

2025 International Conference on Cyber Resilience and Endogenous Safety & Security (CRESS 2025)

**Nanjing, China
27-29 November 2025**

IEEE Catalog Number: CFP255AS-POD
ISBN: 979-8-3315-7105-4



Copyright © 2025, IEEE

All Rights Reserved

Copyright and Reprint Permissions:

Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

*** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.

IEEE Catalog Number:	CFP255AS-POD
ISBN (Print-On-Demand):	979-8-3315-7105-4
ISBN (Online):	979-8-3315-5949-6

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA

Phone:	(845) 758-0400
Fax:	(845) 758-2633
E-mail:	curran@proceedings.com
Web:	www.proceedings.com

TABLE OF CONTENTS

Mitigating ORM-Induced SQL Injection via Keyword Randomization	1
<i>Pengwei Yin, Gaofei Zhang, Hao Liu, Yuan Yao</i>	
A Resilient Arbitration and Scheduling Mechanism with Weight Dispersion for Dynamic Heterogeneous Redundancy	8
<i>Hongge Wu, Weida Li, Bo Liu, Jiuxin Cao</i>	
Design of Generalized Mimic Defense Module Based on Virtual Heterogeneous Containers	14
<i>Shen Li, Xu Chenwei, Wu Zicheng, Chen Shi, Zhang Song, Li Zhaozhao</i>	
A Redundant-Channel Switching Method for Secure and Resilient Control of Industrial Systems under FDI Attacks	20
<i>Xinmei Li, Xuan Li, Xianghui Cao</i>	
TEE-Based Privacy-Preserving Arbitration for Dynamic Heterogeneous Redundancy in Industrial Control Systems	28
<i>Yukun Niu, Lei He, Xiaopeng Han, Yu Xie</i>	
Dual-Agent Adversarial Framework Based on Endogenous Security and Multi-Objective Reinforcement Learning	36
<i>Xiyou Qian, Yuxuan Ye, Kai Wang, Siyuan Mao, Yujie Wang, Xuewen Yu, Hantao Zhao</i>	
RHDC: A Redundant and Heterogeneous Defense Chain Mechanism for Endogenous Security-Oriented Switches	44
<i>Haoyu Zhang, Yuyu Zhao, Guang Cheng, Yuyang Zhou</i>	
DHR-LLM: A Dynamic Heterogeneous Redundancy Framework for Resilient Large Language Model Inference	52
<i>Ping Chen, Zhuyang Yu, Shuting Zhang</i>	
Resilient Event-Triggered Control for MAS under DoS Attacks: Harnessing Data and Smart Edge Weights	59
<i>Wenrui Liang, Mingyang Yu, Ying Wan, Guanghui Wen</i>	
Cyber Resilience Quantification: A method for Resistance and Recovery Capabilities Measurement	67
<i>Dalong Zhang, Zhilong Han, Shuguang Ding, Gangtao Han, Zhiqing Tang</i>	
Translating Code Changes to Test Updates: An NMT-based Framework for Automated Production-Test Co-evolution	75
<i>Xing Wang, Qikai Chen, Changyi Deng, Chang Zhang, Yuhan Huang, Jiaxuan Hou, Jianlei Chi</i>	
Multi-Metric Fusion Based Quantitative Analysis Method for Comprehensive Cyber Resilience	83
<i>Gangtao Han, Fengpeng Xiong, Zhiqing Tang, Gaofeng Pan, Changhao Du, Dalong Zhang</i>	
AIGC-HRSTG: Dissecting API Behaviors in Encrypted AIGC Traffic via Heterogeneous-Relational Spatio-Temporal Graph Learning	91
<i>Zenghan Guan, Weiwei Liu</i>	
A Framework for Quantitative Assessment of Cyber Resilience in Multi-Attack Scenarios	98
<i>Gangtao Han, Boya Zhang, Zhiqing Tang, Dalong Zhang, Shijie Shi</i>	

Efficient Widening Operations for Static Analysis of Bit-Vector Programs	104
<i>Guangsheng Fan, Dengping Wei</i>	
ACSP: An Adaptive Cloud-Native Security Platform Oriented to Cyber Resilience	111
<i>Bing Hao, Yu Cao, Ruoxi Chen, Zhaosen Deng, Yaming He, Junfeng Hu</i>	
ReGLEn: Resilient Critical Node detection in Cyber-Physical Systems via Self-Supervised Graph Representation Learning	119
<i>Yancheng Mu, Junjie Zhang, Lixin Ji, Shuxin Liu, Lan Wu, Qi Ouyang</i>	
Blockchain-Based Secure and Composable Model for Semi-Honest Privacy-Preserving Computation	125
<i>Longyang Yi, Jian Liu, Zhiguo Wan</i>	
STGNI: Spatio-Temporal Graph Node Importance for Software-Defined Networking Traffic Prediction	132
<i>Yanxin Jia, Long Xu, Hengsheng Zhang, Kailai Peng, Hui Zuo, Lihu Pan, Junhua Kuang</i>	
A Two-Stage Anomaly Detection Framework for 5G Core Networks Based on Multi-Source Data	139
<i>Xinming Wang, Xingxing Liao, Jie Yang, Runhan Feng, Jingchen Xu</i>	
TS-Morph: A Generative Covert Timing Channel over QUIC via Multi-Head Time Series Prediction	147
<i>Zeshun Qiu, Weiwei Liu</i>	
A Hybrid Attribute-Content-Based Access Control Model for Medical Information Systems	153
<i>Ke Ma, Xinyu Xu, Yizhen Yang, Pingping Xu</i>	
A Blockchain-Based Lightweight Distributed Identity Authentication Mechanism	160
<i>Bingjing Wang, Xiuju Huang, Cong Zuo, Licheng Wang, Youqi Li</i>	
Survey of Language Level Memory Safety	168
<i>Xinming Guo, Guangliang Yang, Haoxiang Zhang, Can Li, Yi Wang, Min Yang</i>	
Blockchain-Based Distributed Identity Supervision and Revocation	176
<i>Qiang Gao, Zhiqi Liu, Youqi Li, Cong Zuo, Licheng Wang</i>	
PhysiKKT-Net: A KKT-based Neural Network with Guaranteed Compliance for Real-Time Power Flow Analysis	183
<i>Qingbin Jiang, Jianglin Feng, Zijun Wang, Haichuan Zhang, Siqi Meng, Ziyue Jia, Yujie Yang, Yang Liu</i>	
LFRNet: A Large Language Model-guided Feature Reweighting Network for Lightweight Intrusion Detection	191
<i>Dalong Zhang, Wenjie Tian, Zhiqing Tang, Yuncong Lu, Wenbo Hu</i>	
Identification of Cyber-Physical Security Boundary for Rotating Bearings under Attacks Using PINNs	199
<i>Ziyue Jia, Yiying Tao, Hanqi Zhou, Siqi Meng, Yuheng Li, Qingao Yuan, Yang Liu</i>	
Anti-Reconnaissance Routing in Non-Cooperative Networks via Reinforcement Learning	207
<i>Danqi Li, Jilong Yang, Weichen Li, Jincheng Deng, Chuanrong Liu, Lina Wang, Jin Zhao</i>	
StateCacheSim based GAN-DISA: A State-Caching-Based Cosimulation Platform with GAN-Based Data Injection Attack Analysis for Cyber-Physical Power System Evaluation	214
<i>Usama Aslam, Tang Yi</i>	
A Lightweight Approach to Multipath Traffic Splitting Against Website Fingerprinting	222
<i>Zirui Zhang, Jilong Yang, Weichen Li, Jincheng Deng, Chuanrong Liu, Lina Wang, Jin Zhao</i>	

Resilient Reinforcement of CPSs against Sparse Sensor Attacks by Prior Information Decomposition	230
<i>Zheyi Zhao, Xuqiang Lei</i>	
The reliable preassigned-time consensus control of the second-order multi-agent systems: An event-triggered sliding-mode control approach*	236
<i>Feida Song, Leimin Wang, Zhi-Wei Liu</i>	
Privacy-Preserving Load Constrained Shortest Distance Queries over Encrypted Graphs in Cyber-Physical Systems	242
<i>Chao Mu, Xiaoming Wu, Ming Yang, Xin Wang, Xianghui Cao</i>	
Underwater Covert Communication with Dynamic Hypergraph and Uniformized Spreading	249
<i>Ming Xu, Haiyu Jin</i>	
An Endogenous Security Defense Strategy for Adversarial Robustness in UAV Target Recognition	255
<i>Yuezhong Zhang, Shaoxun Liu, Jinfeng Zhang, Shiyu Wang, Yongshang Li, Peng Fu, Wei Qing Zhen Zhang</i>	
A Resilient LLM-driven Agent Framework for Multi-UAV Mission Planning and Control	261
<i>Haoyang Chen, Shaoxun Liu, Jinfeng Zhang, Yupeng Zhang, Shiyu Wang, Chenchen Liu, Peng Fu Yuezhong Zhang, Dongchen Ji</i>	
Retrieval-Confused Generation: An Effective Provider-Side Defense Against Privacy Violation Attacks in Large Language Models	269
<i>Wanli Peng, Xin Chen, Hang Fu, Xinyu He, Juan Wen, Yiming Xue</i>	
A Progressive Fusion Architecture for Validating Distance Estimation in Aftermarket ADAS Installations	278
<i>Gangtao Han, Gang Shen, Song Wang, Gaofeng Pan, Changhao Du</i>	
Reinforcement Learning-Based Critical Scenario Generation for Safety Verification of Autonomous Cyber-Physical Systems	286
<i>Hongbin Wang, Siqi Peng, Jiale An, Yuhan Hao, Xiaodong Zhang</i>	
DHR-Based Threat Detection Method For ADAS	292
<i>Qingyu Shen, Wenbo Hu, Shuguang Ding, Gangtao Han, Dalong Zhang</i>	
JailbreakMaster: Low-Interaction Jailbreak Prompt Generation via Feature-Guided Strategy Search and Adaptive Fusion	299
<i>Zezhi Ba, Jiawei Zhao, Kejiang Chen, Weiming Zhang, Nenghai Yu</i>	
An LLM-Assisted Fuzz Testing Framework for Unmanned System Software	305
<i>Yupeng Zhang, Qing Wei, Shaoxun Liu, Yankun Xu, Haoyang Chen, Jinfeng Zhang</i>	
GraphDistill-TI: A Temporal-Structural-Aware Data Distillation Framework for Fine-tuning Threat Intelligence LLMs	312
<i>Kaihua Zheng, Jianan Huang, Jinsheng Sun, Weiwei Liu</i>	
DSA-LoRA: A Seamless Content-Style LoRA Fusion for Adversarial Sample Generation	320
<i>Gangtao Han, Xinhai Zhong, Lingling Li, Song Wang</i>	
TEAL: Efficient and Effective Anti-Money Laundering based on Dynamic Spatio-Temporal Feature Modeling and LLMs	328
<i>Xiaolei Yin, Zihan Wang, Xing'E Yan</i>	

Diffuse++: Semantic-Aware Diffusion Attacks with Progressive Prompting	336
<i>Xiang Wu, Fengpeng Xiong, Boya Zhang, Gangtao Han</i>	
Enhancing Result Verification of Convolutional Neural Network Predictions	343
<i>Yitong Sun, Lingling Wang, Yuxiang Wang, Xiaozhou Wang</i>	
SLFGR StegoGAN: Self-Adaptive Local Fusion and Global Recovery StegoGAN for Few-shot Coverless Image Steganography	349
<i>Daqiu Li, Miao He, Lv Shi, Haihua Gu</i>	
Towards Understanding Masked Distillation	357
<i>Tuo Chen, Jie Gui</i>	
SLMark: Robust Watermarking Against Image Editing via Simulation-Based Noise Layer and Low-Frequency Embedding	365
<i>Mingyang Li, Yichao Tang, Yuliang Xue, Sheng Li, Zhenxing Qian, Xinpeng Zhang, Ji He, Hongda Li</i>	
CPP: A Stealthy Attack through Critical Path Poisoning in Federated Reinforcement Learning	372
<i>Chengze Zhang, Jia Wang, Xianghui Cao</i>	
Threshold Anonymous Credential Scheme Based on Attribute-Based Encryption	380
<i>Zhengxi Zhong, Hongyang Yan, Weichu Deng, Gongming Zhang, Zhexuan Ni</i>	