:** 121921
- **Papers:** CN3037, CN4054, CN4046, CN3040, CN4055, CN4053

CN3037 14:00-14:15	LHR-SN: A SuperNet-Aware Layered Hybrid Routing Protocol with Bordercasting Author(s): Tuo Wang, Dong Ke Presenter: Tuo Wang, Wuhan Marine Communication Institution, China **Abstract:** The Super Net represents a specialized form of tactical ad hoc network composed of heterogeneous subnets operating across multiple systems and frequency bands. Tactical and emergency coordination scenarios impose stringent demands for low latency, scalability, and robustness. However, conventional proactive, reactive, and hybrid routing protocols struggle to simultaneously suppress flooding overhead and ensure convergence latency in highly heterogeneous and dynamic environments constrained by subnet boundaries. To address these challenges, this paper proposes LHR-SN: A Super Net-aware Layered Hybrid Routing Protocol. Within each subnet domain, the protocol maintains routes proactively within a ρ-hop radius, while employing a Border casting Routing Protocol (BRP) for directed, on-demand route discovery at the domain boundaries. At the inter-subnet level, multi-network nodes perform interface binding and load-aware forwarding, enabling efficient cross-subnet communication. Simulation results demonstrate that in multi-subnet and mobility-varying scenarios, LHR-SN significantly reduces end-to-end delay, enhances PDR and throughput, and maintains superior scalability with substantially lower routing overhead compared to AODV and DSDV.
CN4054 14:15-14:30	Hierarchical Single GEO All-Electric Propulsion Orbit -Event Effect Avoidance and Handling Methods for TT&C Links of - Injection Satellites Author(s): Haixu Wang, Xin Wang, Jianglei Gong, Yu Zhang Presenter: Haixu Wang, China Academy of Space Technology, China **Abstract:** GEO all-electric propulsion orbit-injection satellites are characterized by longer transfer orbit duration and more orbit maneuver cycles, making them more susceptible to space single-event effects (SEEs). Aiming at the mission characteristics of all-electric propulsion orbit-injection satellites, this paper analyzes the varying degrees of impact of the space single-event environment on satellites and proposes corresponding hierarchical SEE avoidance and handling methods. These methods provide valuable references for the development and design of subsequent satellites.

CN4046 14:30-14:45	Load Balancing Routing Technique for LEO Satellite Networks Based on Regional Partitioning Author(s): Ziye Xu, Quan Chen, Jiaqi Li, Chenyang Ding, Lei Yang Presenter: Ziye Xu, National University of Defense Technology, China **Abstract:** To achieve global high-speed internet coverage, numerous Low Earth Orbit (LEO) satellite network projects have been proposed, leading to the rapid proliferation of LEO constellations. However, challenges such as the vast number of satellite nodes and the non-uniform distribution of the terrestrial population result in slow routing convergence and network load imbalance. To address these issues, this paper proposes a partition-based load balancing routing algorithm. The algorithm partitions the network into multiple domains to isolate redundant signaling overhead and accelerate routing convergence. For inter-domain routing, it dynamically selects low-load paths among those with the minimum hop count. Within each domain, a secondary load balancing is performed by holistically considering propagation cost and current load status. The simulation results demonstrate that the partition-based load balancing technique achieves significant advantages in end-to-end delay and traffic balance compared to minimum hop routing.
CN3040 14:45-15:00	A Survey of Model Inversion Attacks: An Interface–Prior Perspective Author(s): Haoyu Liu, Yuwen Chen, Zhen Yang Presenter: Haoyu Liu, Beijing University of Technology, China **Abstract:** Model Inversion Attacks (MIA) pose an increasingly severe threat to the privacy and security of machine learning models deployed across various applications. This survey provides a systematic review and consolidation of existing MIA research. We propose a core two-dimensional taxonomy to organize current attack methodologies along two orthogonal axes: the Observable Interface, which includes posteriors, hard labels, intermediate features, and gradients; and the Generative Prior, covering regularization methods with no prior, as well as those based on GANs and Diffusion models. This framework allows us to unify the objective functions of different attacks, quantify their fidelity-efficiency trade-offs, and establish a foundation for fair cross-study comparisons. Furthermore, we conduct an in-depth analysis of architectural sensitivity, revealing that under fixed attack conditions, architectures such as CNNs and Transformers exhibit distinct information leakage patterns and layer-wise invertibility. Finally, we consolidate a full lifecycle of defense strategies---spanning training, inference, and deployment---and analyze their respective privacy-utility-cost trade-offs. By offering a clear and consistent analytical framework and evaluation criteria, this paper aims to promote the standardization and advancement of future MIA research.
CN4055 15:00-15:15	Environment Perception and Remote Control Method for Intelligent Power Box Oriented to Secure Communication Author(s): Lei Wang, Zhigao Wu, Jianmin Lü, Dezhong Guo, Chenliang Guo, Delong Li, Fangfang Guo Presenter: Lei Wang, Liujiaxia Hydropower Plant of State Grid Gansu Electric Power Company, China **Abstract:** With the accelerated evolution of the Industry 4.0 era and the deepening

	development of smart grid construction, higher demands are placed upon the perception capabilities, control parameters, and intelligent advancement of end-point grid equipment. Building upon the design of an intelligent power box, this paper proposes a method for environmental perception and remote control of smart power box oriented towards secure communications. This intelligent power box designed for secure communications, employs a main controller in conjunction with various sensor modules, utilizing fuzzy control and edge algorithms to achieve environmental perception and remote control. Through a multi-source heterogeneous information fusion strategy, it collaboratively processes multidimensional data such as voltage, temperature, humidity, and gas concentration, establishing a method for real-time status monitoring and regulation. At the remote secure communication control level, the system employs encrypted communication technology to connect with a cloud service platform, providing an intuitive, convenient, and secure operating method. This approach offers a secure, efficient, and adaptive solution for the intelligent operation and maintenance of power system facilities, contributing to the advancement of next-generation reliable and green intelligent management systems.
CN4053 15:15-15:30 (Online)	Design and Analysis of Fiber Optic Sensor System for Monitoring Leakage Parameters in Apron Pipeline Network Author(s): Youcheng Liang, Haitao Chen, Xiuli Wang, Zibo Zhuang Presenter: Youcheng Liang, Guangzhou Civil Aviation College, China **Abstract:** The apron fuel pipeline network is a critical area in civil aviation transportation operations, primarily responsible for the transmission of aviation fuel. To ensure reliable fuel transmission, the safety and operational integrity of the pipeline network must be maintained. This study focuses on monitoring the environmental parameter characteristics of the apron fuel pipeline network. Based on spectral absorption and optical interference theories, a fiber-optic sensor structure model suitable for simultaneous monitoring of both gas and liquid parameters is developed. By analyzing the spectral signal characteristics, the relationship between gas concentration and the absorption spectral lines of the output signal is established. Similarly, by analyzing the optical interference signal characteristics, the relationship between liquid depth and the spectral shift of the output signal is determined, forming a signal transmission model for the fiber-optic sensor. The design model parameters are then used to analyze data transmission characteristics, further validating the implementation approach of the signal sensing theory. Building on this foundation, a multi-parameter monitoring optical sensor structure for the apron pipeline network is designed, capable of simultaneously monitoring other parameters and liquid parameters, thereby establishing a multi-parameter monitoring measurement solution based on fiber-optic sensing technology.

Onsite Oral Session 2

Information and Network Security & Privacy Protection

- **Session Chair:** Assoc. Prof. Thien Wan Au, Universiti Teknologi Brunei, Brunei
- **Time:** 15:50-17:20, December 20, 2025 | GMT+8 (Beijing Time)
- **Venue:** Meeting Room 3 | 1F
- **Papers:** CN1006, CN2018, CN1005, CN2017, CN3044, CN3036

CN1006 15:50-16:05	Governing Cybersecurity for Small Developing State: Challenges, Drivers and Way Ahead Author(s): Au Thien Wan, Keith Lim Chun Chir, Sharul Tarazjiman Jajuddin, Serina Mohd Ali Presenter: Au Thien Wan, Universiti Teknologi Brunei, Brunei **Abstract:** This is a unique case of where the researchers have the chance to study and observe the approaches of assessing the governance of the cybersecurity of major public and quasi-public organizations of a small state in ASEAN. Global digitalisation poses greater challenges for small countries since the digital environment that subjects of small countries are exposed to is international rather than local. In this research the researchers developed the approaches to comprehensively understand the cybersecurity governance framework, processes, policies and practices of 5 public and quasi-public organizations. The organisations consisted of the law enforcer, the telco, the regulator, the cybersecurity agent, and the government. They were evaluated against the governance (GN) aspect of the established cyber security standard, NIST Cybersecurity Framework (CSF) 2.0. in relation to the shortfalls identified through the consultation of the global cybersecurity index (GCI) published by ITU. The study employed a multifaceted research methodology encompassing literature reviews, qualitative and quantitative data collection methods, and meticulous analysis of feedback and responses. Insights gleaned from the study were elucidated, contributing to a deeper understanding of the cybersecurity issues of the small state and the way forward to improve the overall landscape.
CN2018 16:05-16:20	A Mobile Crowdsourced Perception Method for Dynamic User Selection Based on UKF-LSTM Parallel Fusion Author(s): Jinze Zhao, Qi Xu, Wei Wang, Zhou Ai, Jianpo Li Presenter: Jinze Zhao, Northeast Electric Power University, China **Abstract:** User selection in Mobile Crowdsourced Sensing (MCS) networks directly impacts data collection quality and cost. This paper proposes a trajectory prediction algorithm based on parallel fusion of Unscented Kalman Filter (UKF) and Long Short-Term Memory (LSTM) networks to optimize user selection. The method models

	physical constraints of user movement via UKF, leverages LSTM to learn complex spatiotemporal patterns, and employs a dynamic weight fusion strategy to adaptively balance their outputs. Experimental results demonstrate that, compared to the UKF algorithm, the proposed fusion algorithm reduces positioning error by 38.7% and improves user selection efficiency by 52.3% in GPS-denied scenarios. This method provides a reliable theoretical tool for MCS task allocation in dynamic environments.
CN1005 16:20-16:35	UAV Intrusion Detection Based on iTransformer for MAVLink Message ID Sequence Author(s): Ruibo Liu, Xin Zhao, Naiwei Liu, Jun Li, Gang Wang Presenter: Ruibo Liu, Inner Mongolia University of Technology, China **Abstract:** MAVLink, a widely used communication protocol for unmanned aerial vehicles (UAVs), transmits plaintext messages that are highly susceptible to network-based attacks. Among these, flooding attacks are particularly disruptive, as they overwhelm the UAV system with a large volume of forged messages, interfering with normal communications. This paper proposes a lightweight UAV intrusion detection method that leverages MAVLink message ID sequences as input features, without relying on the original message content or contextual information. By employing the iTransformer model, we effectively learn and model the temporal patterns of message ID sequences to automatically identify both normal communication and various types of flooding attacks. Specifically, the method exploits the behavioral patterns embedded in message ID sequences and utilizes the powerful sequence modeling capabilities of iTransformer to detect three typical flooding attacks: Heartbeat Flood, Ping Flood, and Request Flood. Experimental evaluations on a MAVLink message ID dataset demonstrate that, compared to traditional approaches, the proposed model achieves superior detection accuracy and robustness in a four-class classification task. The effectiveness of the approach is further validated by confusion matrices and training curves, highlighting the feasibility and advantages of using MAVLink message ID sequences for UAV intrusion detection.
CN2017 16:35-16:50	Design and Adversarial Robustness Verification of Network Intrusion Detection Model for Raw Traffic Author(s): Juntong Zhu, Xinyue Zhang, Guanjie Wang, Rong Cong, Hongyu Sun, Yanhua Dong Presenter: Juntong Zhu, Jilin Normal University, China **Abstract:** Network intrusion detection plays a crucial role in maintaining computer network security. One of the mainstream methods in this field is to detect and analyze abnormal traffic by extracting traffic features. However, this method relies on manually designed features, which is time-consuming, labor-intensive, and may lose key information, thereby affecting detection efficiency and accuracy. This study adopts an innovative strategy of directly extracting information from raw data for analysis, avoiding the limitations of traditional methods, and proposes a deep learning architecture - a layered network model, which combines the improved LeNet-5 with LSTM neural network structure to simultaneously capture traffic spatial characteristics and time series features. By using network cascading technology, a unified training process for the entire system can be achieved, rather than training each component independently. To enhance the robustness of the model, adversarial training mechanism is introduced. The results show that the proposed hierarchical network model performs

	well and stably in both multi classification and binary classification experiments. The accuracy of adversarial attack experiments on the CICIDS-2017 dataset is over 98%, and the performance is significantly better than other intrusion detection schemes.
CN3044 16:50-17:05	A Non-Intrusive Real-Time Runtime Integrity Verification Framework for PLC Programs Author(s): Tianqi Liu, Yingxu Lai Presenter: Tianqi Liu, Beijing University of Technology, China **Abstract:** Programmable Logic Controllers (PLCs) are the core of Industrial Control Systems (ICS), and ensuring their runtime integrity is critical, as any unauthorized code modification or control-flow hijacking may lead to severe physical consequences. Existing solutions often introduce substantial overhead to the PLC scan cycle due to heavy instrumentation or frequent communication, making them unsuitable for time-sensitive ICS. This paper presents Cache-Heartbeat, a non-intrusive and real-time runtime integrity verification framework for PLC programs. Instead of relying on extensive instruction insertion or external communication, Cache-Heartbeat leverages microarchitectural cache behaviors as implicit heartbeat signals to dynamically verify the integrity of PLC control programs. Evaluation shows that Cache-Heartbeat can detect anomalies within 1 ms while introducing negligible scan-cycle overhead, offering a practical and real-time-safe solution for PLC integrity verification in time-sensitive ICS environments.
CN3036 17:05-17:20	DLKD-FL: Dynamic Layer-wise Aggregation with Knowledge Distillation for Personalized Federated Learning Author(s): Linbo Zhi, Jiahao Zhang, Sen Zhang Presenter: Linbo Zhi, Beijing University of Technology, China **Abstract:** Federated Learning (FL) has become a cornerstone technology for privacy-preserving distributed intelligence, enabling collaborative model training without the need to share raw data. However, in Non-IID (non-independent and identically distributed) scenarios, conventional aggregation methods often suffer from poor generalization and unstable convergence due to client drift. To address these challenges, we propose DLKD-FL, a novel personalized federated learning framework that integrates dynamic layer-wise aggregation and data-free knowledge distillation. In DLKD-FL, convolutional layers are dynamically aggregated based on kernel importance to enhance shared feature extraction, while fully connected layers are retained locally to preserve personalization. A data-free knowledge distillation module further enables cross-group knowledge transfer without compromising privacy, using proxy data synthesized via Generative Adversarial Networks (GANs). Additionally, a blockchain-based secure coordination layer ensures the integrity and verifiability of model updates and distilled knowledge exchanges. Extensive experiments on benchmark datasets demonstrate that DLKD-FL outperforms state-of-the-art methods in terms of accuracy, convergence stability, personalization, and communication efficiency under diverse Non-IID conditions. The results confirm that integrating dynamic aggregation, data-free distillation, and secure coordination provides a unified and trustworthy framework for scalable, privacy-preserving federated learning.

Online Oral Session 1

Information and Network Security-1

- **Session Chair:** Assoc. Prof. Zhongyuan Qin, Southeast University, China
- **Time:** 10:00-11:45, December 21, 2025 | GMT+8 (Beijing Time)
- **ZOOM ID:** 82313016185 | **Password:** 121921
- **Papers:** CN1002, CN2012, CN3034, CN3033, CN4052, CN3035, CN2020

CN1002 10:00-10:15	Certificateless Signcryption Scheme for Emergency Communication Author(s): Jianing Li, Hongyan Qian Presenter: Jianing Li, Nanjing University of Aeronautics and Astronautics, China **Abstract:** With the rapid development of the Internet of Things (IoT), unmanned aerial vehicles (UAVs) are being increasingly deployed in various applications. However, most UAV communications occur in open environments, where the security of transmitted data cannot be guaranteed. To address this issue, certificateless signcryption (CLSC) schemes have been proposed. Nevertheless, adversaries with public key replacement capabilities (adversaries) and malicious key generation centers (adversaries) can compromise the security of existing CLSC schemes. Taking Yu et al.'s CLSC scheme as an example, this paper demonstrates its vulnerability to Type I attacks in terms of unforgeability. To enhance communication security in post-disaster emergency scenarios involving detection UAVs, relay UAVs, and ground stations, we propose an improved certificateless aggregate signcryption (CLASC) scheme. The proposed scheme achieves confidentiality and unforgeability against both and adversaries. Furthermore, to reduce the resource consumption, our scheme not only minimizes the computational and communication overhead for individual messages, but also incorporates a batch unsigncryption mechanism to efficiently handle scenarios involving multiple communication messages.
CN2012 10:15-10:30	Modelling and Solving Problems in Communications and Network Security Elegantly Using a Unified Framework for Intelligence and Intelligent Systems Author(s): Harris Wang Presenter: Harris Wang, Athabasca University, Canada **Abstract:** The escalating complexity of modern communication networks and the sophistication of cyber threats demand increasingly intelligent security solutions. This paper presents Constrained Object Hierarchies (COH), a neuroscience-grounded theoretical framework for artificial general intelligence, and its Python implementation GISMOL (General Intelligent System Modelling Language) as a unified approach for developing intelligent systems in communications and network security. COH formalizes intelligent systems through a 9-tuple representation integrating compositional hierarchy, adaptive neural components, and multi-domain constraints. We demonstrate how this framework enables the development of provably secure,

	adaptive, and autonomous network security systems through five detailed implementations and seven summarized examples. Our work shows that COH/GISMOL provides a mathematically rigorous yet practical foundation for building next-generation intelligent security systems capable of hierarchical reasoning, constraint-aware adaptation, and autonomous threat response.
CN3034 10:30-10:45	Improved quantum differential Meet-In-The-Middle attack and some applications Author(s): Jichen Wei, Jian Zou, Rongwei Lin Presenter: Jichen Wei, Fuzhou University, China **Abstract:** To enhance the efficiency of the quantum differential Meet-In-The-Middle attack, an improved scheme based on quantum collision search is proposed. The traditional quantum search steps were replaced with Ambainis' quantum collision search algorithm. This replacement optimized the matching process between candidate keys and plaintexts in the Meet-in-the-Middle phase and significantly reduced time complexity. The improved attack scheme is applied to PIPO-128, SKINNY-128-384, and AES-256, achieving key recovery attacks for 8, 23, and 12 rounds, respectively. Analysis results under both Q1 and Q2 models demonstrate that the proposed scheme outperforms existing classical and quantum attacks in both time and memory complexity, validating its effectiveness and superiority in cryptanalysis.
CN3033 10:45-11:00	Optimized Diamond Structure Construction and Its Application to Enhanced MITM Nostradamus Attacks Author(s): Jiajie Dai, Jian Zou, Rongwei Lin, Qiufu Lan Presenter: Jiajie Dai, Fuzhou University, China **Abstract:** At EUROCRYPT 2006, Kelsey and Kohno originally proposed the Nostradamus attack, a cryptographic vulnerability in which an adversary can pre-determine a hash value y and later fabricate a suffix S such that H(P||S) = y for an a priori unknown prefix P. Their attack framework achieved a time complexity of O(sqrt(n) * 2^(2n/3)), where n denotes the hash function's output bit-length. At ASIACRYPT 2022, a quantum variant of the Nostradamus attack was introduced by Benedikt et al., reducing the time complexity to O(n^(1/3) * 2^(3n/7)). In ToSC 2023, the first dedicated Nostradamus attack targeting AES-like hash functions was proposed by Zhang et al., and in ToSC 2024 the meet-in-the-middle attack framework was improved by Dong et al., yielding enhanced attack results. In this paper, we propose a more efficient algorithm for constructing diamond structures. By designing an unbalanced diamond structure shaped as an unbalanced binary tree, the time complexity of the offline phase in the qRAM setting is reduced from O(k^(1/3) * 2^((n+2k)/3)) to O(2^((n+2k)/3)), where k represents the height of the diamond structure. In particular, the time complexity of the quantum Nostradamus attack is improved from O(n^(1/3) * 2^(3n/7)) to O(2^(3n/7)). Furthermore, applying this new offline structure to the MITM Nostradamus attack targeting AES-MMO yields lower time complexity results in the qRAM setting.
CN4052 11:00-11:15	Improved Classical Meet-in-the-Middle Nostradamus Attack Author(s): Rongwei Lin, Jian Zou, Jiajie Dai, Jichen Wei Presenter: Rongwei Lin, Fuzhou University, China **Abstract:** At EUROCRYPT 2006, Kelsey and Kohno first proposed the Nostradamus

	attack, which required a time cost of O(n^(1/2) · 2^(2n/3). At ToSC 2023, Zhang et al.\ proposed the first dedicated Nostradamus attack based on the meet-in-the-middle (MITM) attacks on AES-like hashing and Whirlpool in both quantum and classical settings. In this paper, we improve the MITM Nostradamus attack results on 7-round AES-MMO and 6-round Whirlpool in classical setting, by combining Zhang et al.'s MITM Nostradamus attack with the elongated diamond structure. For AES-MMO, our method reduces the time complexity of the attack from 2^(83)to 2^(70) with the memory complexity 2^(65), while for Whirlpool, we can improve time complexity from 2^(334) to 2^(262)with the memory complexity 2^(257).
CN3035 11:15-11:30	Parasite: A Steganography-based Backdoor Attack Framework for Diffusion Models Author(s): Jiahao Chen, Yu Pan, Li Wang, Yi Du Presenter: Jiahao Chen, Shanghai Polytechnic University, China **Abstract:** Recently, the diffusion model has gained significant attention as one of the most successful image generation models, which can generate high-quality images by iteratively sampling noise. However, recent studies have shown that diffusion models are vulnerable to backdoor attacks, allowing attackers to enter input data containing triggers to activate the backdoor and generate their desired output. Existing backdoor attack methods primarily focused on target noise-to-image and text-to-image tasks, with limited work on backdoor attacks in image-to-image tasks. Furthermore, traditional backdoor attacks often rely on a single, conspicuous trigger to generate a fixed target image, lacking concealability and flexibility. To address these limitations, we propose 'Parasite', a novel backdoor attack method for image-to-image tasks in diffusion models. This approach not only represents the first use of steganography for trigger concealment, but also allows attackers to dynamically specify target image content through the steganographic mechanism after injection, enabling fully customizable backdoor attacks. "Parasite" as a novel attack method effectively bypasses existing detection frameworks to execute backdoor attacks. In our experiments, "Parasite" achieved a 0 percent backdoor detection rate against the mainstream defense frameworks. In addition, in the ablation study, we discuss the influence of different hiding coefficients on the attack results. You can find our code at https://anonymous.4open.science/r/Parasite-1715/.
CN2020 11:30-11:45	Malware Image Classification Based on Lightweight Vision Transformer and Progressive Focal Loss Author(s): Zichao Lu, Shanshan Tu, Zexu Li Presenter: Zichao Lu, Beijing University of Technology, China **Abstract:** Malware remains a major cybersecurity threat, while traditional signature-based detection struggles to cope with its scale and diversity. Converting binaries into grayscale images has enabled the use of deep learning for automatic feature extraction, but existing approaches face critical challenges: convolutional neural networks (CNNs) capture only local patterns, and standard Vision Transformers (ViTs) demand large datasets and heavy computation, limiting their use in practice. We propose a malware image classification framework that integrates three components: a lightweight Transformer backbone (LeViT) for efficient feature extraction, a Progressive Focal Loss for adaptive handling of class imbalance, and Automatic Mixed Precision (AMP) for faster, memory-efficient training. The

	Progressive Focal Loss schedules the focusing factor γ over training epochs, mitigating the instability of fixed-γ variants and improving recognition of minority classes. Experiments on the Malimg dataset show that our method achieves state-of-the-art results, with improvements in Macro-F1 (0.953) and Cohen's Kappa (0.966) over cross-entropy and fixed Focal Loss, while maintaining high accuracy (0.969). AMP further reduces GPU memory consumption by about 25\% and shortens training time by 30\%. These results highlight the effectiveness of combining lightweight Transformers with adaptive loss design for scalable and resource-aware malware detection.

Online Oral Session 2

Information and Network Security-2

- **Session Chair:** Assis. Prof. Muhammad Rizwan, University of Derby, UK
- **Time:** 14:00-15:30, December 21, 2025 | GMT+8 (Beijing Time)
- **ZOOM ID:** 82313016185 | **Password:** 121921
- **Papers:** CN4047, CN2021, CN3030, CN3042, CN3043, CN2023

CN4047 14:00-14:15	GateFormer-CS: Enhancing Dynamic Malware Detection through Channel-Sequence Gating and Multi-Scale Expansion Fusion Author(s): Shiyao Liu, Yubo Wang, MinJun Wu Presenter: Shiyao Liu, Beijing University of Technology, China **Abstract:** This paper presents GateFormer-CS, a lightweight Transformer-based framework for dynamic malware detection that improves early feature separability and robustness on long, noisy behavioral sequences. Conventional Transformer encoders lack channel re-weighting and local priors along the sequence dimension, making them sensitive to high-frequency but weakly discriminative events and padding noise. GateFormer-CS extends a two-layer Transformer encoder with two plug-in modules. The Channel-Sequence Gating (CSGA) module performs channel recalibration and position-wise selective enhancement through multi-kernel one-dimensional convolutions and gated linear units. The Multi-Scale Dilated Gating Fusion (MDGF) module introduces multi-scale dilated token mixing and applies parallel channel and sequence gates with adaptive fusion. Both modules use depthwise one-dimensional convolutions and linear mappings, retaining approximately linear complexity with respect to sequence length and channel dimension. Evaluated on the Speakeasy and Avast-CTU behavioral datasets, GateFormer-CS achieves substantial gains under strict false-positive constraints. On the Speakeasy benchmark at an FPR of 0.001, our method improves TPR, AUC, F1, and accuracy by 0.2801, 0.0291, 0.0444, and 0.0695, respectively, over the Nebula baseline. Ablation results further confirm that CSGA and MDGF are complementary, and per-family analyses show notable improvements on hard malware types such as Dropper. These results demonstrate that GateFormer-CS is an effective and efficient framework for behavior-sequence-based malware detection.
CN2021 14:15-14:30	PUF-Enhanced Lightweight Authentication and Key Agreement for UAV Networks Author(s): Jiakai Dou, Shanshan Tu, Kun Li, Dazhong Liu, Zexu Li Presenter: Jiakai Dou, Beijing University of Technology, China **Abstract:** With the advancement of Internet of Things (IoT) and 5G technologies, unmanned aerial vehicles (UAVs) are increasingly deployed across diverse domains such as smart cities, disaster relief, and environmental monitoring. However, data interactions conducted by UAVs frequently encounter security threats including

	identity leakage and session hijacking, which may lead to unauthorized disclosure of sensitive data or illicit device control. To enhance the security of UAV communications, this paper proposes a lightweight multi-factor authentication and key agreement scheme based on Physical Unclonable Functions. The proposed scheme integrates PUF hardware characteristics, cryptographic hash functions, and fuzzy extractor techniques for biometric features to establish secure authentication between users and UAVs. Through security analysis and comparative evaluation with existing works, the protocol is proven resistant to multiple known attacks while maintaining lower system overhead.
CN3030 14:30-14:45	A Quantum-Resistant Authentication and Key Agreement Protocol for UAV Networks Author(s): Kaifeng Wu, Zhenhu Ning, Jiakai Dou, Lei Wang, Yuren Xie Presenter: Kaifeng Wu, Beijing University of Technology, China **Abstract:** The unmanned aerial vehicle (UAV) network serves as the core infrastructure of the future low-altitude intelligent network, providing flexible aerial smart services for various industries through inter-UAV collaboration and ground-air connectivity. With the advancement of quantum computing, quantum algorithms pose a serious threat to UAV communication networks. Traditional authentication protocols based on classical number-theoretic problems are no longer secure against quantum attacks. To address the challenges of quantum threats and the inherent characteristics of UAVs, such as high mobility and resource constraints, this paper proposes a quantum resistant authentication and key agreement protocol for UAV networks. The comprehensive informal security analysis demonstrates the robustness of the protocol against various attacks, particularly attacks based on quantum computing. Furthermore, the authentication component of the protocol adopts a lightweight design, reducing computational overhead by up to 53.57%, thereby balancing security and efficiency.
CN3042 14:45-15:00	A Cross-Domain Authentication and Key Agreement Scheme for Industrial IoT Author(s): Jingxuan Fan, Shanshan Tu, Zitao Wang, Hangchuan Zhang, Long Wang Presenter: Jingxuan Fan, Beijing University of Technology, China **Abstract:** The rapid development of the Industrial Internet of Things (IIoT) has accelerated the digitalization and intelligence of industrial manufacturing. However, during cross-domain collaboration, device authentication and secure communication still face numerous challenges. Due to heterogeneous trust anchors and diverse security policies among different management domains, traditional cross-domain authentication mechanisms suffer from issues such as single-point failure of the trusted authority, complex certificate management, and low authentication efficiency. To address these challenges, this paper proposes a cross-domain authentication and key agreement scheme based on Elliptic Curve Cryptography (ECC). The proposed scheme enables bidirectional authentication and session key establishment between domains and nodes through collaborative operations of Edge Servers (ESs). Security analysis demonstrates that the scheme can resist common attacks and satisfies essential security properties, including mutual authentication, anonymity, and forward secrecy. Performance evaluation results further show that, compared with recent ECC and bilinear pairing-based schemes, the proposed protocol achieves superior computational efficiency.
CN3043 15:00-15:15	An Integrated CL-PKC and PUF-Based Authentication and Key Agreement Protocol for Cross-Domain UAVs Author(s): Juntao Zhu, Dapeng Tang, Yuanbo Cui, Zitao Wang, Long Wang

	Presenter: Juntao Zhu, Beijing University of Technology, China **Abstract:** With the continuous development of unmanned aerial vehicle (UAV) technologies, secure authentication in cross-domain collaborative operations has become increasingly crucial. To address the persistent challenges of certificate management and key escrow in traditional Public Key Infrastructure (PKI) and Identity-Based Public Key Cryptography (IB-PKC) systems, this paper proposes a novel cross-domain authentication protocol for UAVs that integrates Certificateless Public Key Cryptography (CL-PKC) with Physical Unclonable Functions (PUF). The protocol utilizes Elliptic Curve Cryptography (ECC) to enable efficient key agreement while avoiding computationally intensive bilinear pairing operations, making it particularly suitable for resource-constrained UAV platforms. The incorporation of PUF enhances physical security and provides robust identity binding for terminal devices. Formal security analysis under the Computational Diffie-Hellman (CDH) assumption, complemented by comprehensive verification using ProVerif, demonstrates the protocol's resilience against both active and passive attacks. Performance evaluation results confirm that the proposed protocol achieves superior communication and computational efficiency compared to existing schemes, establishing its practical applicability in dynamic multi-domain UAV collaborative environments.
CN2023 15:15-15:30	Adaptive RLWE-Based Lightweight Mutual Authentication Protocol for Medical RFID Systems Author(s): Dazhong Liu, Shanshan Tu, Kun Li, Jiakai Dou, Zexu Li Presenter: Dazhong Liu, Beijing University of Technology, China **Abstract:** Radio Frequency Identification (RFID) is now widely used in medical Internet of Things (IoT) systems. As its use grows, protecting patient data has become a major concern. The rise of quantum computing makes this challenge even more serious. In this paper, we present an adaptive and lightweight mutual authentication protocol for medical RFID systems. The protocol is based on the Ring Learning With Errors (RLWE) problem, which provides strong post-quantum security. It introduces an adaptive mechanism that adjusts RLWE parameters for tags with different security needs. This design achieves a balance between protection and resource use. To improve robustness, the protocol also includes a pseudonym update process that prevents desynchronization. We analyze its security in detail. The analysis combines a formal proof in the Random Oracle model and symbolic verification with the Scyther tool. Results show that the protocol can resist replay, man-in-the-middle, and impersonation attacks. It also preserves tag anonymity and forward secrecy. Performance tests further confirm its efficiency. On the tag side, the average computation time is only 7.67931 ms. These results suggest that the protocol is well-suited for secure and efficient authentication in resource-limited medical RFID environments under post-quantum threats.

Online Oral Session 3

Communication and Information Engineering, Data Security & Privacy Protection

- **Session Chair:** Lijun Zhang, E-surfing Vision Technology Co., Ltd, China Telecom, China
- **Time:** 15:50-17:20, December 21, 2025 | GMT+8 (Beijing Time)
- **ZOOM ID:** 82313016185 | **Password:** 121921
- **Papers:** CN2016, CN2007-A, CN4050, CN4049, CN3029, CN4048

CN2016 15:50-16:05	High-Accuracy Data Aggregation via Personalized Local Differential Privacy in Smart Grid Author(s): Haina Song, Jinhang Sun, Zhangqing He, Nan Zhao, Minghu Wu Presenter: Jinhang Sun, Hubei University of Technology, China **Abstract:** As smart grid technologies continue to evolve, concerns regarding the privacy and security of users' electricity consumption data are increasingly prominent. Existing privacy-preserving schemes either fail to accommodate personalized privacy preferences or suffer from low data aggregation accuracy. To address these challenges, we propose a high-accuracy data aggregation scheme based on personalized local differential privacy (PLDP-HDAS). The scheme allows each smart terminal to independently select its own privacy-preserving level according to personal privacy requirements and then perturbs its true consumption data using a personalized randomized response mechanism. The gateway gathers all perturbed data and then enhances aggregation accuracy by applying a weighted aggregation strategy based on mean-square error. Experiments demonstrate that the proposed PLDP-HDAS improves aggregation accuracy by at least 50% compared with existing methods, while also exhibiting strong robustness and scalability.
CN2007-A 16:05-16:20	Multi-Domain Adaptive Network Traffic Classification Author(s): Xueman Wang Presenter: Xueman Wang, Beijing University of Technology, China **Abstract:** With the continuous advancement of network technologies, network traffic classification plays an increasingly important role in areas such as network security and anomaly detection. However, traffic data often undergoes concept drift due to changes in network structure, application updates, or other dynamic factors. Specifically, the data used during testing is frequently not independent and identically distributed (non-IID) compared to the training data. As a result, classification models trained on previously collected traffic may suffer significant drops in accuracy when applied to new traffic samples, thereby weakening their generalization capability. To address this practical challenge, we propose a multi-domain adaptive network traffic classification method. This method explicitly accounts for distributional differences across traffic domains and leverages invariant features to enable robust classification under drift. In

	particular, we introduce a dynamic domain adaptation model that adjusts its parameters in real time to accommodate traffic from varying sources, resulting in more generalizable cross-domain learning. Furthermore, to enhance the model's reliability and applicability, we integrate an evidential uncertainty mechanism that quantifies the credibility of predictions and effectively manages open-set scenarios involving unknown classes. Overall, the proposed approach addresses both concept drift and open-set detection, demonstrating improved practicality, scalability, and adaptability in dynamic network environments.
CN4050 16:20-16:35	Dataset Ownership Protection Method Based on Maximizing Distribution Discrepancy Author(s): Xiaoliang Wang, Liqin Wei, Chang Qin, Ruiping Yin Presenter: Xiaoliang Wang, TravelSky Technology Limited, China **Abstract:** In recent years, diffusion-based generative models have significantly advanced, enabling users to create high-quality images with simple text prompts. This ease of use has led to the widespread adoption of such models across various creative domains. However, the accessibility of open-source diffusion models also raises concerns about unauthorized use of personal or artistic data, particularly through fine-tuning techniques such as Dream Booth. To address the challenge of protecting image datasets from unauthorized fine-tuning, prior methods have introduced adversarial perturbations that rely heavily on prompt information. However, these approaches face limitations when prompt alignment between original and fine-tuning stages cannot be guaranteed. In this work, we propose a prompt-agnostic dataset ownership protection method that avoids the reliance on textual prompts. Rather than relying on prompts, our method generates protected datasets by calculating the distributional discrepancy between the original and protected datasets in the latent space using Wasserstein distance. By maximizing this discrepancy, we hinder the model's ability to learn from protected samples. We evaluated our method on Stable Diffusion V1.5 using multiple benchmark datasets. Experimental results demonstrate that our approach effectively impairs unauthorized fine-tuning while preserving the visual quality of original images, offering a robust and practical solution to dataset ownership protection in the era of generative models.
CN4049 16:35-16:50	TCSS: Traceable Contributory Secret Sharing for Secure Multi-Tenant AI Model Serving Author(s): Yuxin Huang, Xinyu Meng, Lifei Wei Presenter: Yuxin Huang, Shanghai Maritime University, China **Abstract:** We study secure multi-tenant AI model serving in which multiple administrative domains decrypt and serve a shared model under joint control, while ensuring that any illicit reconstruction of the decryption secret can be attributable. We introduce Traceable Contributory Secret Sharing (TCSS), a dealer-less variant of traceable secret sharing tailored to this setting. Participants collaboratively synthesize an implicit Shamir secret via a Pedersen-style verifiable secret sharing (VSS) workflow. Against an adversary providing only black-box access to a pirate reconstruction oracle, TCSS adds a lightweight, discrete-log-based publicly verifiable tracing (PV-Trace) layer: an auditor can non-interactively produce a trace that (i) identifies at least one leaking participant with probabilit1 $-negl(\lambda)$, and (ii) comes with a publicly verifiable non-interactive zero-knowledge (NIZK) proof. This conference version contributes:

	(i) a clean, dealer-less instantiation with a formal correctness proof; (ii) a PV-Trace construction sketch in the DLog setting with proofs and verification cost linear in the number of traitors; (iii) a robust tracing mechanism based on list decoding that reconstructsa "culprit polynomial" from noisy black-box queries, with explicit parameter bounds; and (iv) a formal security model for black-box traceability and soundness. We provide a security analysis understandard assumptions (the Discrete Logarithm problem and in the Random Oracle Model) and outline an evaluation plan.
CN3029 16:50-17:05	Research on Collaborative Task Offloading Strategy for Space-Air-Ground-Sea Communication in Offshore Wind Farms Author(s): Lingzhi Li, Zhengtao Wang, Chanjuan Tang Presenter: Chanjuan Tang, State Grid Shanghai Economic Research Institute, China **Abstract:** To address the dual optimization problem of task offloading latency and energy consumption in offshore wind farms under heterogeneous Space-Air-Ground-Sea link environments, this paper proposes a collaborative task offloading strategy. First, we establish a physical model integrating local computing nodes, Unmanned Aerial Vehicle (UAV) relay nodes, and Low Earth Orbit (LEO) satellite links. An optimization model is constructed to minimize total latency and total energy consumption while satisfying channel reliability and node resource constraints. Then, an improved genetic algorithm (GA) is designed, incorporating standard deviation-normalized fitness, multi-path Rayleigh fading-averaged channel modeling, adaptive mutation rate, and diversity preservation mechanisms to enhance convergence stability and search efficiency. Finally, simulations demonstrate the superiority of the proposed method over traditional local processing and single-domain offloading strategies in terms of latency and energy consumption.
CN4048 17:05-17:20	Fault Prediction for Power Information Systems Based on Hierarchical Vertical Federated Contrastive Learning Author(s): Chaoyang Qu, Chong Wang, Jing Zhang, Guang Huo Presenter: Chong Wang, Northeast Electric Power University / State Grid Eastern Inner Mongolia Electric Power Co., Ltd., China **Abstract:** Traditional fault prediction in power information systems faces persistent challenges arising from data silos, privacy constraints, and limited feature representation. To address these issues, this paper presents a Hierarchical Vertical Federated Contrastive Learning (HVFCL)–based fault prediction framework. The proposed method establishes a three-tier terminal–edge–cloud vertical federated architecture and introduces a federated contrastive learning mechanism that improves feature consistency and robustness through global memory construction and contrastive optimization. Furthermore, a differential privacy mechanism and a trust-based aggregation strategy are jointly designed to ensure secure and reliable cross-organizational collaboration. Experimental results show that the HVFCL model improves accuracy, F1-score, and AUC by 5.8%, 6.1%, and 4.9%, respectively, compared with traditional centralized models. In addition, HVFCL demonstrates strong early-warning capability, achieving fault detection approximately 20 minutes in advance, and exhibits superior cross-node generalization performance. These findings highlight the potential of HVFCL as a practical and scalable paradigm for distributed intelligent fault prediction in power information systems.

Notes