Context-aware Automotive Intrusion Detection

Armin Wasicek[1]
Mert D.Pesé[2], André Weimerskirch[2],
Yelizaveta Burakova[2], Karan Singh[2]

[1]Technical University Vienna, Austria
[2]University of Michigan

ESCAR USA
June 21, 2017

Motivation for Security

Dominant motives of organizations for security:

- Avoiding and mitigating loss
- Avoiding negligence
- Enhancing strategic business values

► **Security is the enabler of business models**

Who is willing to pay for Security?

Incentives for investment in security are lacking

- Making a **strong business case** for security is hard:
  - Quantifying risk in a dynamic environment
  - Rapidly changing, unpredictable threats
  - Demonstrating consequences of attacks

► **Who is willing to pay for security?**

Vulnerability Black Market

Zero-day exploits are a tradable asset

- Full disclosure to improve software is utopia
- New professionalism in security market
- Cost of exploit: $ 1k-5k (2k), good >10 month
- “Realistically, we’re selling cyberweaponry”

► **There is already a market for security!**

Rising need for Security

Automotive security requirements

- Cost effective
- Reusable
- Adaptive
- Cyber-Physical nature

Security toolkit

★ ECU security

★ Secure On-board Comm.

★ Perimeter security

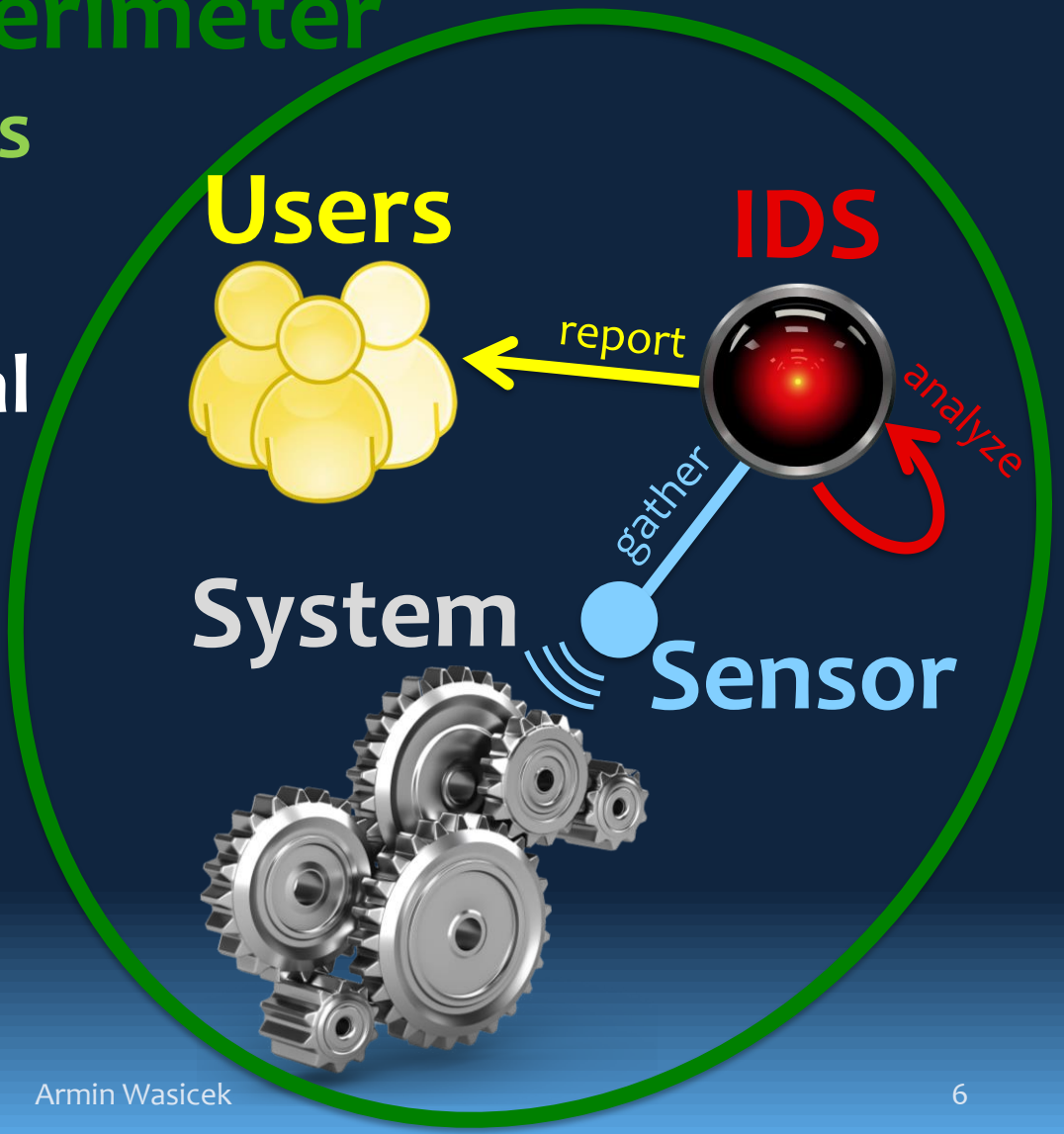
★ Intrusion detection

► Raise the bar to prevent (simple) attacks

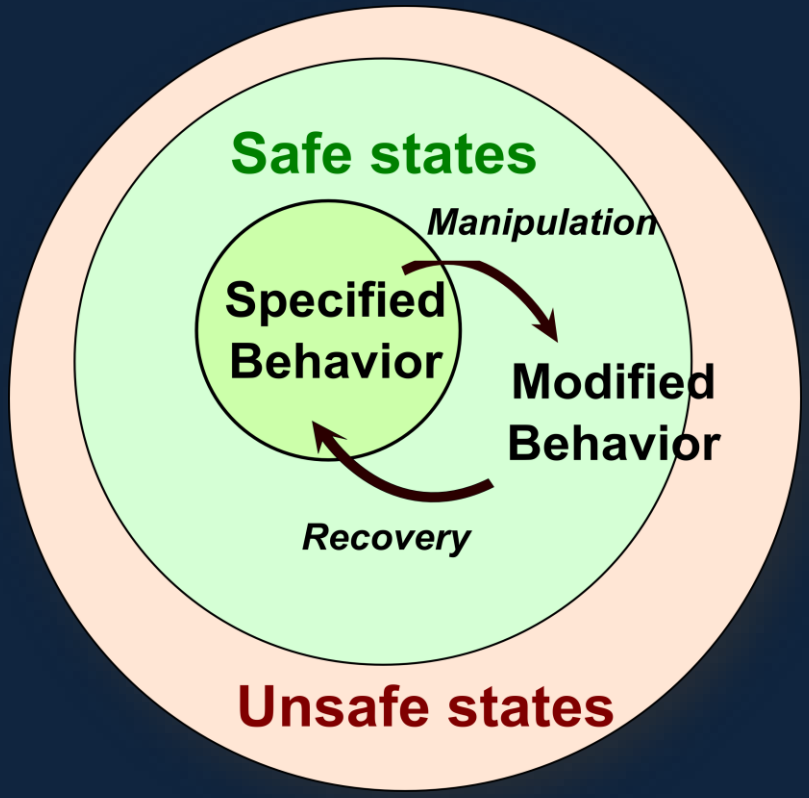
What is Intrusion Detection?

Gathers and analyzes information

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



Manipulation and Fault tolerance

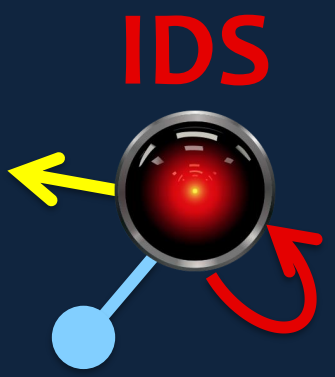


- Triggering unsafe states will stop the system
- **Manipulations are subtle**
- Stay within safe states, but modified behavior
- Recognition and Recovery

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

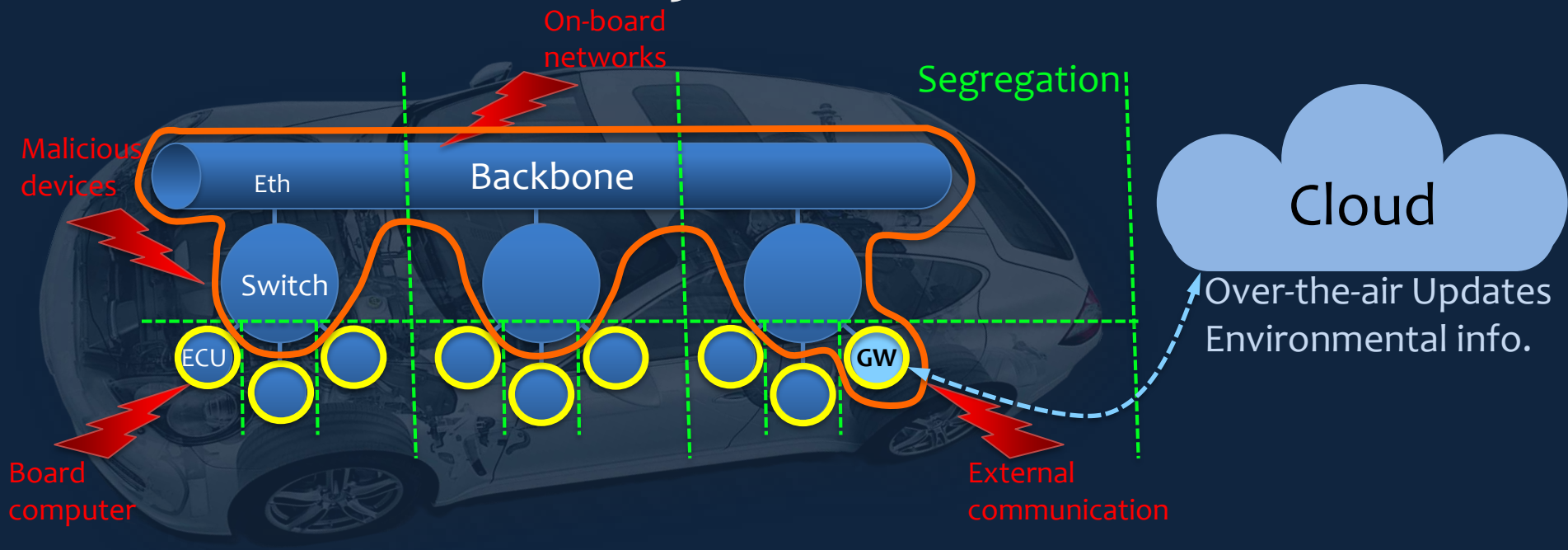
Development of the processes, algorithms, reporting requirements, and data requirements for ***both local and global detection functions***;

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!**

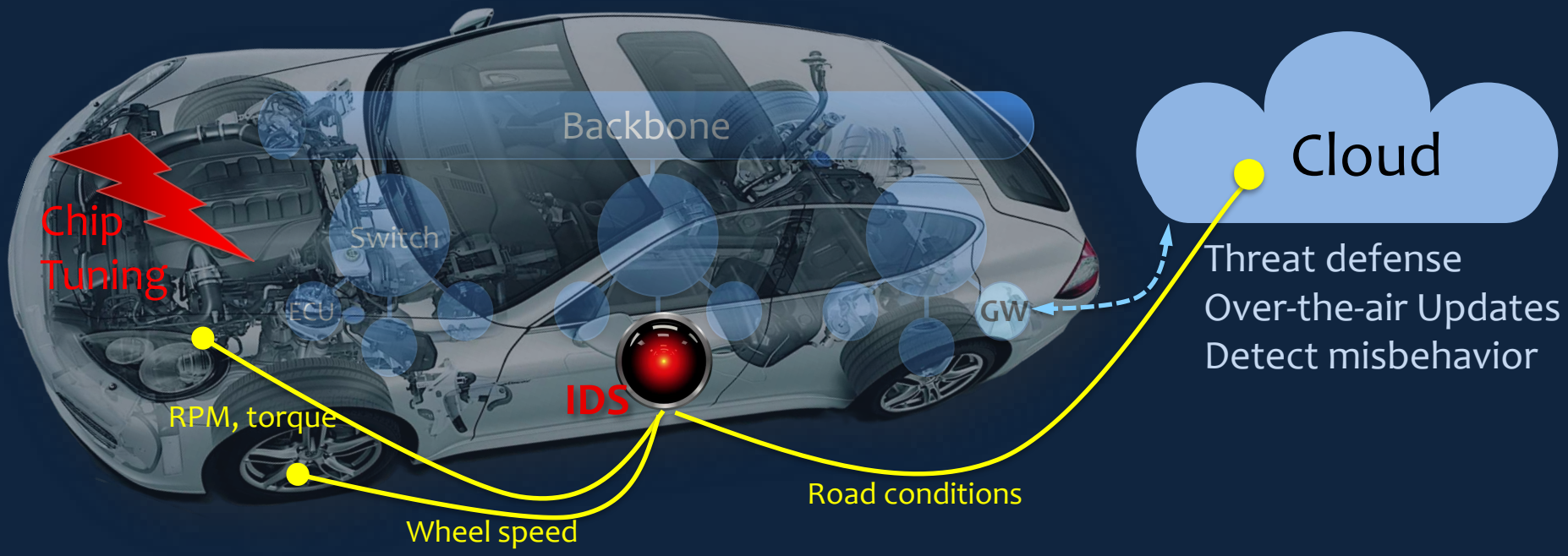
Cyber-Physical Attacks

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 Selection

Select parameters capturing engine behavior

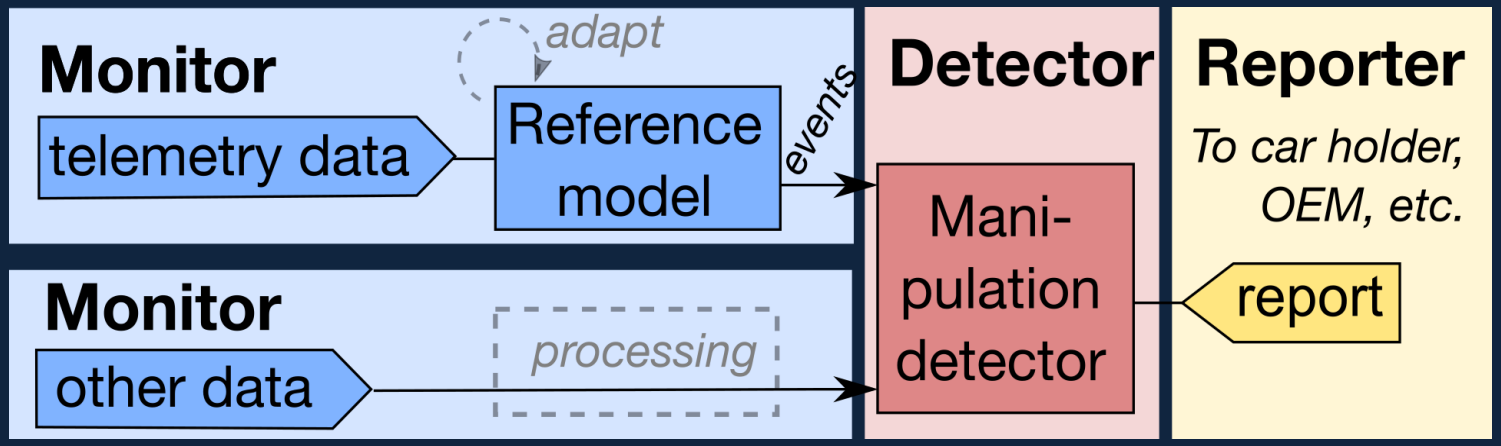
Engine control measures many useful parameters

- Speed … velocity of vehicle
- RPM … angular velocity of engine
- Torque … turning force

- We want to detect modifications, like going around the curve slightly faster, having more torque on a slope, etc.

Intrusion Detection Layer

Compares current to reference behavior



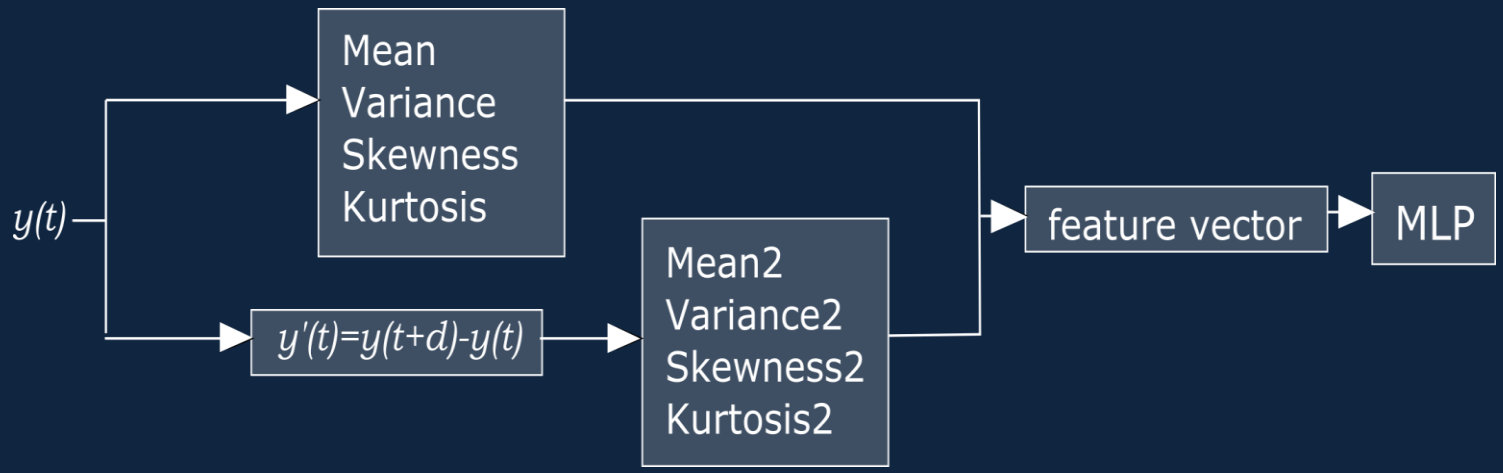
- Trained model reconstructs some features poorly
- These are considered as outliers

► **Manipulation, if num. of outliers exceeds threshold**

Feature Extraction

Convert a time series to a feature vector

Processing pipeline works on a time slice

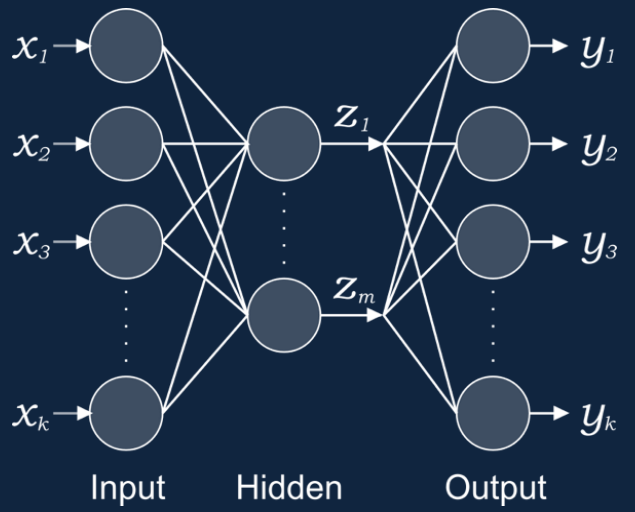


- Use original signal and its differentiation
- Use statistical moments to expand features
- Normalize feature vector

Artificial Neural Networks

Solve a one-class classification problem

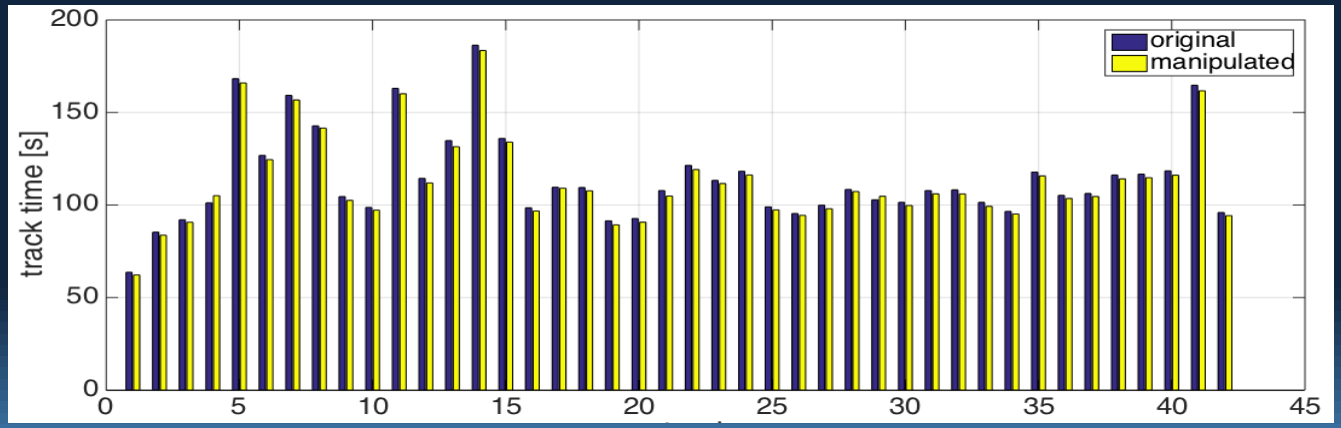
Autoencoder Neural Network:



- 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

Evaluation

- Racing car simulation TORCS
- Car model ‘p406’ simulating a Peugeot 406
- Increase engine torque by 10 Nm and 30 Nm
- Let the robot do the driving!



Engine tuning

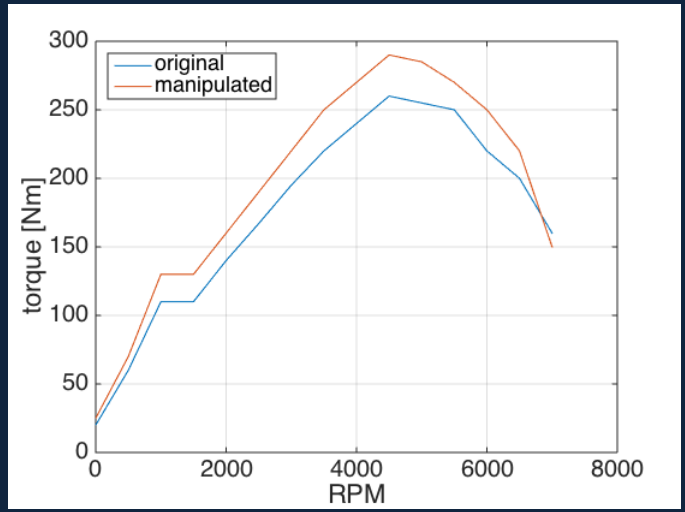
Modification

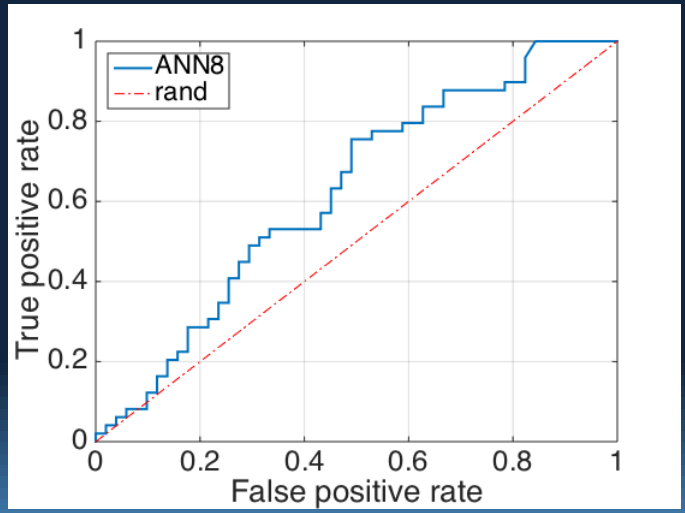
- Modify RPM/Torque ratio

Recognizing manipulation

- Bottleneck ANN
  - 8 hidden perceptron
- ROC curve looks promising

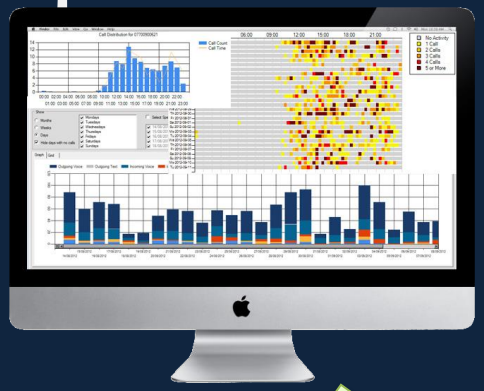
Note: This is unsupervised learning!





Experimental Setup

Perform analytics, detect presence

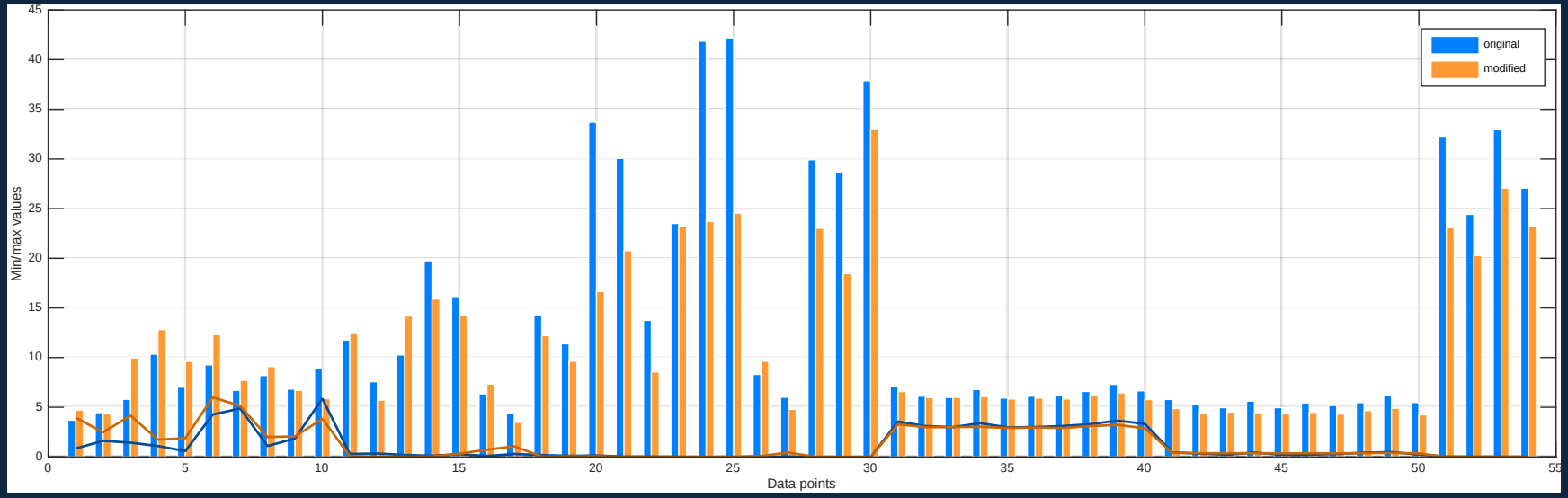


Power boxing to manipulate engine control

Read out data via OBD II

Urban/Highway driving cycles

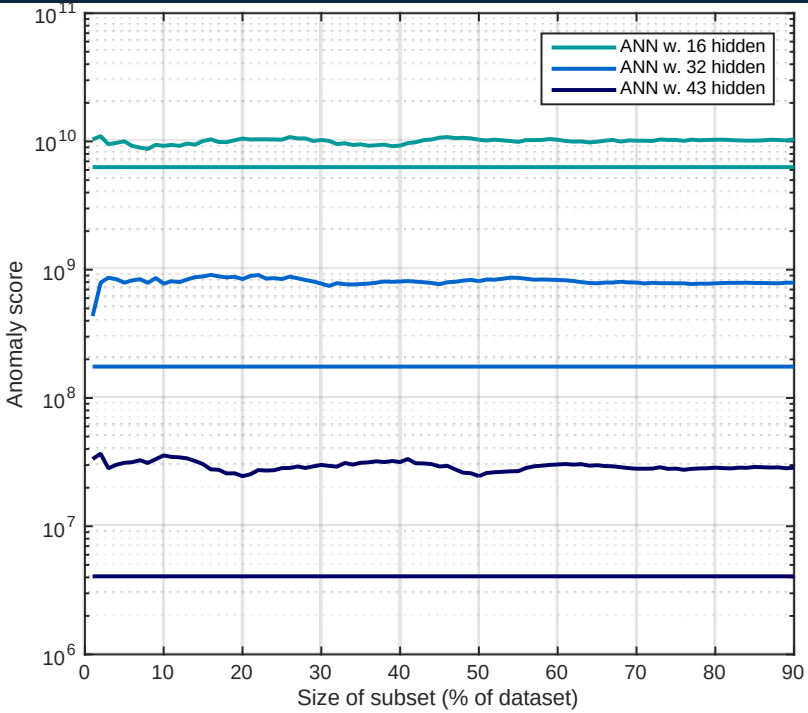
Real car data

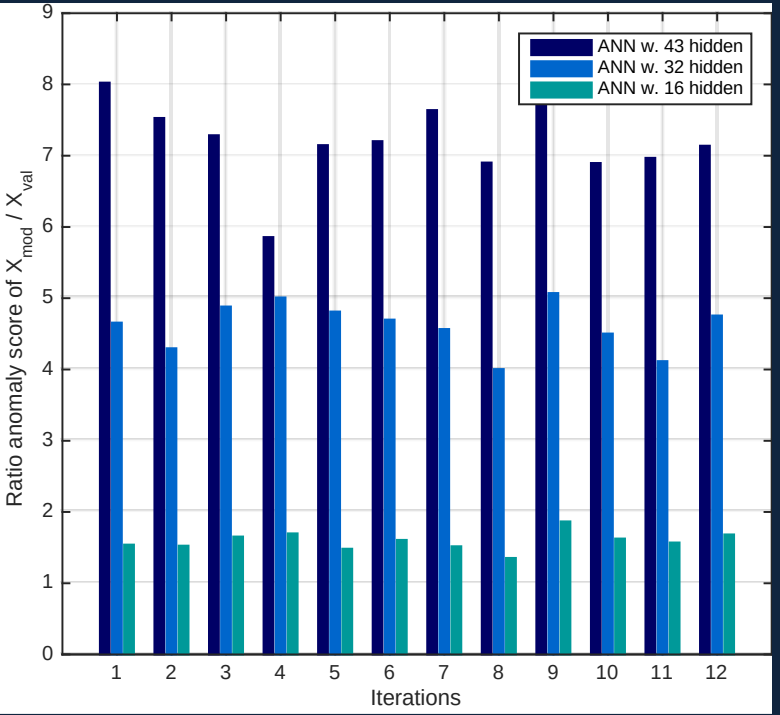


Vehicle speed
Engine RPM
Fuel rate
Fuel/Air commanded equivalence
Accelerator pedal position D

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

Recognition result

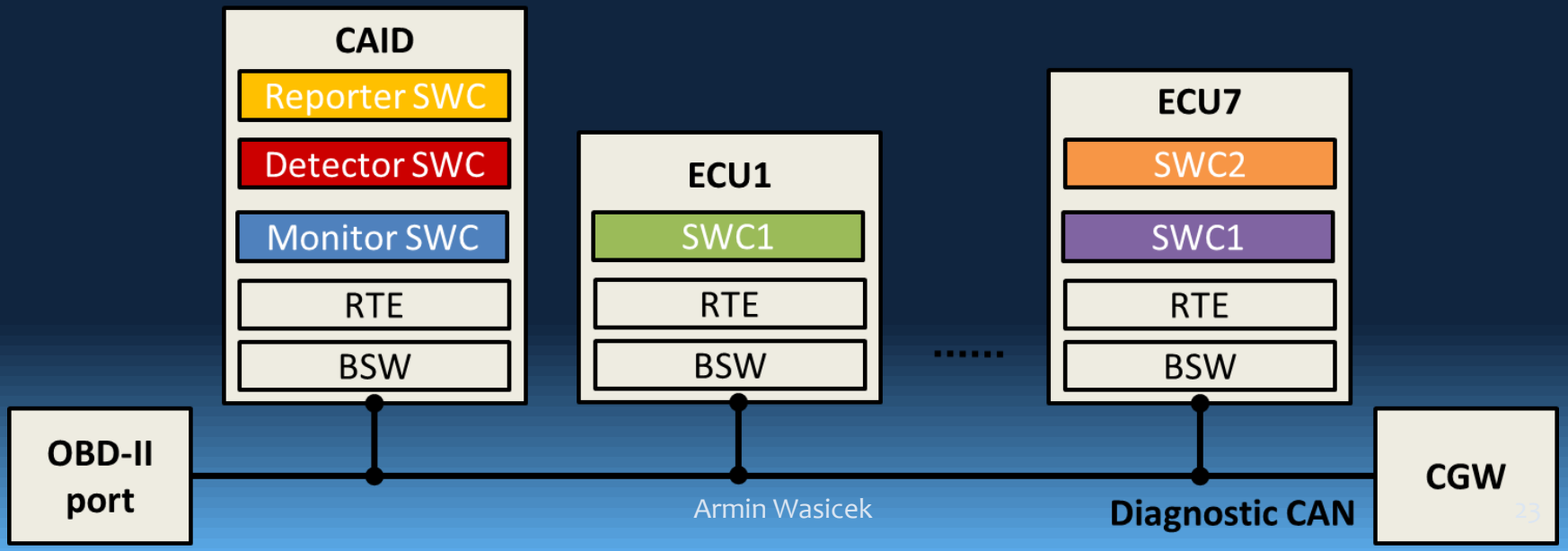




ANN with 43 hidden nodes has 6-8 times higher anomaly score than validation set. 16 ~ factor 1.5

Integration options

- Software Component (SWC) in AUTOSAR terminology
- Subscribe to relevant data via Virtual Function Bus (VFB)
- CAID integration options
  - **Standalone**: on the CAN bus connecting the Central Gateway (CGW) to the OBD port
  - **Integrated:** Part of the CGW



Related Work

- CAN message statistics [Hoppe et al., 2007]
- Entropy-based IDS [Muter et al., 2011]
- Commercial IDS/IPS: Deep Packet Inspection identifies abnormal behavior
- Context-aware IDS [Wasicek and Weimerskirch, 2015]

Conclusion and Outlook

- Automotive systems are Cyber-Physical
- IDS need to recognize cyber and physical attacks
- 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: armin.wasicek@gmail.com

Yelizaveta Burakova

Response and Recovery

What to do after an intrusion has been detected?

- Not yet clear
- Depends on location, current state of vehicle
  - Log threat
  - Disable/inhibit features
  - Service procedure

- **What are means to react on intrusions/misuse?**

Automotive IDS Architecture