CPS: Breakthrough: Collaborative Research: Track and Fallback: Intrusion Detection to Counteract Carjack Hacks with Fail-Operational Feedback

Gedare Bloom, University of Colorado Colorado Springs

Joseph Zambreno, Iowa State University

https://rcl.ece.iastate.edu/projects/CAN-Security

Abstract: Vehicle cybersecurity becomes more important as cars become more connected and intelligent. The objective of this project is to protect in-vehicle networks using an intrusion detection system (IDS) with novel approaches to address the physical uncertainty and resource constraints of automotive control systems.

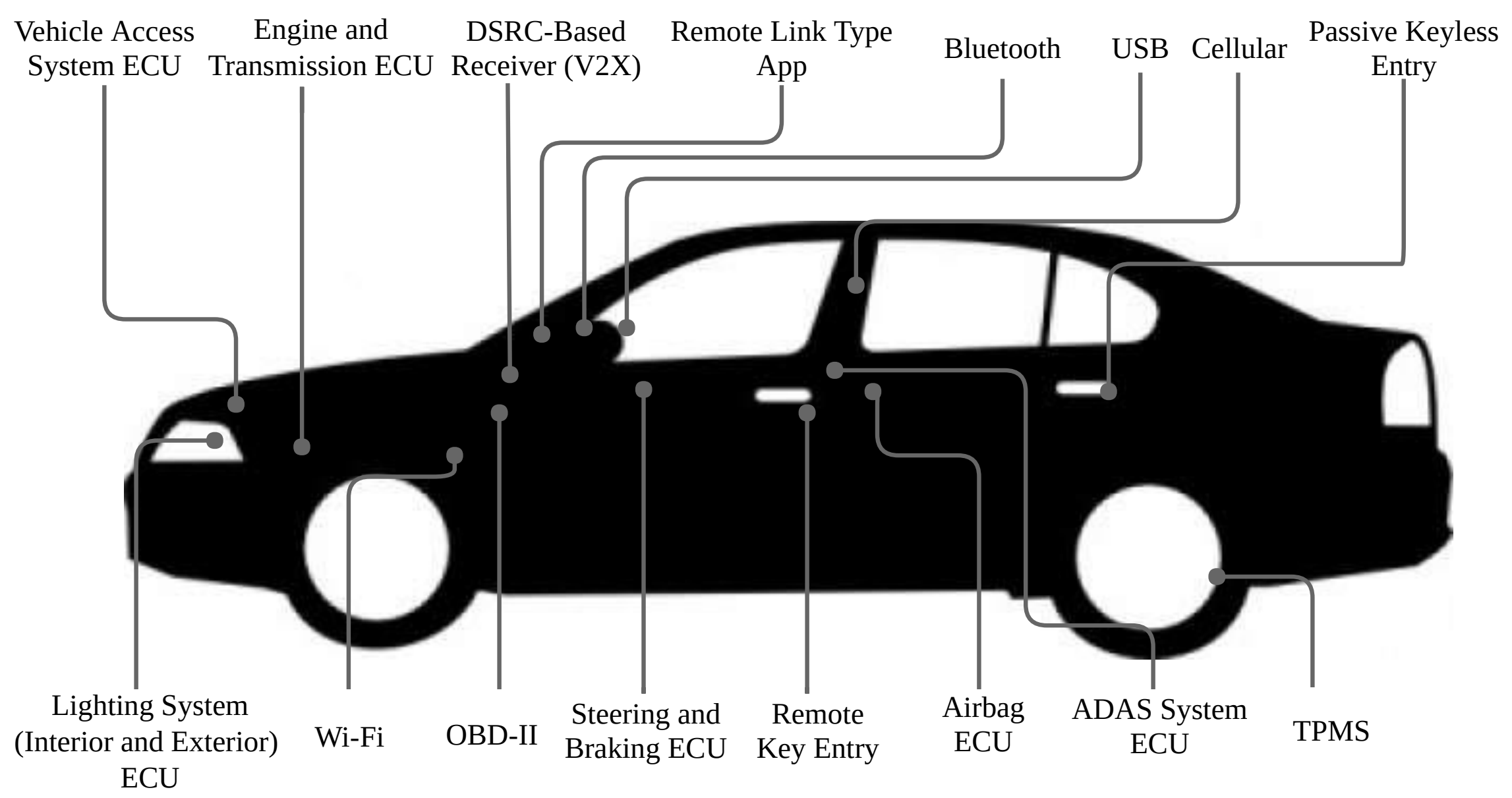
Challenge

Automotive cybersecurity is a risk to human safety

Increasing complexity

Increasing connectivity

Increasing attack surfaces



Drivers are not cyber savvy

- Need for automation and exact security mechanisms

Scientific Impact

IDS techniques may generalize to other CPS

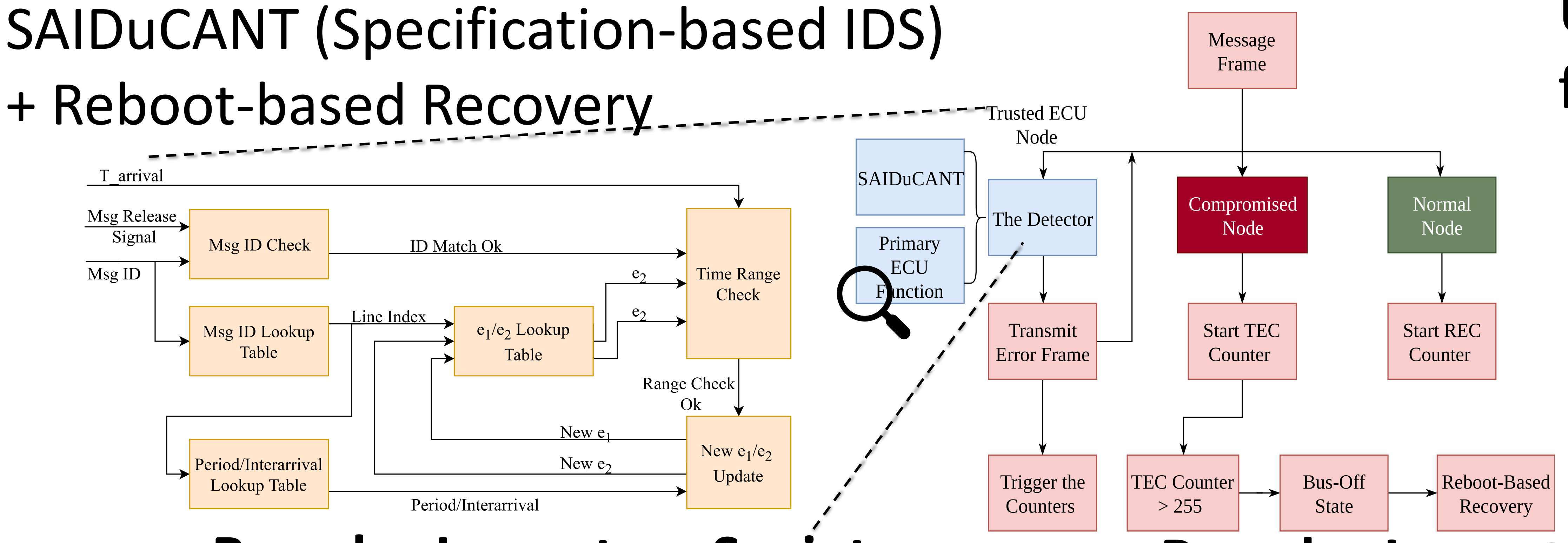
- Specification-based approach based on real-time theory
- Frequency and CUSUM techniques rely on CPS regularity

Machine Learning to understand relationship between cyber and physical components

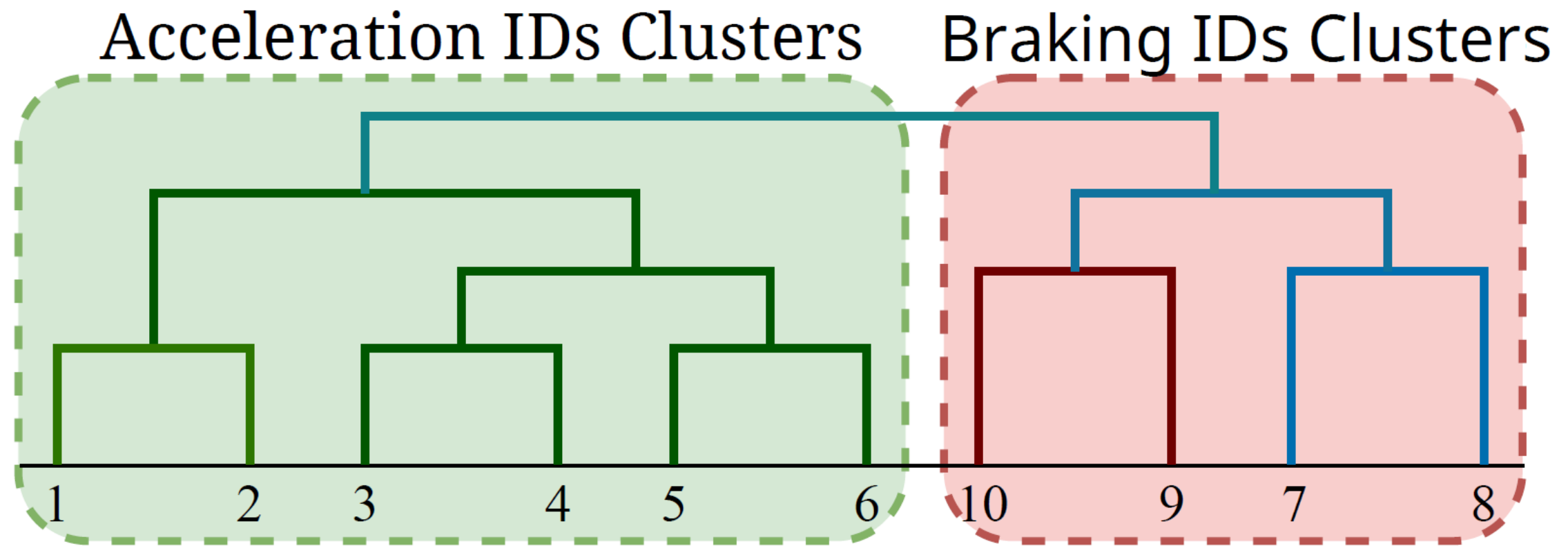
New understanding of attacks stimulates further discovery

Technical Approach

SAIDuCANT (Specification-based IDS) + Reboot-based Recovery



Unsupervised Learning for CAN ID function reverse engineering

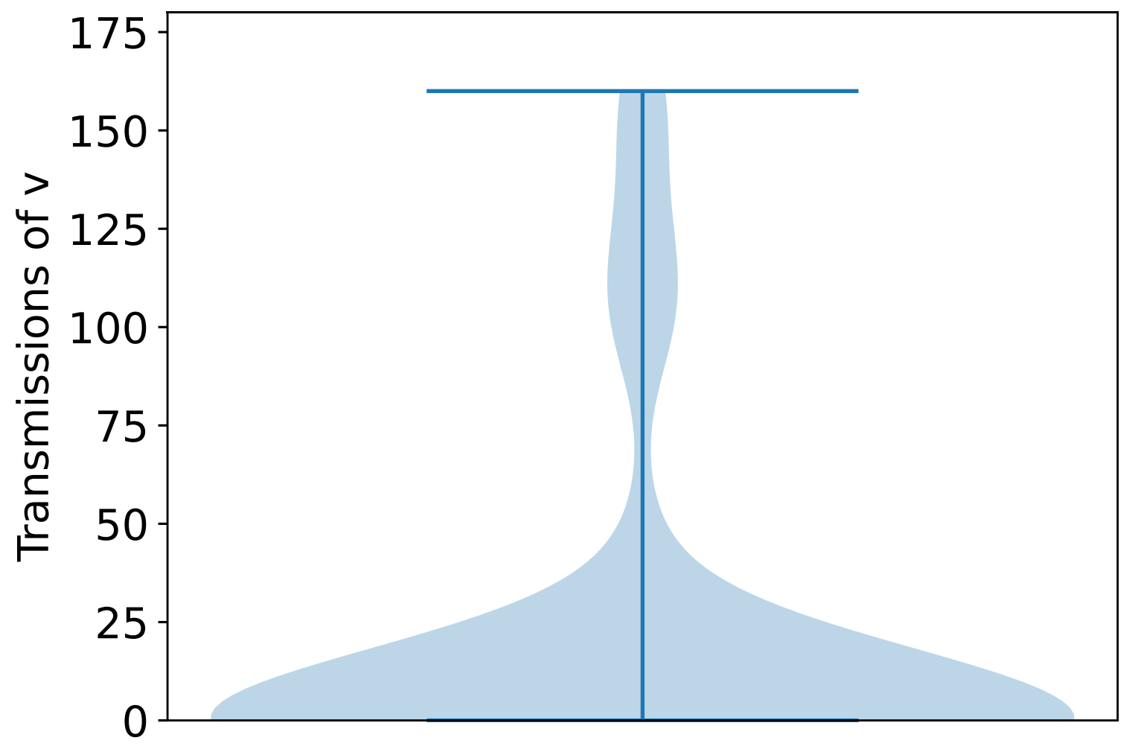


Driving functions grouped by ID with good performance on cars and tractors

WeepingCAN Stealthy Bus-off

Attacker transmissions over 75 trials

0 transmissions most of the time



Attack works in a live vehicle test

Broader Impact on Society

- ➢ Increase resilience of infrastructure
- ➢ Strong engagement with industry
- ➢ Broadening Participation
  - ➢ 2 Black PhD students, 4 Black REU students

Broader Impact on Education/Outreach

- ➢ Mentoring in open-source software
- ➢ 4 PhD students supported
  - ➢ 3 PhD students graduated
- ➢ 6 REU students trained in research

Other Broader Impacts

- ➢ Share datasets and research tools
- ➢ New collaborations formed
  - ➢ Cummins, NMFTA, John Deere, Italian National Research Council, NXP Semiconductors, RTI Inc., Altia

2021 NSF Cyber-Physical Systems Principal Investigators' Meeting
June 2-4, 2021

2011620, Univ. of Colorado Colorado Springs
1645987, Iowa State University