CRII:CPS: Cooperative Neuro-Inspired Actor Critic Model for Anomaly Detection in Connected Vehicles

Heena Rathore, PhD
Assistant Professor, Texas State University
https://www.nsf.gov/awardsearch/showAward?AWD_ID=2313351

Challenges:

The number of Connected Vehicles (CV) in the United States is predicted to reach 146 million by 2030. They are equipped with sensors and communication devices capable to communicate with vehicles and infrastructure. These sensors can be compromised with malicious actors or can be manifested with faults which lead to erroneous measurements. This project tasks include:

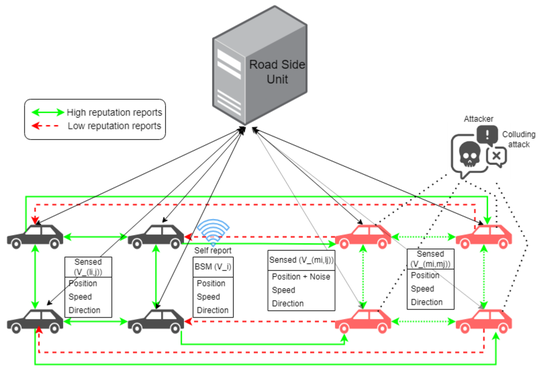
1. Develop novel algorithmic methods for classifying different types of sensor failures and learning new anomalous attacks in CV networks.
2. Design scalable safe multi-agent reinforcement learning (RL) models to build trust and reputation among the CVs for effective information sharing.
3. Develop new consensus-based protocols for CVs to provide resilience and adaptivity in the presence of malicious activity in the network.

Solutions:

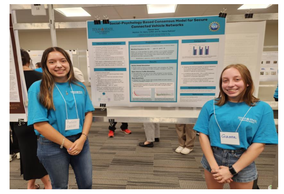
- Developed approaches to encompass peer-based measurements, in addition to self-reported measurements from individual vehicles, to establish trust-based frameworks [1].
- Developed graph neural network with RL algorithms to enable vehicles to create reputation estimates of their nearby vehicles by analyzing broadcasted kinematic data and onboard sensor estimates, as well as the network connectivity topology [2].
- Developed social psychology inspired distributed acyclic graph for enabling classification between attacks and faults [3]. Developed social psychology inspired algorithms to address colluding malicious vehicle attacks.

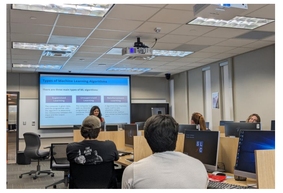
Scientific Impact

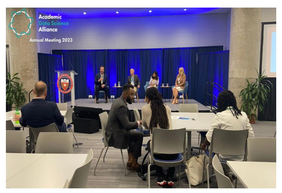
- By classifying sensor failures, malicious attacks, the algorithms can be generalized to other CPS application that involve sensor-based systems, multi-agent systems, and suffer security and conflict related challenges.
- The novel RL algorithms developed for anomaly detection in CV can be applied to other security problems in CPS where data integrity is important.
- Trust and reputation-based algorithms can be further scaled to enhance moral uncertainty for CV where virtue ethics (ethical theory) can enable multi agent collaborations.
- In terms of pedagogical methods, the project have involved the development of educational materials for the UG class CS4371 and graduate class CS5378 and CS7389F.



Majority-Malicious Vehicles
(a)


(b) NSF REU


(c) Transfer Bridge


(d) ADSA Panel


(e) NSF stEM Peer

Broader Impacts (Impact on Society)

- Enhanced Safety and Security: Detection and classification of sensor failures helps prevent accidents mitigate their effects by alerting drivers and triggering appropriate safety measures.
- Mitigation of Malicious Attacks: Algorithms can facilitate secure information sharing, collaborative learning, and collective decision-making processes, thereby reducing the risk of malicious attacks.

Broader Impact (Education and Outreach)

- Focused on curriculum development to expand the scale and diversity of the CPS security workforce [4].
- NSF stEm PEER Academy Fellow for building transfer pipelines from community colleges to Texas State University.
- Developed accelerated pathways in data science and AI, with AWS, Academic Data Science Alliance (ADSA).
- Supporting Mentor for Texas State University NSF REU.

Boarder Impact (Quantify Potential Impact)

- Two REU students published manuscripts: one at the ACM REUNS Mobihoc 2023 and the other at the IEEE 42nd ICCE conference. Additionally, the findings of a group project involving five UG students from CS4371 were disseminated in IEEE IOTSMS 2023.
- 3 Transactions papers and 14 conference papers published. These publications have received a total of 20+ citations.

[1] H. Griffith, M. Farooq and H. Rathore, "A Data Generation Workflow for Consensus-Based Connected Vehicle Security," 2023 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2023, pp. 1-2, doi: 10.1109/ICCE56470.2023.10043181.
[2] H. Rathore and H. Griffith, "Leveraging Neuro-Inspired Reinforcement Learning for Secure Reputation-based Communication in Connected Vehicles," 2023 IEEE Conference on Communications and Network Security (CNS), Orlando, FL, USA, 2023, pp. 1-6, doi: 10.1109/CNS59707.2023.10289058
[3] H. Rathore, S. Sai and A. Gundewar, "Social Psychology Inspired Distributed Ledger Technique for Anomaly Detection in Connected Vehicles," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 7, pp. 7092-7107, July 2023, doi: 10.1109/TITS.2023.3262398
[4] H. Rathore, "Integrating Cyber Physical System Security Concepts in Computer System Security Curriculum," 2023 IEEE Integrated STEM Education Conference (ISEC), Laurel, MD, USA, 2023, pp. 397-399, doi: 10.1109/ISEC57711.2023.10402293..

Award ID# 2153510 and # 2313351