# Detecting and Reconstructing Network Anomalies and Intrusions in Heavy Duty Vehicles

Indrakshi Ray, Computer Science Department, Colorado State University

https://rayscyberlab.org/home/projects/heavy-vehicle-security/

- SAE J1939 protocol for internal communication in heavy vehicles
- Attack detection and mitigation in real-time under resource constraints
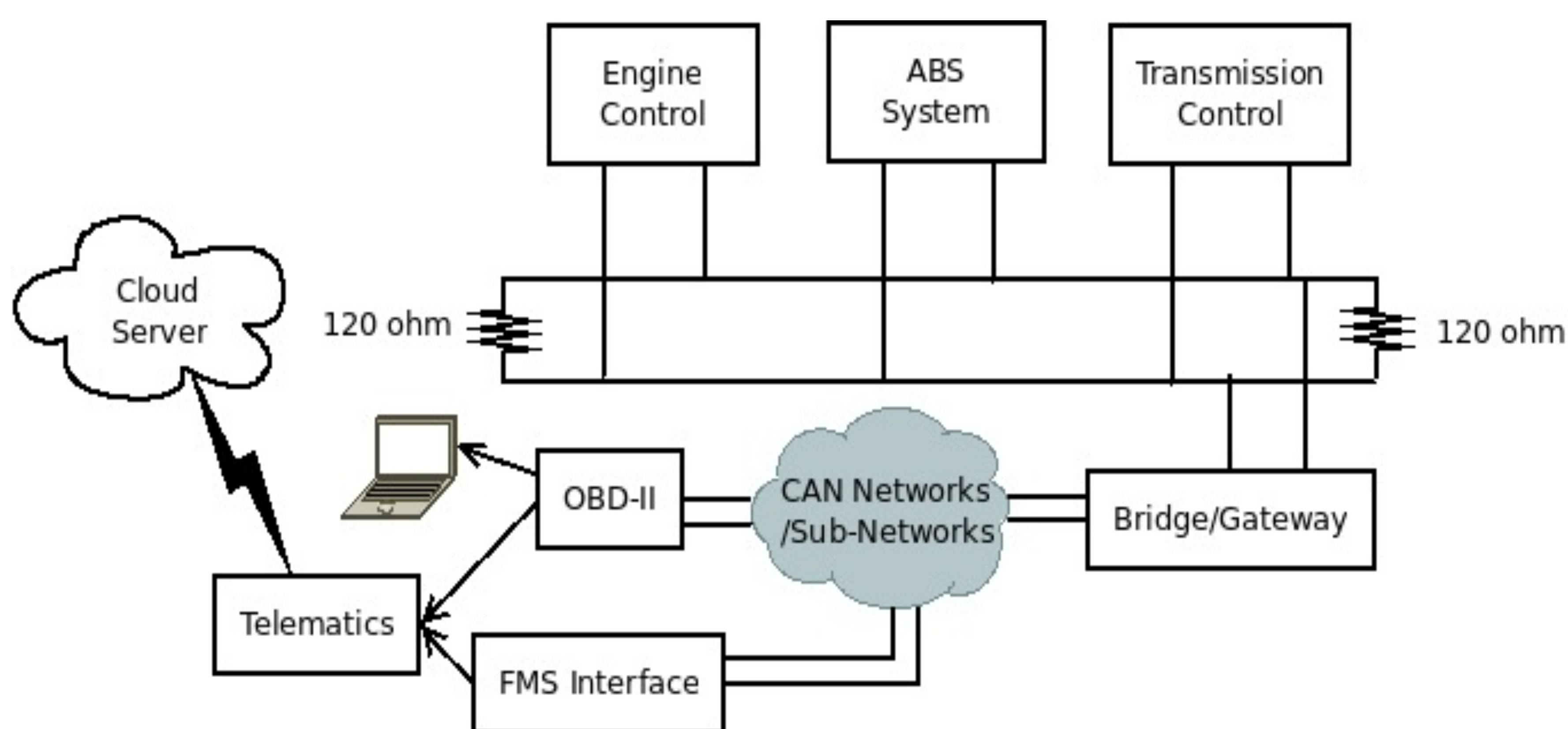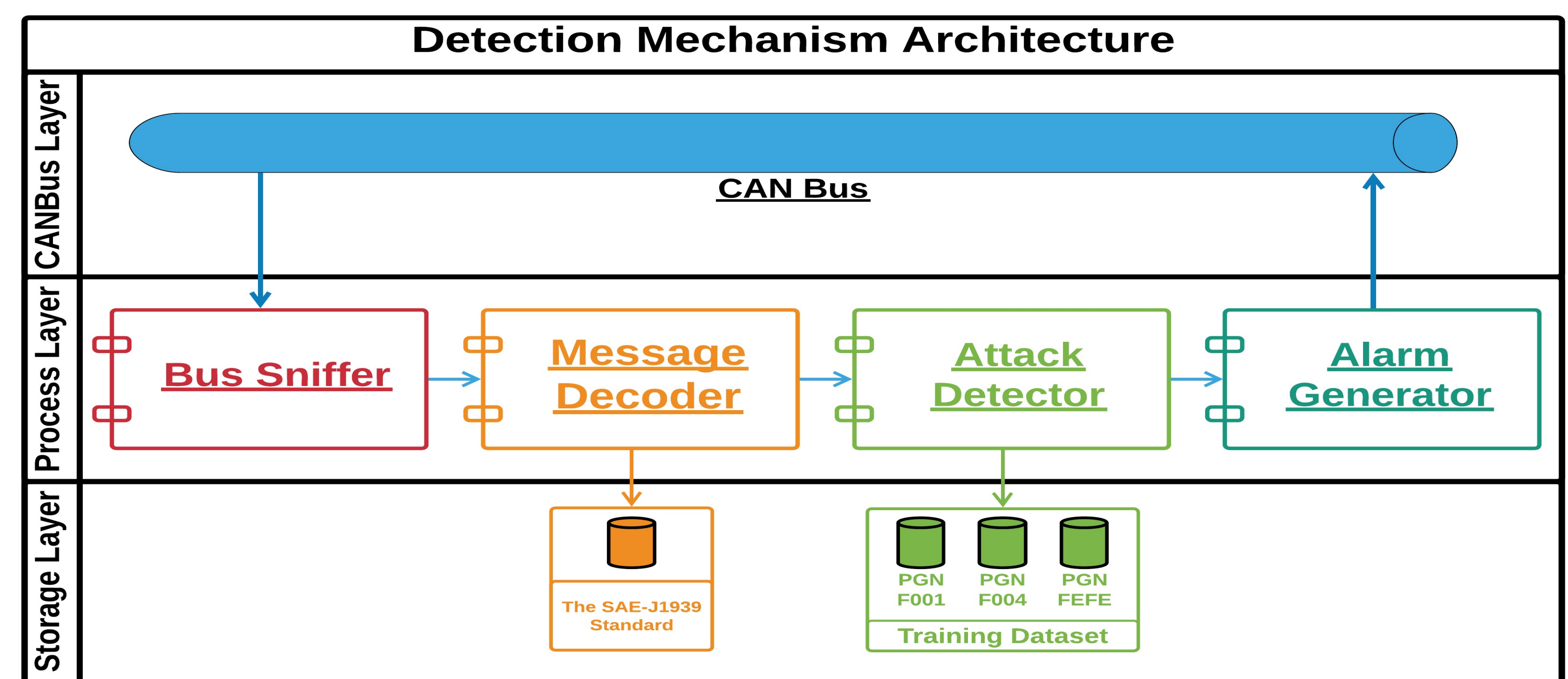

- **Scientific Impact**
- Investigating how to use data from multiple sources collectively for anomaly detection and compromised value reconstruction
- Investigating how redundancies in CPS can be used for resiliency

- **Solution**
- Using ML to fingerprint ECU behavior for anomaly detection
- Using predictive analytics to reconstruct values of compromised ECUs

- **Broader Impacts**
- Direct Stakeholders
  - Heavy vehicle fleet managers
  - US Military
- Research Stakeholders
  - Heavy vehicle manufacturers
  - Heavy vehicle security researchers

- **Broader impact and education participation**
- Educating students in multiple disciplines
- Engaging NMFTA and OEMs
- Cyber truck Challenge Competition

- **Broader Impact and Broader Participation:**
- SAE refined specs after revealing potential attacks
- Mentored two minority students
- Mentored two 1st gen students
  - Hired by TESLA, PwC

NSF Award No. NSF CNS 1715458