Program: The 1st Workshop on Securing Next-Generation Intelligent Transportation Systems (SecureTrans 2025)

8:50-9:00 Opening

9:00-10:00 Keynote

Speaker: Cristina Nita-Rotaru, Professor of Computer Science and Associate Dean for Faculty in Khoury College of Computer Sciences at Northeastern University

Title: Towards Resilient Autonomous Vehicular Systems

Abstract:
Autonomous vehicular systems are self-driving vehicles that operate with limited or no human input by integrating advanced sensors, artificial intelligence, and real-time data processing. Communication capabilities, such as Vehicle-to-Everything (V2X), allow them to interact with other vehicles and infrastructure for enhanced situational awareness. Safety and security are critical in autonomous vehicular networks because these systems directly impact human lives and public infrastructure. A failure in safety mechanisms could lead to accidents, injuries, or fatalities, especially in complex traffic environments. Security is essential to prevent cyberattacks that could compromise vehicle control, disrupt traffic, or leak sensitive data.

In this talk, I will explore the goals and challenges involved in designing autonomous vehicular systems that are resilient to both failures and cyberattacks. I will delve into various types of attacks targeting vehicles with different levels of autonomy and discuss corresponding mitigation strategies. The focus will include core autonomous driving features such as Adaptive Cruise Control (ACC), which governs longitudinal motion, and Automatic Lane Centering (ALC), which manages lateral control. I will also examine security threats and defenses in connected vehicle environments, particularly in scenarios involving vehicle-to-vehicle communication used to enable Cooperative Adaptive Cruise Control (CACC). Finally, I will present insights into how such attacks can ripple through and impact broader metropolitan traffic systems.

Bio:

Cristina Nita-Rotaru is a Professor of Computer Science in the Khoury College of Computer Sciences at Northeastern University where she leads the Network and Distributed Systems Security Laboratory (NDS2) and is a founding member of the Cybersecurity and Privacy Institute. Prior to joining Northeastern, she was a faculty in the Department of Computer

Science at Purdue University (2003 - 2015). She served as an Associate Dean of Faculty at Northeastern University (2017 - 2020),
Director of the Undergraduate Cybersecurity Program (2024 - 2025), and as an Assistant Director for CERIAS at Purdue University (2011 - 2013). Her research lies at the intersection of cybersecurity, distributed systems, and computer networks. The overarching goal of her work is designing and building resilient distributed systems and network protocols that are resilient to faults, misconfigurations, and attacks. Her work received several best paper awards in NETYS 2023, ACM SACMAT 2022, IEEE SafeThings 2019, NDSS 2018, ISSRE 2017, DSN 2015, three IETF/IRTF Applied Networking Research Prize in 2018, 2016 and 2024, and Test-of-Time award in ACM SACMAT 2022. She is a recipient of the NSF Career Award in 2006.

Cristina Nita-Rotaru has served on the program committee of numerous conferences in networking, distributed systems and security such as ISOC NDSS, IEEE S&P, IEEE Euro S&P, IEEE/IFIP DSN, IEEE ICNP, IEEE ICDCS, IEEE INFOCOM, ACM CCS, ACM Wisec, ACM SOCC, ACM SIGCOMM, ACM CoNEXT, ACM Web, ACM Eurosys, ASPLOS, USENIX Security, USENIX OSDI, USENIX ATC. She was an Associate Editor for Elsevier Computer Communications (2008 - 2011), IEEE Transactions on Computers (2011 - 2014), ACM Transactions on Information Systems Security (2009 - 2013), Computer Networks (2012 - 2014), IEEE Transactions on Mobile Computing (2011 - 2016), and IEEE Transactions on Dependable and Secure Systems (2013 - 2017). She was a member of the steering committee of ISOC NDSS, ACM Wisec, and IEEE/IFIP DSN. She was a general chair for IEEE DSN 2022 and ISOC NDSS 2023, 2024, and a chair of the Steering Group of NDSS 2024. She was a chair of the CRA Outstanding Undergraduate Research Award Committee (2019, 2020). She is currently a member of the IFIP Working Group on Dependable Computing and Fault-tolerance and the Steering Committee of ACM SACMAT, the Vice-Chair of the IEEE Technical Community on Dependable Computing and Fault Tolerance (TCFT), and the co-chair of IEEE S&P 2025 and S&P 2026.

10:00-10:30 Break (Poster Session)

Posters:

- Protecting Connected and Autonomous Vehicles from Laser Attacks on Traffic Signals Using Vehicle to Everything Communication. A K M Sazzadul Alam (University of Houston), Mansoureh Jeihani (Morgan State University), Ehsan Mahryaar (Morgan State University), Yunpeng Zhang (University of Houston)

- Classifier-Aware Defense for Visual Recognition in Connected Autonomous Vehicles. Bill Deng Pan (Embry-Riddle Aeronautical University), Richard Guo (Irvine Valley College), Dahai Liu (Embry-Riddle Aeronautical University), Hongyun Chen (Embry-Riddle Aeronautical University), Yongxin Liu (Embry-Riddle Aeronautical University)

- In-Progress: Enhancing Cybersecurity in Advanced Traffic Management Systems by Detecting Evasion and False Data Injection Attacks. Venkata Naga Sai Ram Nomula (University of Houston), Yunpeng Zhang (University of Houston), Suxia Cui (Prairie View

A&M University), Ed Pearson (Alabama A&M University), Xiang Zhao (Alabama A&M University)

- In-Progress: Blockchain-Based Secure Data Exchange in ATMS with End-to-End Encryption (E2EE). Narayan Soni (University of Houston), Yunpeng Zhang (University of Houston), Dakai Zhu (The University of Texas at San Antonio)

- In-Progress: CNN-Based Misbehavior Detection with Batch Message Verification for V2X Communications. Jiaqi Huang (University of Central Missouri), Jingze Dai (MacMaster University), Yili Jiang (Georgia State University), Sohan Gyawali (East Carolina University), Fangtian Zhong (Montana State University)

- In-Progress: Exploring Cybersecurity Risks and Solutions for Public Transit Agencies: A Nationwide Survey. Kiranben Jaysinh Dodia (University of Houston), Dr. Zia Ud Din (University of Houston), Yuhao Wang (University of Houston), Dr. Kailai Wang (University of Houston)

- Comparative Analysis and Evaluation of P4-Based Network Emulation Testing Environments. Dong Jin (University of Arkansas)

- Simulation Large-Scale Connected and Autonomous Vehicle Systems: An Agent-based Modeling Framework. Raj Kumar Konka (University of Houston), Yunpeng Zhang (University of Houston), Rakesh M Verma (Professor), Shun Cao (Assistant Professor)

- Safety and Performance Assurance for Swarm UAV Operations: A Survey. Rajdeep Singh (University of California, Santa Cruz), Iris Pellani (Ithaca College), Samuel Peccoud (Colorado State University), William Reimer (Embry-Riddle Aeronautical University), Sang Xing (Embry-Riddle Aeronautical University), Yujing Zhou (Embry-Riddle Aeronautical University), Yongxin Liu (Embry-Riddle Aeronautical University), Richard Stansbury (Embry-Riddle Aeronautical University), Hong Liu (Embry-Riddle Aeronautical University), Jian Wang (University of Tennessee at Martin)

- Mitigation of Phishing Attacks Through Comprehensive Education of Internet Users. Michael Andrews (University of Houston - Victoria), Dr. Daya Nand (University of Houston - Victoria)

- In-Progress: Structured Pruning in the Wild: Benchmarking Practical Robustness Under Real-World Corruptions. Jiamu Zhang (Rice University), Shaochen (Henry) Zhong (Rice University), Hoang Anh Duy Le (Rice University), Xia Hu (Rice University)

10:30-12:00 Paper Presentations

Full Paper Presentations (18 min for presentation and Q&A):

- Analyzing the Spatiotemporal Dynamics and Social Influences on the Transportation Cybersecurity Industry through a Business Visitor Flow Perspective. Yuhao Wang (University of Houston), Kailai Wang (University of Houston), Yunpeng Zhang (University of Houston)

- An Agent-based Model for Evaluating Connected and Autonomous Vehicles, Collective Behaviors and Traffic System Performance. Raj Kumar Konka (University of Houston), Rakesh M. Verma (University of Houston), Yunpeng Zhang (University of Houston), Shun Cao (University of Houston)

- Explainable Machine Learning for Cyberattack Identification from Traffic Flows. Yujing Zhou (Embry-Riddle Aeronautical University), Marc L. Jacquet (Embry-Riddle Aeronautical University), Robel Dawit (Embry-Riddle Aeronautical University), Skyler Fabre (Embry-Riddle Aeronautical University), Dev Sarawat (Embry-Riddle Aeronautical University), Faheem Khan (Embry-Riddle Aeronautical University), Madison Newell (Embry-Riddle Aeronautical University), Yongxin Liu (Embry-Riddle Aeronautical University), Dahai Liu (Embry-Riddle Aeronautical University), Hongyun Chen (Embry-Riddle Aeronautical University), Jian Wang (University of Tennessee at Martin), Huihui Wang (Northeastern University, Arlington)

Short Paper Presentations (7 min for presentation and Q&A):

- In-Progress: Hybrid Edge Intelligence for Real-Time Intrusion Detection in Advanced Traffic Management Systems. Rohith Reddy Depa (University of Houston), Yunpeng Zhang (University of Houston), Dianxiang Xu (Univesity of Missouri-Kansas City)

- In-Progress: Enhancing Traffic Signal Perception for Connected and Autonomous Vehicles (CAVs) via Multi-Sensor Fusion of Camera, LiDAR, Radar, and SPaT Data. A K M Sazzadul Alam (University of Houston), Xiali Hei (University of Louisiana at Lafayette), Yunpeng Zhang (University of Houston)

- In-Progress: Exploring Tire Pressure Monitoring Systems (TPMS) for Secure Key Generation for Intra-Vehicular Device Authentication. Omar Achkar (University of Houston), Shahryar Raza (University of Houston), James McAvoy (University of Houston), Rushikesh Shirsat Loyola University Chicago, Neil Klingensmith (Loyola University Chicago), Kyu In Lee (University of Houston)

- In-Progress: Reinforcement Learning for Cyberattack Defense in Autonomous Intersection Management Systems. Wesley Duclos (University of Tennessee at Martin), Yujing Zhou (Embry-Riddle Aeronautical University), Jian Wang (University of Tennessee at Martin), Qing Wang (University of Tennessee at Martin), Yongxin Liu (Embry-Riddle Aeronautical University), Huihui Wang (Northeastern University, Arlington)

- In-Progress: Augmenting Explainable AI with LLMs to Enhance User Trust in Intelligent Transportation Systems. Sohan Gyawali (East Carolina University), Yili Jiang (Georgia State University), Jiaqi Huang (University of Central Missouri)

12:00-1:00 Lunch Break (lunch will be provided by the conference)

1:00-2:30 Paper Presentations

Full Paper Presentations (18 min for presentation and Q&A):

- Do Adversarial Patches Generalize? Attack Transferability Study Across Real-time Segmentation Models in Autonomous Vehicles. Prashant Shekhar (Embry-Riddle Aeronautical University), Bidur Devkota (Embry-Riddle Aeronautical University), Dumindu Samaraweera (Embry-Riddle Aeronautical University), Laxima Niure Kandel (Embry-Riddle Aeronautical University), Manoj Babu (University of Warwick)

- Exploring Traffic Simulation and Cybersecurity Strategies Using Large Language Models. Lu Gao (University of Houston), Yongxin Liu (Embry-Riddle Aeronautical University), Hongyun Chen (Embry-Riddle Aeronautical University), Dahai Liu (Embry-Riddle Aeronautical University), Yunpeng Zhang (University of Houston), Jingran Sun (University of Texas at Austin).

- TrafficPulse: A Road-Sensor-Assisted Traffic Tweet Misinformation Detection System. Frank Ran (Rice University), Yifan Wu (Rice University), Delaram Pirhayatifard (Rice University), Joao Mattos (Rice University), Arlei Silva (Rice University).

Short Paper Presentations (7 min for presentation and Q&A):

- Privacy-preserving Mutual Authentication Protocol for Federated Learning in Intelligent Transportation Systems. Rohini Poolat Parameswarath (National University of Singapore), Biplab Sikdar (National University of Singapore)

- Demo: A Calibrated, Open-Source Toolkit for MitM Cyberattacks Visualization, Analysis, and Traffic Optimization at Connected Intersections. Yifan Xu (University of Cincinnati), Zhixia Li (University of Cincinnati), Heng Wei (University of Cincinnati), Guohui Zhang (University of Hawaii at Manoa), Yongxin Liu (Embry-Riddle Aeronautical University), Chen Chen (University of Cincinnati)

- Demo: Disrupting In-Car mmWave Sensing Through IRS Manipulation. Hanqing Guo (University of Hawaii at Manoa), Dong Li (University of Maryland, Baltimore County) , Ruofeng Liu (Michigan State University), Yao Zheng (University of Hawaii at Manoa)

- Demo; Abstract: A Probabilistic Model-based Deep Reinforcement Learning Strategy to Maximize Safety under Cyberattacks on A Connected Intersection - Bridging Stochasticity and Real-world Driving Data. Chen Chen (University of Cincinnati), Zhixia

Li (University of Cincinnati), Heng Wei (University of Cincinnati), Guohui Zhang (University of Hawaii at Manoa)
, Yifan Xu (University of Cincinnati).

2:30-3:00 Break (Poster Session)

Posters:

- Protecting Connected and Autonomous Vehicles from Laser Attacks on Traffic Signals Using Vehicle to Everything Communication. A K M Sazzadul Alam (University of Houston), Mansoureh Jeihani (Morgan State University), Ehsan Mahryaar (Morgan State University), Yunpeng Zhang (University of Houston)

- Classifier-Aware Defense for Visual Recognition in Connected Autonomous Vehicles. Bill Deng Pan (Embry-Riddle Aeronautical University), Richard Guo (Irvine Valley College), Dahai Liu (Embry-Riddle Aeronautical University), Hongyun Chen (Embry-Riddle Aeronautical University), Yongxin Liu (Embry-Riddle Aeronautical University)

- In-Progress: Enhancing Cybersecurity in Advanced Traffic Management Systems by Detecting Evasion and False Data Injection Attacks. Venkata Naga Sai Ram Nomula (University of Houston), Yunpeng Zhang (University of Houston), Suxia Cui (Prairie View A&M University), Ed Pearson (Alabama A&M University), Xiang Zhao (Alabama A&M University)

- In-Progress: Blockchain-Based Secure Data Exchange in ATMS with End-to-End Encryption (E2EE). Narayan Soni (University of Houston), Yunpeng Zhang (University of Houston), Dakai Zhu (The University of Texas at San Antonio)

- In-Progress: CNN-Based Misbehavior Detection with Batch Message Verification for V2X Communications. Jiaqi Huang (University of Central Missouri), Jingze Dai (MacMaster University), Yili Jiang (Georgia State University), Sohan Gyawali (East Carolina University), Fangtian Zhong (Montana State University)

- In-Progress: Exploring Cybersecurity Risks and Solutions for Public Transit Agencies: A Nationwide Survey. Kiranben Jaysinh Dodia (University of Houston), Dr. Zia Ud Din (University of Houston), Yuhao Wang (University of Houston), Dr. Kailai Wang (University of Houston)

- Comparative Analysis and Evaluation of P4-Based Network Emulation Testing Environments. Dong Jin (University of Arkansas)

- Simulation Large-Scale Connected and Autonomous Vehicle Systems: An Agent-based Modeling Framework. Raj Kumar Konka (University of Houston), Yunpeng Zhang (University of Houston), Rakesh M Verma (Professor), Shun Cao (Assistant Professor)

- Safety and Performance Assurance for Swarm UAV Operations: A Survey. Rajdeep Singh (University of California, Santa Cruz), Iris Pellani (Ithaca College), Samuel Peccoud (Colorado State University), William Reimer (Embry-Riddle Aeronautical University), Sang Xing (Embry-Riddle Aeronautical University), Yujing Zhou (Embry-Riddle Aeronautical University), Yongxin Liu (Embry-Riddle Aeronautical University), Richard Stansbury (Embry-Riddle Aeronautical University), Hong Liu (Embry-Riddle Aeronautical University), Jian Wang (University of Tennessee at Martin)

- Mitigation of Phishing Attacks Through Comprehensive Education of Internet Users. Michael Andrews (University of Houston - Victoria), Dr. Daya Nand (University of Houston - Victoria)

- In-Progress: Structured Pruning in the Wild: Benchmarking Practical Robustness Under Real-World Corruptions. Jiamu Zhang (Rice University), Shaochen (Henry) Zhong (Rice University), Hoang Anh Duy Le (Rice University), Xia Hu (Rice University)

3:00-4:00 Keynote

Speaker: David Balenson, Senior Supervising Computer Scientist, Interim Director, Networking and Cybersecurity Division in the Information Sciences Institute at University of Southern California

Title: Catalyzing Cybersecurity Research in Transportation: Datasets, Tools, and Community via PIVOT

Abstract:
As vehicles become increasingly connected and autonomous, the availability of telematics and other vehicular data—along with the tools to analyze them—is essential for advancing research and building applications that enhance both vehicle systems and their surrounding environments. However, such datasets remain scarce and fragmented, due in part to the technical challenges of data collection and the privacy concerns involved. To unlock the full potential of vehicle-based innovation, the research community needs open access to diverse, high-quality datasets and tools. The Platform for Innovative use of Vehicle Open Telematics (PIVOT) is an NSF-funded, community-driven initiative designed to support the sharing and use of datasets and tools relevant to automotive and heavy-duty vehicle research. PIVOT supports researchers and practitioners working in areas such as vehicle system cybersecurity, intelligent transportation systems, and smart and connected communities.

This talk will provide an overview of the PIVOT platform, highlighting the types of datasets and tools being cataloged and shared. It will also showcase a number of ongoing research efforts in automotive and autonomous vehicle security that are leveraging or contributing to the platform.

Ongoing efforts include development of a custom driving simulator, techniques for extracting personally identifiable information (PII) from infotainment systems, and classification methods for automated driving systems. Additional work focuses on building an automotive CAN logger, analyzing remote attack surfaces in electronic logging devices (ELDs) used in commercial trucks, and studying truck driver behavior through data collection and analysis. Other research includes enhancing the SPHERE testbed for experimentation with simulated and real vehicles, and applying privacy patterns and privacy-enhancing technologies (PETs) to data collected by autonomous vehicles such as robotaxis. The talk will also summarize broader community engagement activities, including PIVOT-hosted workshops and related conferences focused on the intersection of transportation and cybersecurity.

Bio: David Balenson is the Interim Director of the Networking and Cybersecurity Division and a Senior Supervising Computer Scientist at the University of Southern California's Information Sciences Institute (USC-ISI). He has extensive experience in critical infrastructure security and resilience, computer and network security, applied cryptography, and R&D program and project management. His current research interests include cybersecurity for critical infrastructure and cyber-physical systems—including automotive and autonomous vehicles—as well as experimentation and test, technology transition, and multidisciplinary research.

Balenson co-leads and serves as Community Outreach Director for two NSF-funded projects: the Open Community Platform for Sharing Vehicle Telematics Data for Research (PIVOT) and the Security and Privacy Heterogeneous Environment for Reproducible Experimentation (SPHERE). He previously co-led the Sharing Expertise and Artifacts for Reuse for Cybersecurity Community Hub (SEARCCH) and the Cybersecurity Experimentation of the Future (CEF) projects, also funded by NSF.

Balenson serves on the program, organizing, and/or steering committees for several prominent events in the field, including the ASRG Secure Our Streets (SOS) Conference, Vehicle Security and Privacy (VehicleSec) Symposium, Annual Computer Security Applications Conference (ACSAC), Learning from Authoritative Security Experiment Results (LASER) Workshop, and Cyber Security Experimentation and Test (CSET) Workshop.

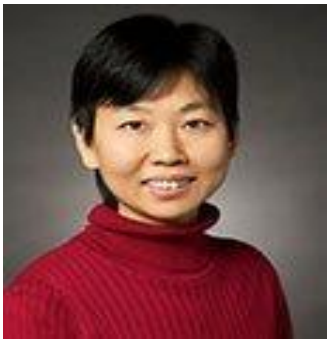
Before joining USC-ISI, Balenson was a senior computer scientist in the Computer Science Laboratory at independent, non-profit research institute, SRI International where he provided technical and programmatic support for the U.S. Department of Homeland Security Science and Technology Directorate (DHS S&T). Earlier in his career, he held positions at the Johns Hopkins University Applied Physics Laboratory, SPARTA, McAfee/Network Associates, Trusted Information Systems, and the National Institute of Standards and Technology. He holds B.S. and M.S. degrees in Computer Science from the University of Maryland.

4:00-5:00 Panel: Preparing the New Generation of Cybersecurity and Transportation Experts for the Challenges of the Next Decade

Panelists:

Jun Dai, Associate Professor of Computer Science at Worcester Polytechnic Institute

Bio: Dr. Jun Dai is currently an Associate Professor in Department of Computer Science at Worcester Polytechnic Institute (WPI). His research interests mainly lie in the intersections of network and distributed system, AI, and cybersecurity, with recent focus on intrusion detection, vulnerability analysis, secure programming, and cybersecurity education. Dr. Dai has published papers in prestigious academic venues, such as NDSS, ACM SIGMOD, IEEE TIFS, and ACM SIGCSE. He is the Workshop Chair of ACM CCS 2023, and has been a reviewer for top journals like TIFS, TDSC, TVT, and TMC. His projects are mainly funded by NSF and other grant agencies. Dr. Jun Dai earned a BS in Information Security in 2007 and an MS in Network Control in 2010 from the University of Science and Technology of China (USTC), and a PhD in Information Sciences and Technology from the Pennsylvania State University (PSU) in 2014 with specialization in cybersecurity.



Huirong Fu, Distinguished University Professor

Bio: Dr. Huirong Fu is a Distinguished Professor at Oakland University (OU) with extensive research expertise in cybersecurity, applied cryptography, trust management, and privacy. She has authored over 100 peer-reviewed journal and conference papers. Dr. Fu has been serving as Principal Investigator (PI) for more than a dozen federally funded projects, including the NSF REU and NSF SFS programs, Lead PI of the NSA/NSF Oakland GenCyber Coalition, and Lead PI of the NSA NCAE-C DRIFT Coalition - DRiving Automotive Industry WorkForce Transformation: Excellence and Innovation in Cybersecurity and Artificial Intelligence. Since 2016, she has served as the Founding Director of the OU Center for Cybersecurity, leading efforts that established OU's cybersecurity capacity and secured its designation as a National Center of Academic Excellence in Cyber Defense (NCAE-C) by the NSA and DHS in 2018, with re-designation in 2024.

5:00-5:15 Closing remarks and awards