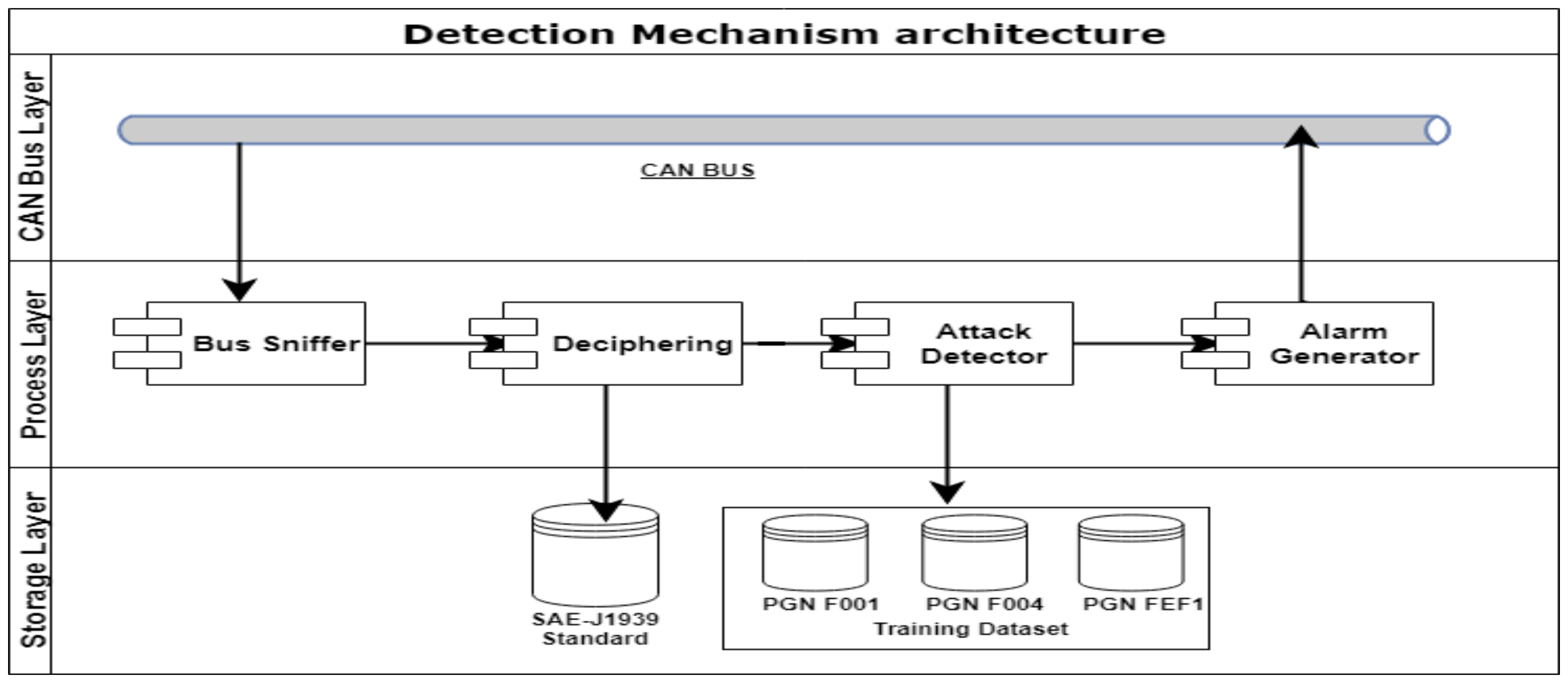
Machine Learning for Anomaly Detection in Heavy Vehicles

Indrakshi Ray, Computer Science Department, Colorado State University

https://www.cs.colostate.edu/dbsec/HeavyVehicle/

- Automobiles have embedded devices (ECUs) to improve safety, efficiency, reliability, and drivability
- ECUs connected over CAN bus are vulnerable to attacks
- SAE-J1939 protocol executes over CAN bus in heavy vehicles

- How do we define normal behavior in heavy vehicles?
- How do we identify anomalies in real-time?



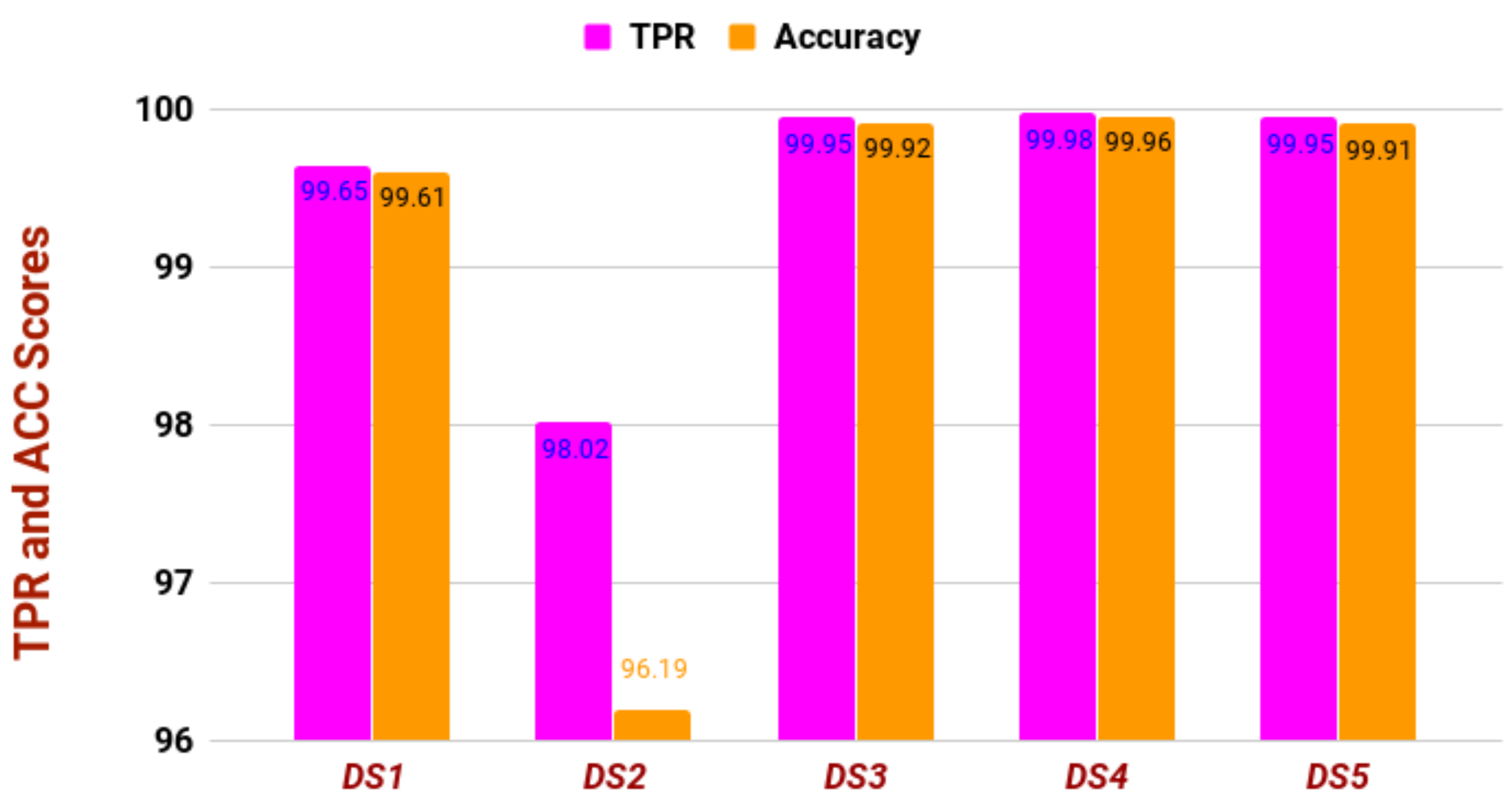
Detection Mechanism architecture

- Modeling regular behavior of ECUs
- Developing profiles by employing machine learning to analyze high-dimensional data generated by the ECUs and detecting anomalies
- Similar machine learning techniques can be used to detect anomalies in IoT devices

- *BusSniffer* connects to the bus and sniffs the messages
- *Message Decoder* converts messages into vehicle's parameters
- *Attack Detector* compares the current state with the appropriately trained model
- *Alarm Generato*r generates alarm if a threat exists

- Anomaly Definition
  - Vector appears out of order
- Attacker Capability
  - Receives all messages on the bus
  - Capable of generating SAE-J1939 message compatible

Weighted average of TPR and accuracy for datasets



- Proposed the use of machine learning for anomaly detection in SAE-J1939 messages
- Proposed modular algorithm uses to generate warning alarms in real-time
- Directly benefits the automotive society

- Graduate students supported
- REU students (1st generation, minority, special needs) supported
- Student participation in Cyber Truck Challenge
- Exposing vulnerabilities in trucks

- Heavy vehicles form nation's infrastructure
- Identifying anomalies in a timely manner can thwart attacks
- Research techniques on machine learning can be applied to other CPS systems, such as, IoT