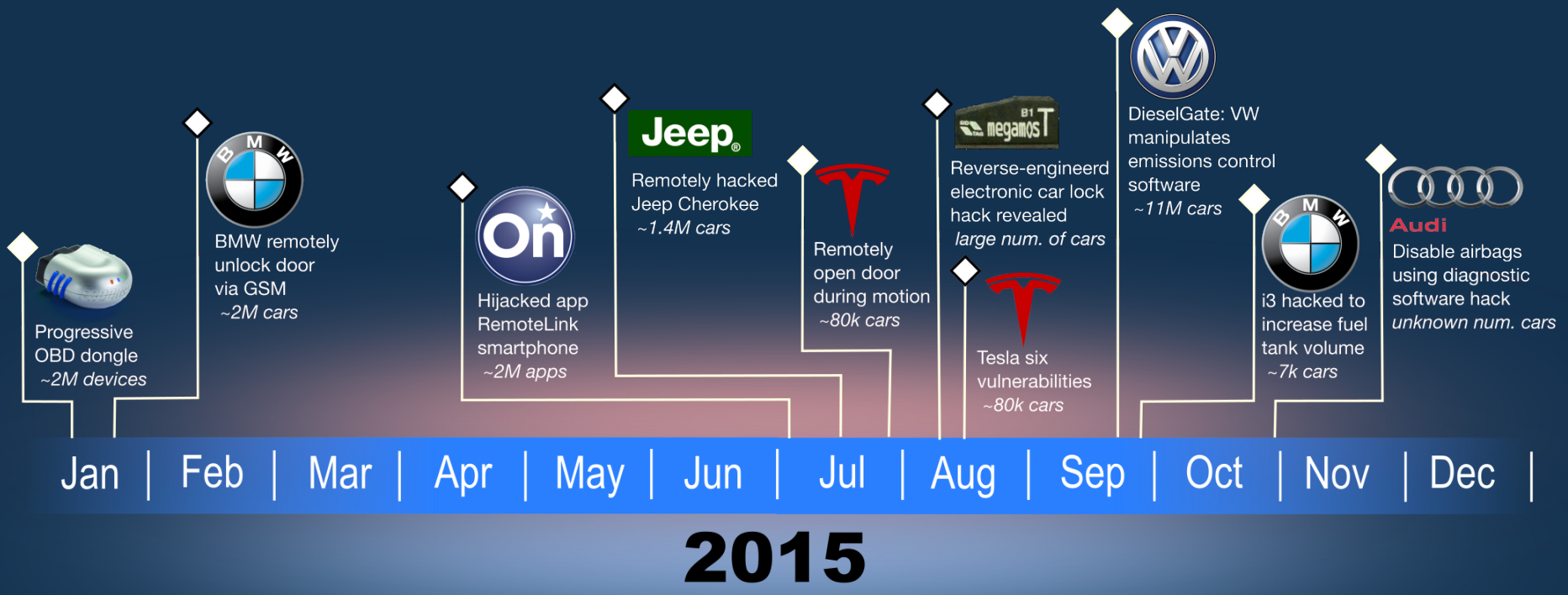
Automotive Intrusion Detection using Reference Models

Armin Wasicek
University of California, Berkeley
Technical University Vienna, Austria

MT-CPS Workshop

April 11, 2016

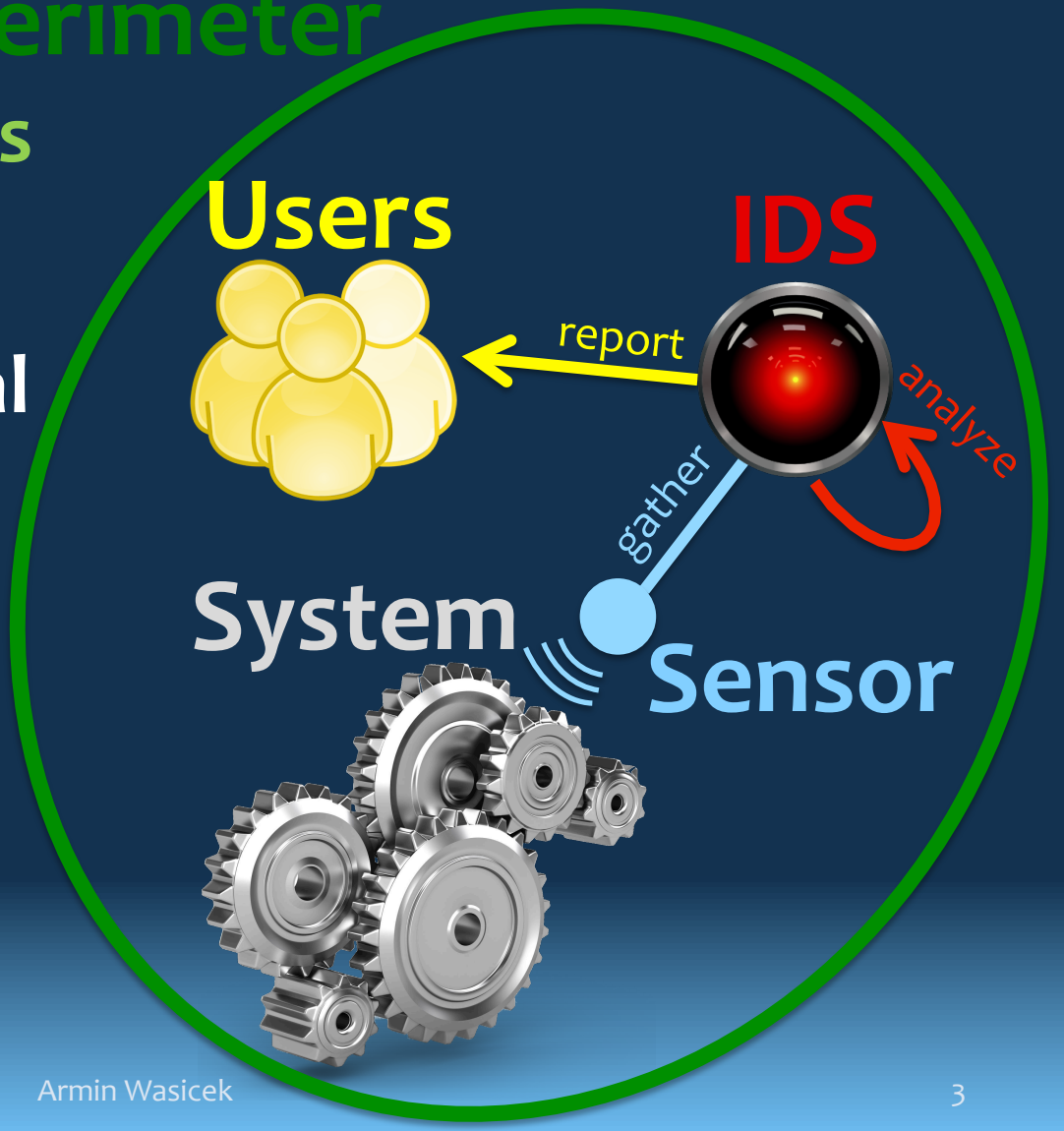
2015 Automotive Security Incidents



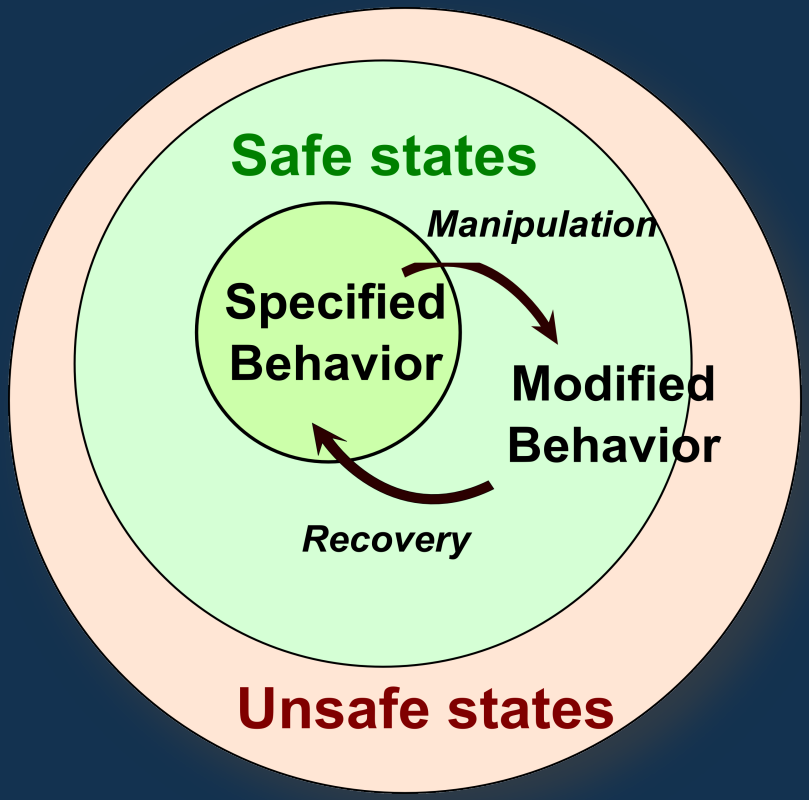
What is Intrusion Detection?

Gathers and analyzes information

- **Identifies potential security breaches**
  - Intrusions
  - Misuse/Fraud
- **Reports to users**



Manipulation and Fault tolerance

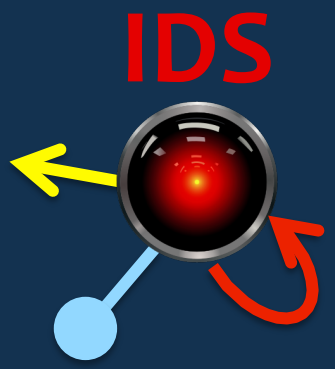


- Triggering unsafe states will stop the system
- **Manipulations are subtle**
- Stay within safe states, but modified behavior
- Recognition and Recovery

NTHSA: **Misbehavior Detection** [DOT HS 812 014]

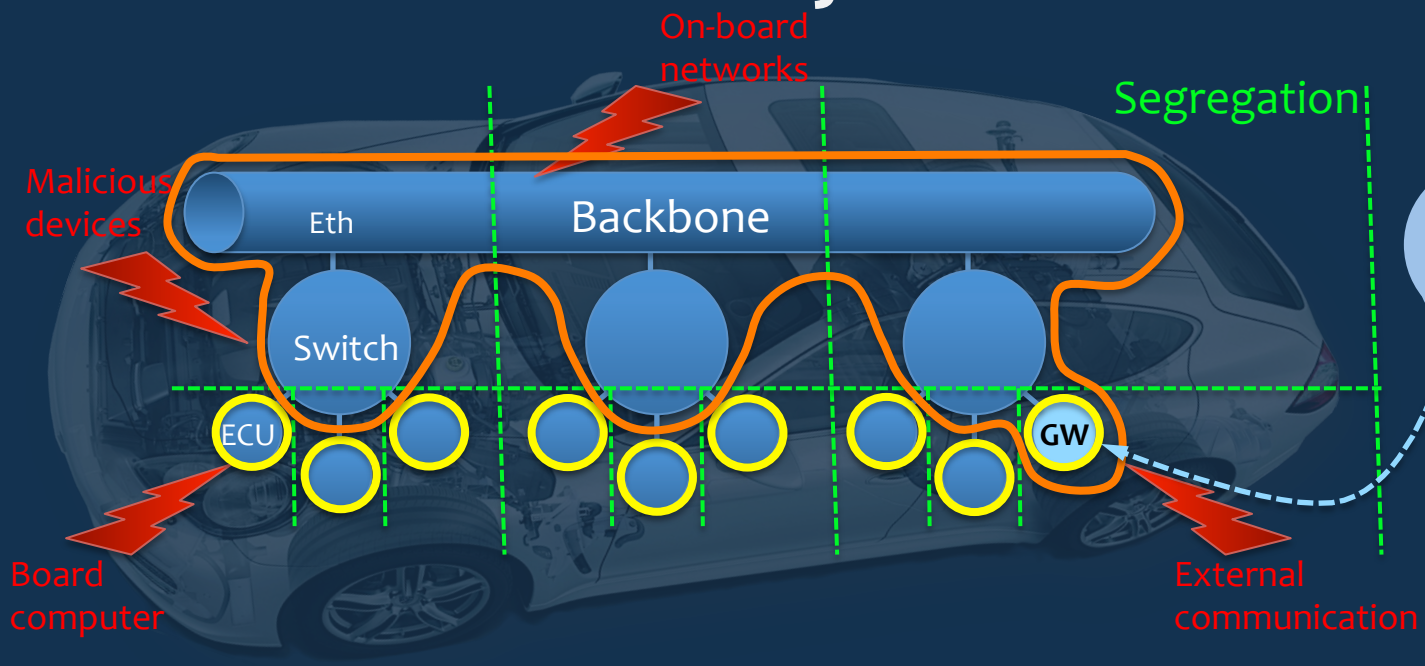
Development of the processes, algorithms, reporting requirements, and data requirements for ***both local and global detection functions***;

Types of IDS



- **Knowledge-based IDS**
  - Patterns/Signatures of malicious activities
  - Low false positive rate, needs frequent updates
- **Heuristic-based IDS**
  - Look for abnormal behavior, e.g., higher entropy
  - Detect new attack patterns
- **Context-aware IDS**
  - Compare to reference model, include *semantics*
  - Check against specifications and regulations

Automotive System Architecture



- **Host-based IDS** monitors ECU
  - CPU & memory usage, syscalls, # processes, …
- **Network IDS** monitors communication
  - Message frequency, patterns, entropy, …

Identify anomalies and outliers

Chip tuning

Modify control algorithm parameters in ECU

- Parameters are stored in a table in flash memory
- Reprogram ECU with new values
  - Debug interface, 3rd party device

► **Messages emitted by ECU seem original!**

Power boxing

Improves low end torque. Plug-in installation in less than 30 minutes.

Modify commands to ECU

- Replace the ECU in the communication system
- Insert device between the ECU and actuators

► **Communication pattern does not change!**

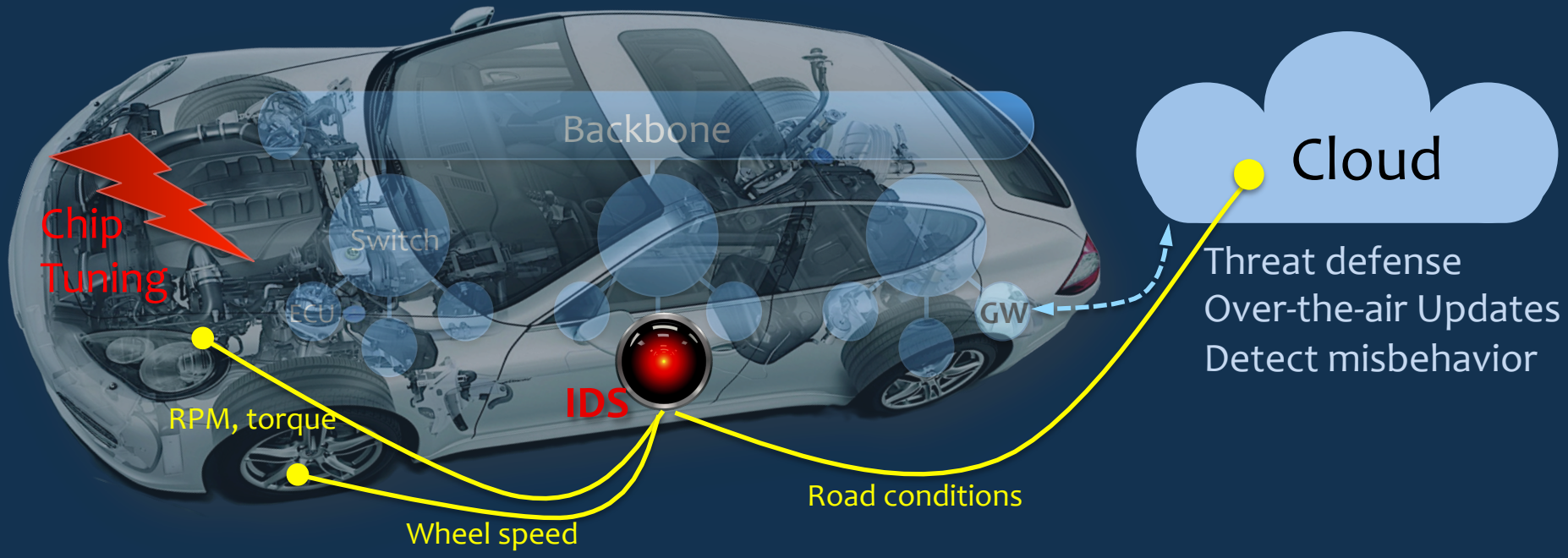
Cyber-Physical Attacks

Automotive systems are Cyber-Physical

- Checking only cyber properties like CAN message frequency might miss important attack vectors
- IDS needs to target attack on the physical part

► **Compare actual behavior to reference model enabling *misbehavior* detection**

Automotive System Architecture

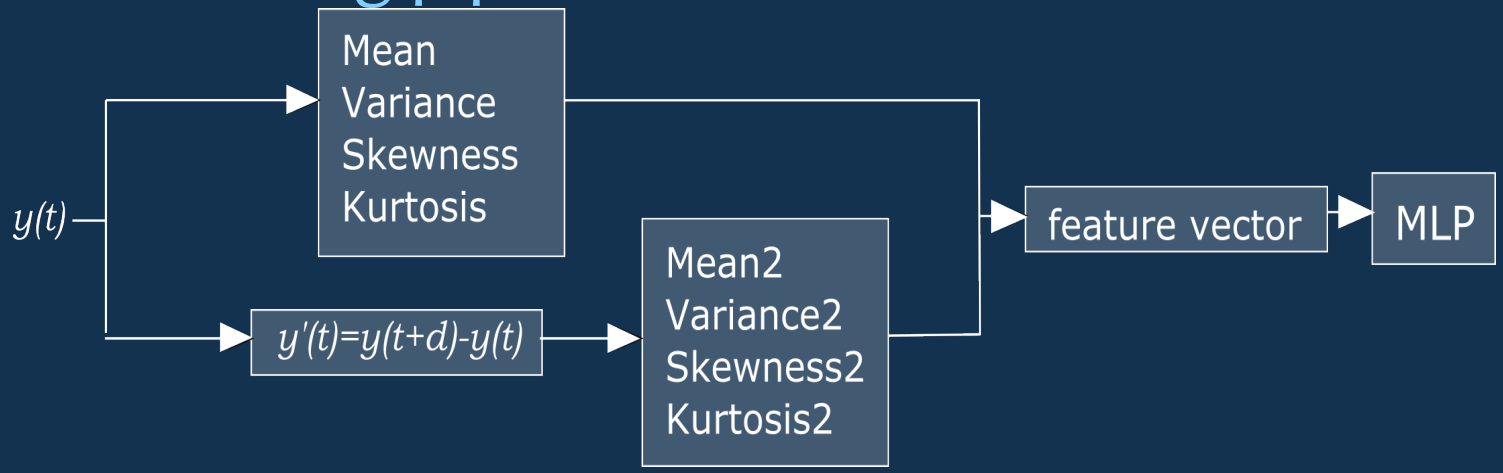


- Integrate firewall, authentication, and detection
- Fuse information from diverse sources
- **Use semantics of control msg to reason about manipulation**

Feature Extraction

Convert a time series to a feature vector

Processing pipeline works on a time slice

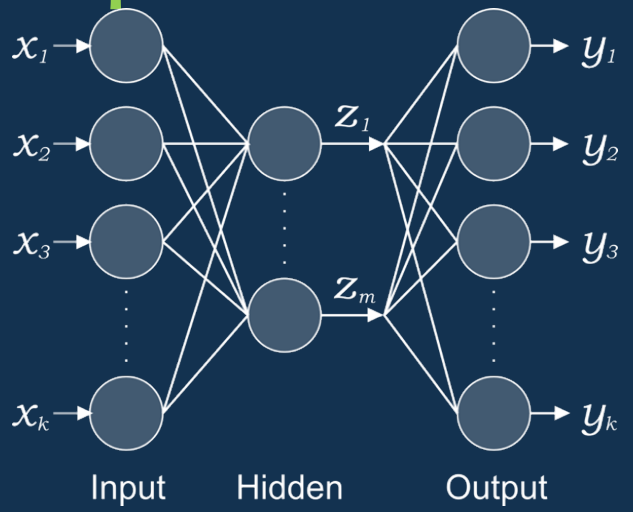


- **Compute feature vector storing the relations between process variables**

Artificial Neural Networks

Frame as a one-class classification problem

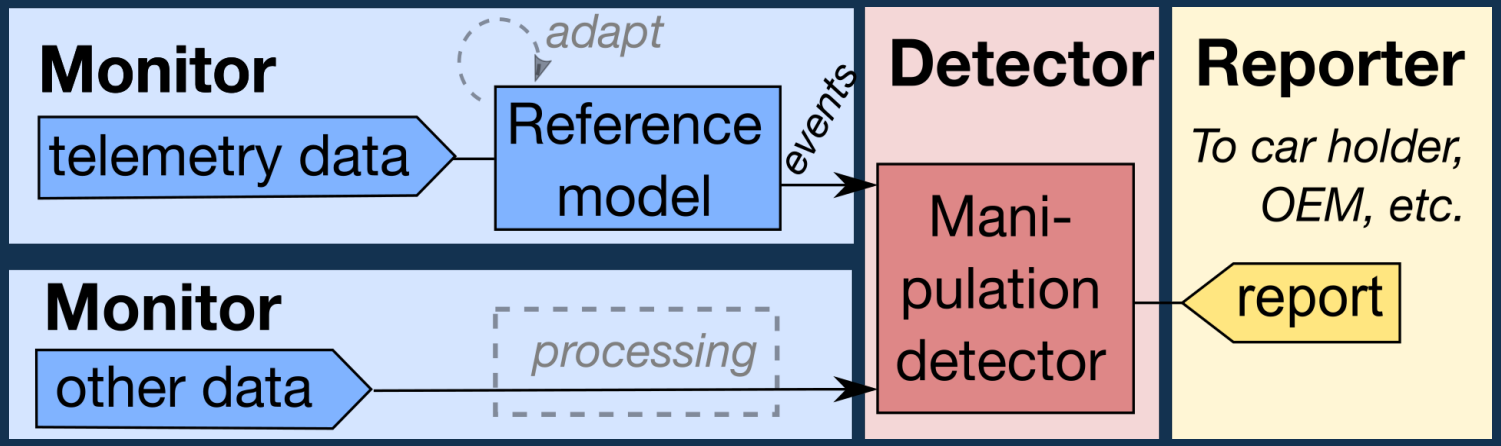
Bottleneck ANN:



- Hidden layer generalizes ***ratio*** between features
- Stores the typical behavior of an engine
- Trained using same vector for input X, output Y
- Anomaly score is error between input and output

Intrusion Detection Layer

Compares current to reference behavior

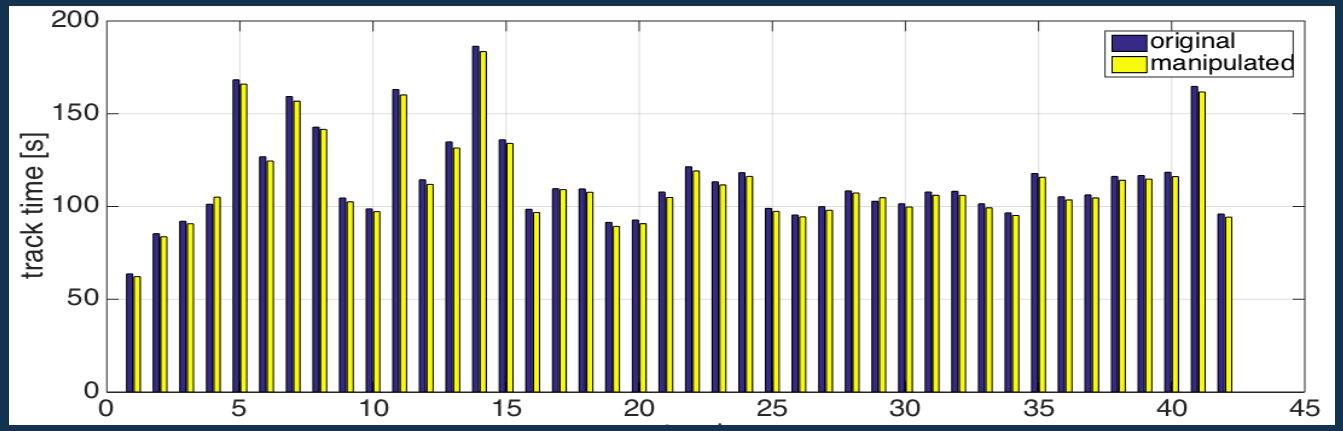


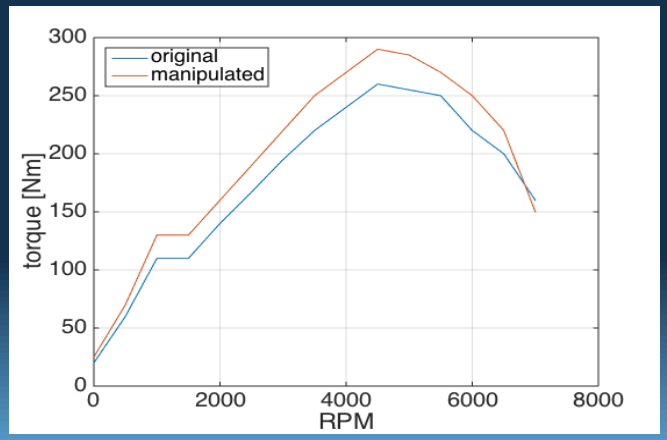
- Monitor converts data to potential manipulations
- Detector uses context and state info to reduce FP

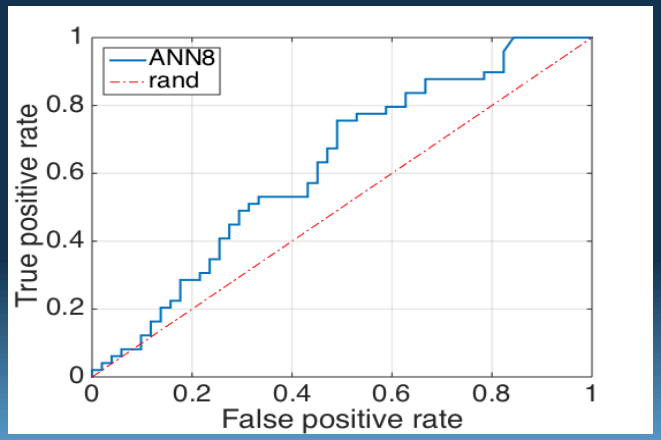
► **Deep Learning approach could extend to Detector**

Evaluation: Simulation

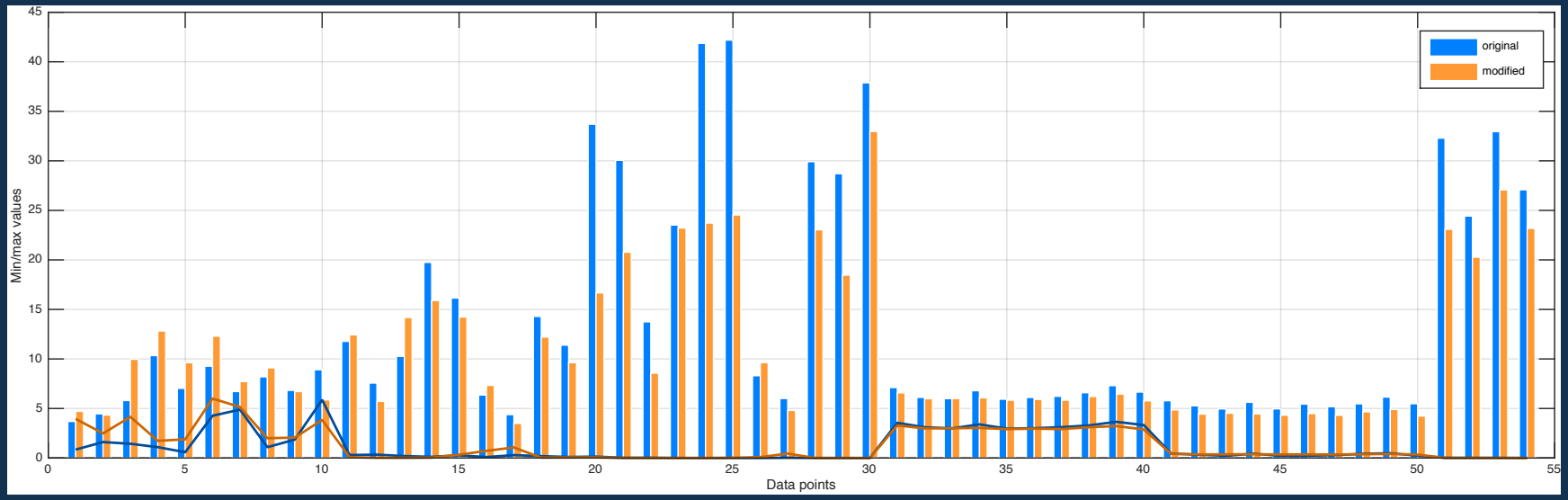
- Racing car simulation TORCS (Peugeot 406)







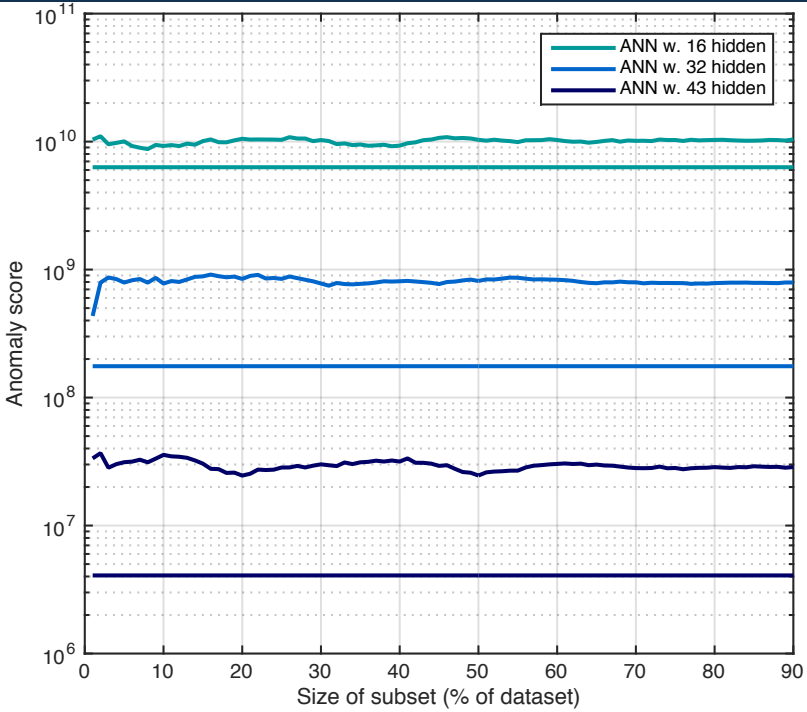
Evaluation: Car data

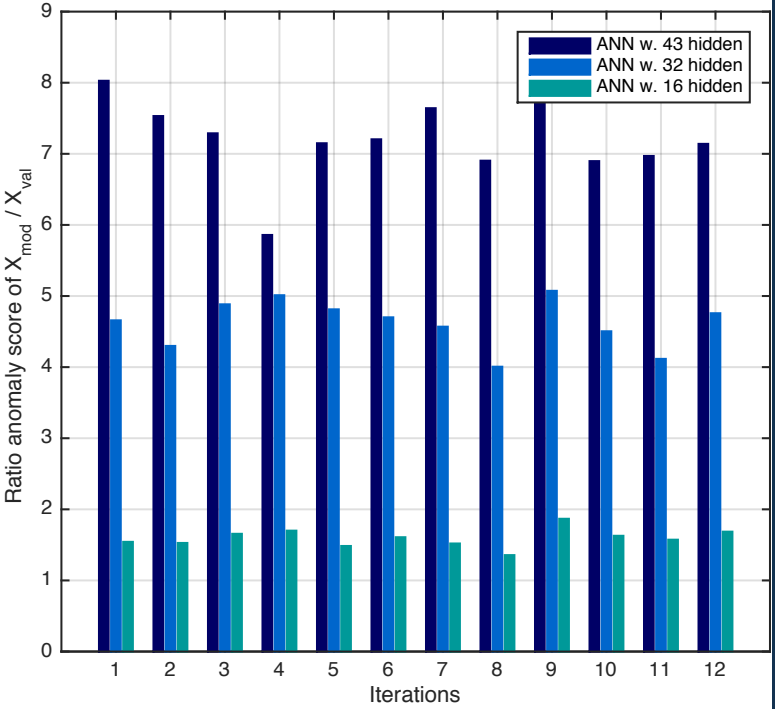


Vehicle speed
Engine RPM
Fuel rate
Fuel/Air commanded equivalence
Accelerator pedal position D

Calculated load value
Absolute throttle position
O2 sensor lambda wide range
Absolute throttle position B
Catalyst temperature

Recognition result





ANN with 43 hidden nodes has 6-8 times higher anomaly score than validation set. 16 ~ factor 1.5

Related Work

- CAN message statistics [Hoppe et al., 2007]
- Entropy-based IDS [Muter et al., 2011]
- Commercial IPS A: Deep Packet Inspection identifies abnormal behavior [2013]
- Commercial IPS B: Detection to prevent malicious communication intrusions [2012]
- Context-aware IDS [Wasicek and Weimerskirch, 2015]

Conclusion and Outlook

- Automotive systems are Cyber-Physical
- IDS need to target both sides of the coin
- Integrate with other security mechanisms
- Intelligently use the cloud to recognize attacks
- **Faults, ageing, and repair effects are challenging**

Thanks for your attention!

Contact me: arminw@berkeley.edu