AI Revolutionizing Automotive Cybersecurity

With a focus on Intrusion Detection Systems

Natasha Alkhatib

21.10.2024

Speaker Introduction

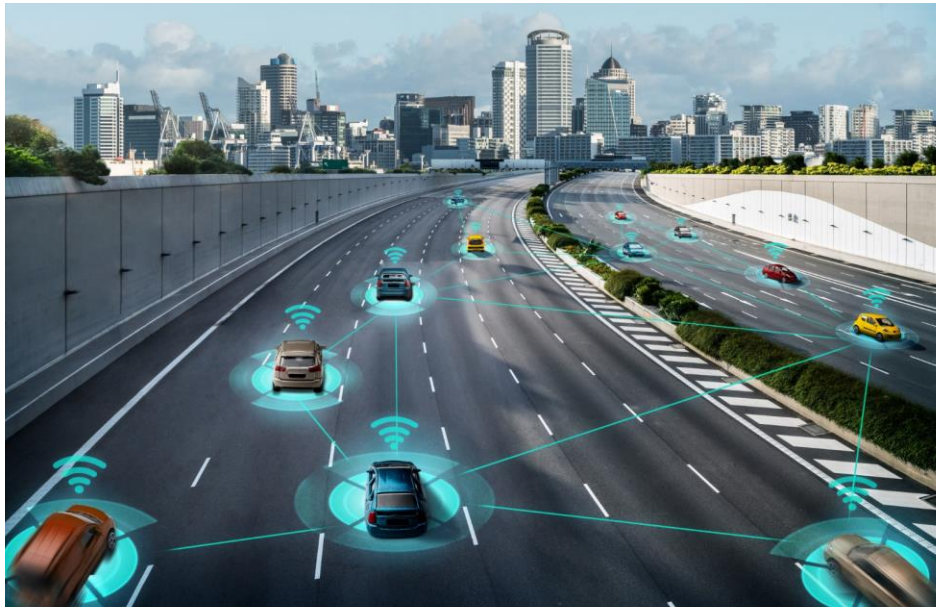
Natasha Alkhatib

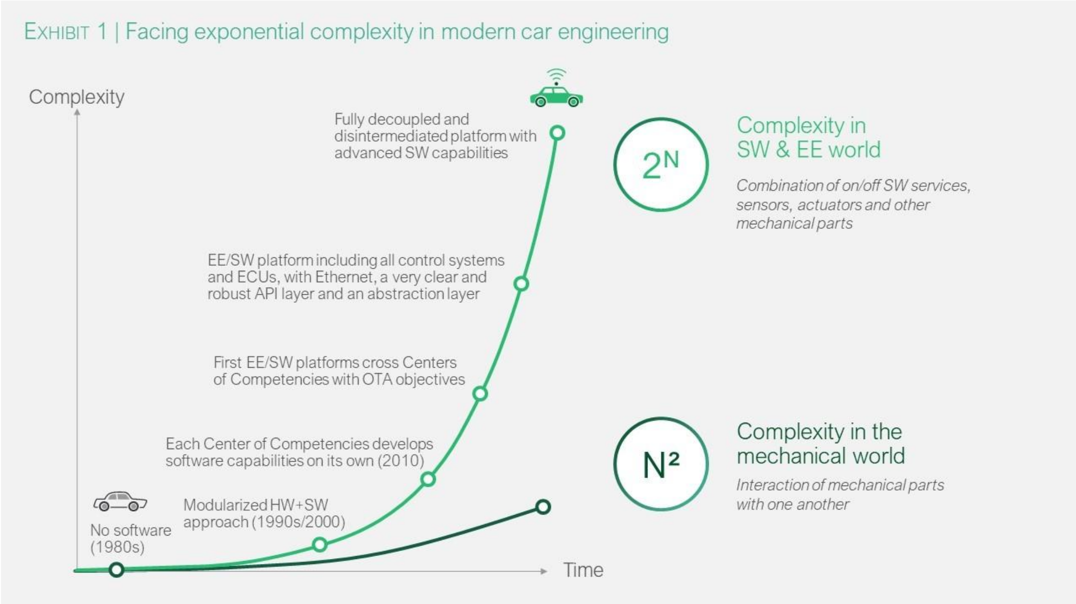
Cybersecurity Consultant at ETAS Bosch

- Holds a Ph.D. in AI for Automotive Cybersecurity from Institut Polytechnique.
- Specializes in AI-powered automotive cybersecurity solutions.
- Holds a PhD in the field and extensive experience in developing in-vehicle intrusion detection systems.
- Consults for clients, implementing security concepts, integrating ETAS products like IDSs, firewalls, and fuzzing systems.

Motivation

Double-edged sword: Automotive Connectivity & Complexity





Connectivity

~ 367M Globally by 2027

Complexity

~ 80M vehicles with high or full automation by 2030

Increased potential for safety-relevant attacks

Motivation
UNECE WP.29 requirements

1. The automotive sector is undergoing a profound transformation with the digitalization of in-car systems that are necessary to deliver vehicle automation, connectivity and shared mobility. This comes with significant cybersecurity risks.

2. The two UN regulations require that measures be implemented across 4 distinct disciplines to tackle these risks by establishing clear performance and audit requirements for car manufacturers:

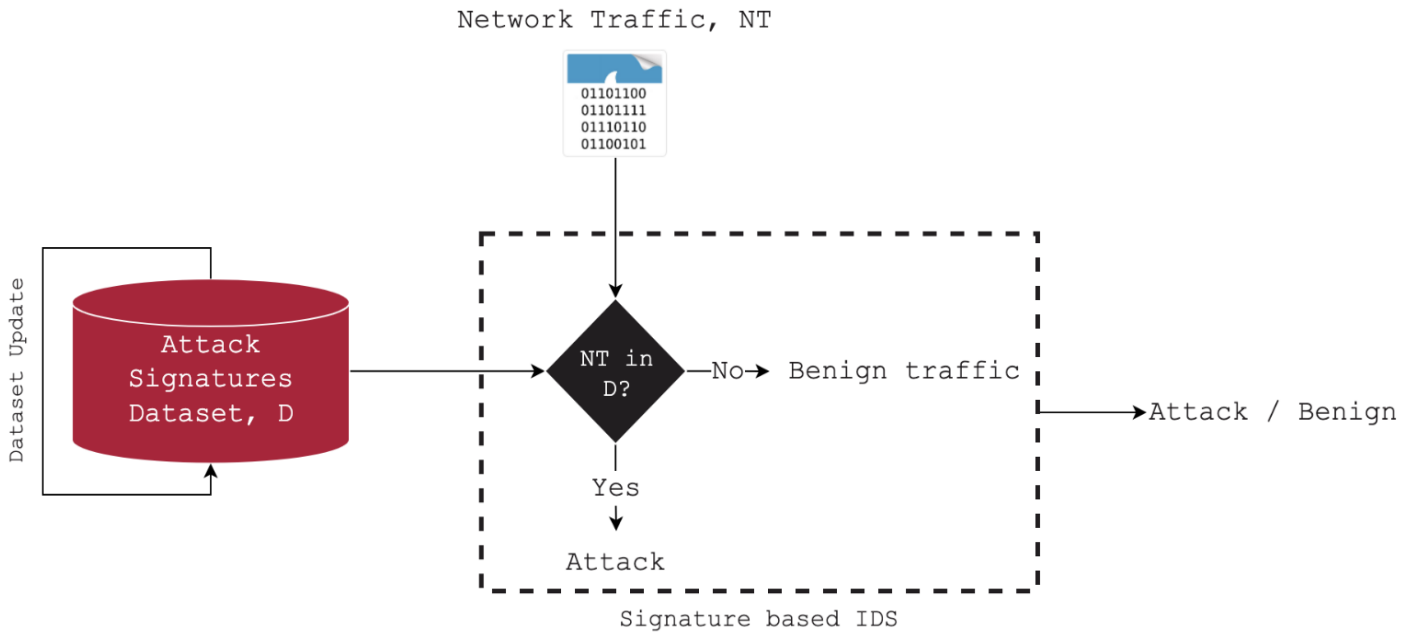
   - Managing vehicle cyber security
   - Securing vehicles by design to mitigate risks along the value chain
   - Detecting and responding to security incidents across vehicle fleet
   - Providing safe and secure software updates and ensuring vehicle safety is not compromised, introducing a legal basis for O.T.A updated to on-board vehicle software.

What is an Automotive IDS ?

- ISO/SAE 21434 standard mandates a defined incident response process.
- This process is bolstered by the automotive Intrusion Detection System (IDS), which functions as an in-vehicle sensor and connects to a backend system.
- The onboard IDS monitors the Electronic Control Units (ECUs) and communication networks for external attacks.
- Upon detection, it collects the data and transmits it to the manufacturer's Security Operations Center (SOC) for analysis.
- Based on the data collected by the automotive IDS, the OEM makes informed decisions on how to respond to these attempted attacks.

Automotive Intrusion Detection principles

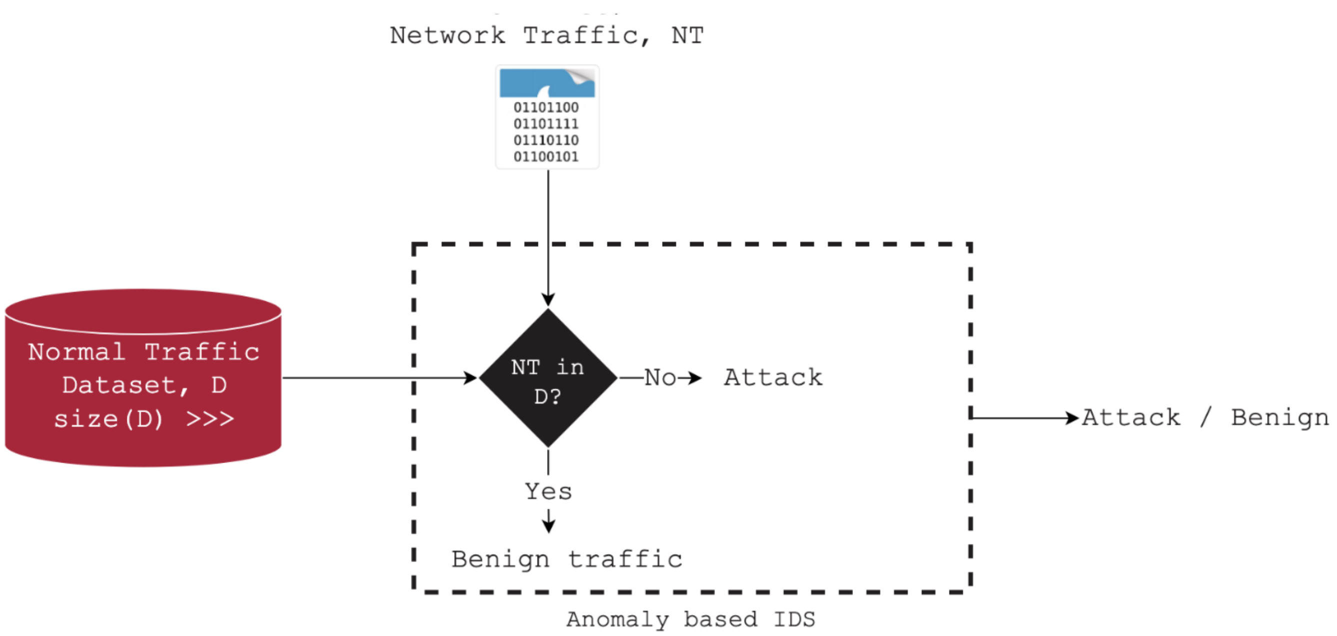
Signature-based technique



- ↘ False positive rate
- Identify previously **known** attacks
- Fail to identify **novel or previously unseen attacks**

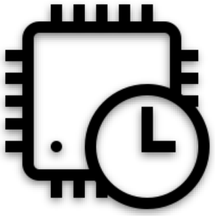
Automotive Intrusion Detection principles

<u>Anomaly-based technique</u>

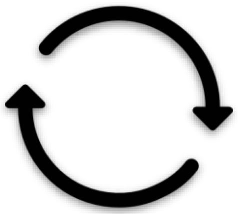


- Capable of identifying novel or previously unseen attacks

Challenges for automotive IDS



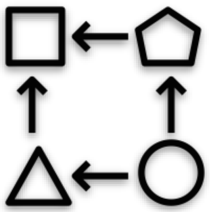
Real-time constraints



Continuous Monitoring

High Detection Rate

Low False-Alarm Rate



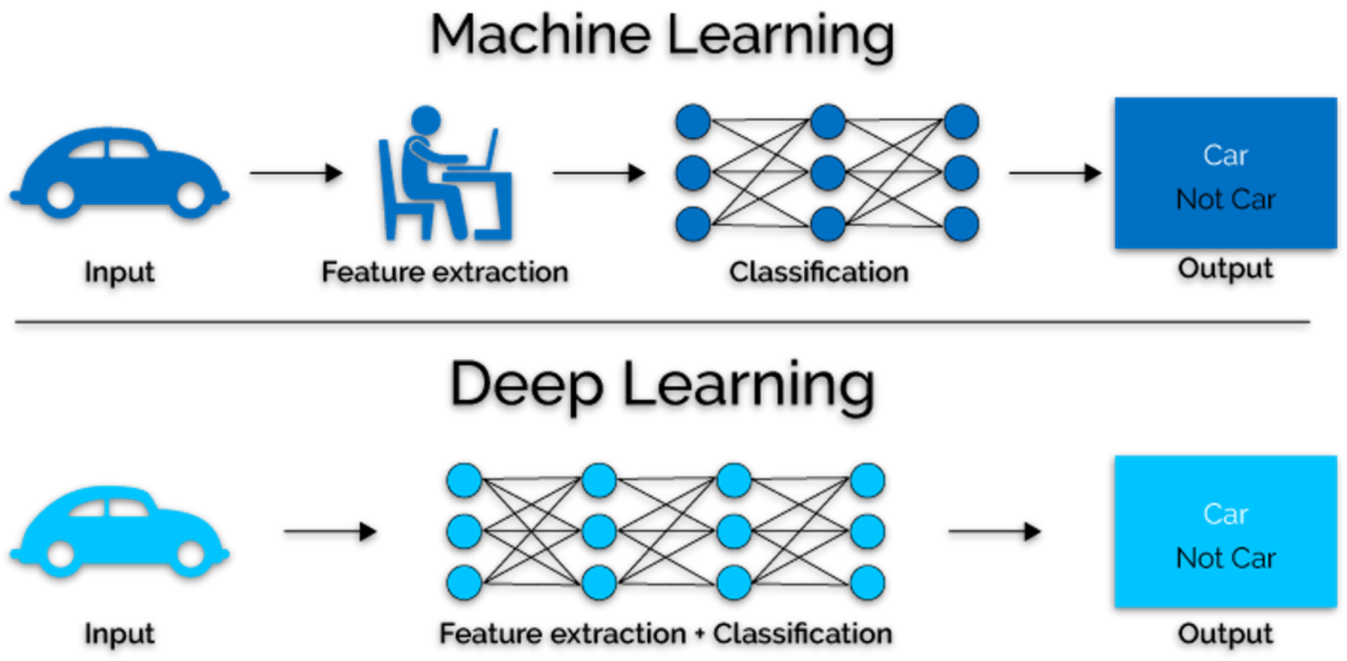
Robustness

The game changer in automotive Intrusion Detection

Deep learning techniques for Intrusion Detection

Deep learning (DL) is a machine learning subfield that uses multiple layers for learning data from representations

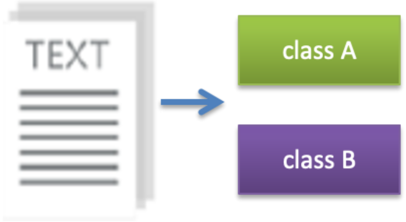
- DL is exceptionally effective at learning patterns



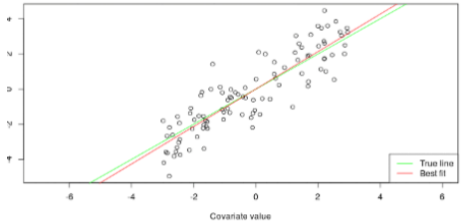
Picture from: https://www.xenonstack.com/blog/static/public/uploads/media/machine-learning-vs-deep-learning.png

Deep learning techniques for Intrusion Detection - learning types

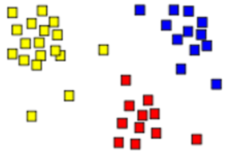
1. **Supervised:** learning with labeled data
   – Signature-based IDS
   – Example: regression for predicting real-valued outputs
   – Example email classification, image classification
2. **Unsupervised:** discover patterns in unlabeled data
   – Example: cluster similar data points
   – Example: Anomaly-based IDS
3. **Semi-supervised/self-supervised:** learn data representations with labeled data
   – Example: anomaly-based IDS

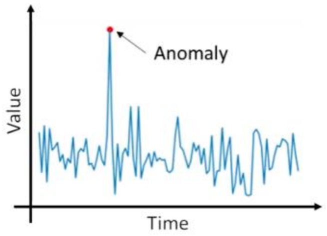


Classification



Regression

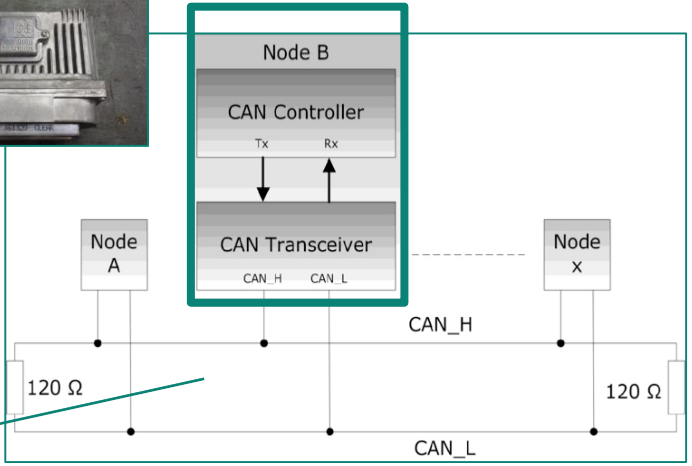

Clustering



Intrusion Detection for Controller Area Network (CAN)

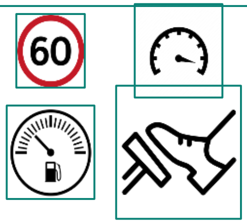
The Controller area network
Protocol definition

– Message-based protocol standard
– Broadcast data frames (current state of the vehicle)



↘ ID ↗ Priority

0.05s	ID 0X102
0.01s	ID 0X45D



The Controller area network
Vulnerabilities

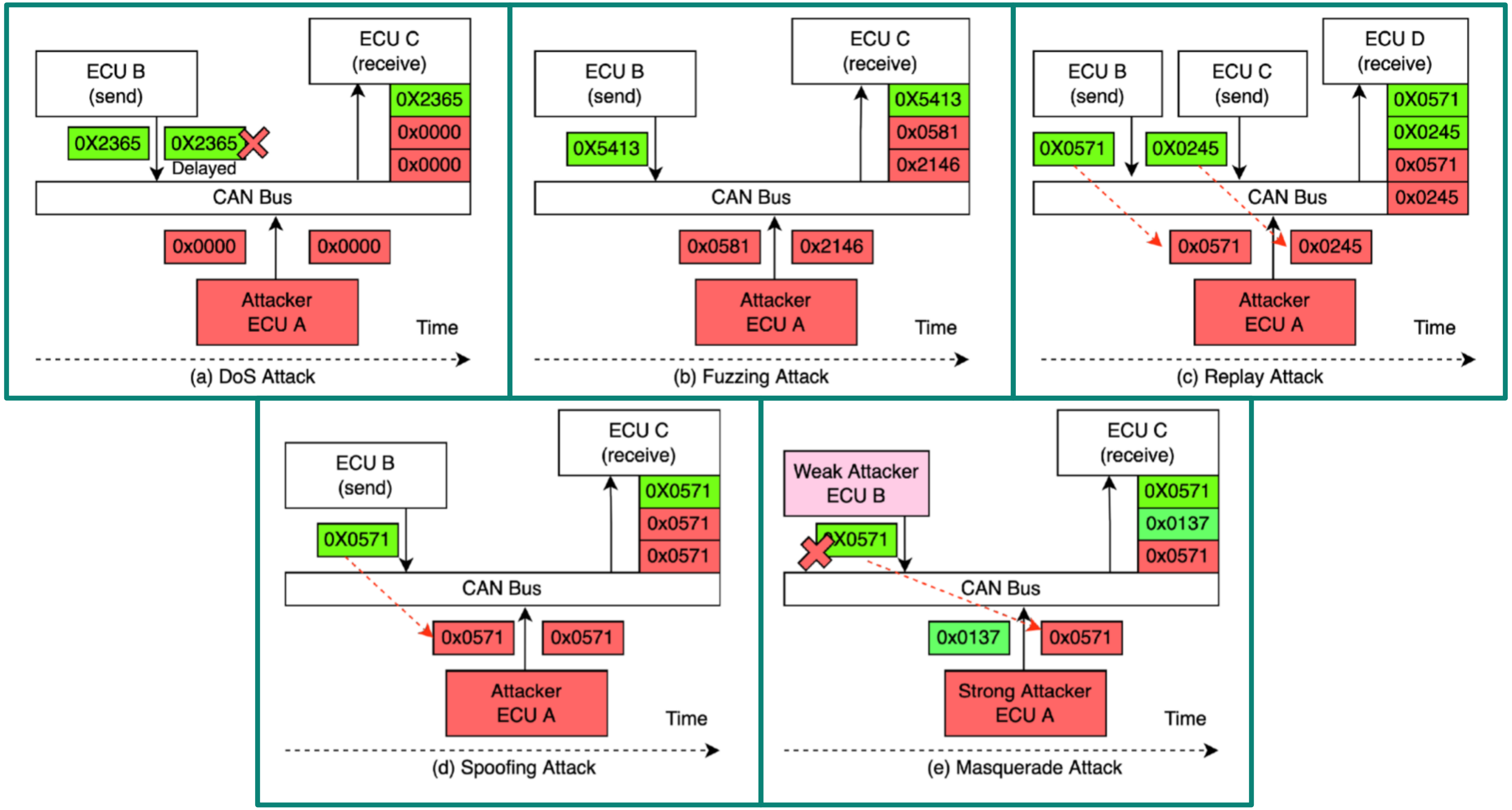
No authentication

Broadcast domain

No encryption

ID-based priority

The Controller area network
Attacks

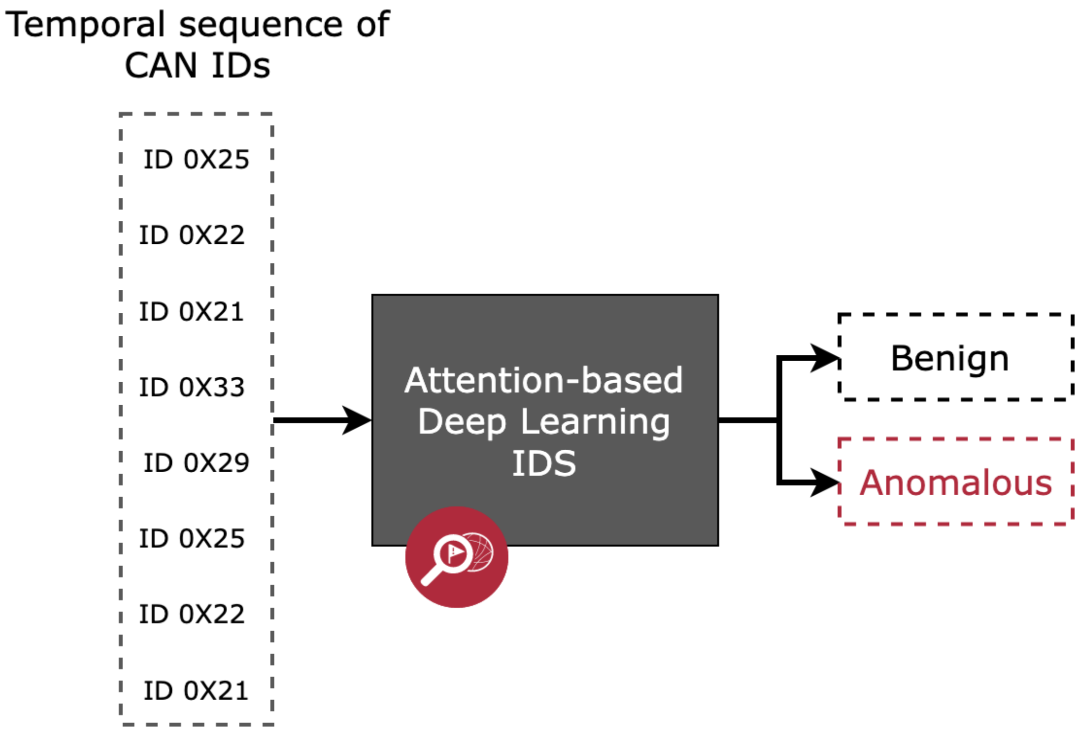


Research question

Can we exploit the structure of **Attention networks** for intrusion detection on CAN?

Motivations

- Model ***sequential*** CAN data
- Make each ID in the sequence **encode** the context information from both ***left*** and ***right***
- ***Objective function*** for capturing normal sequence behavior:
  - Prediction of next ID message isn't enough
  - ***Self-supervised learning for whole sequence contextual encoding***



Methodology

How to exploit the structure of **Attention networks** for intrusion detection on CAN?

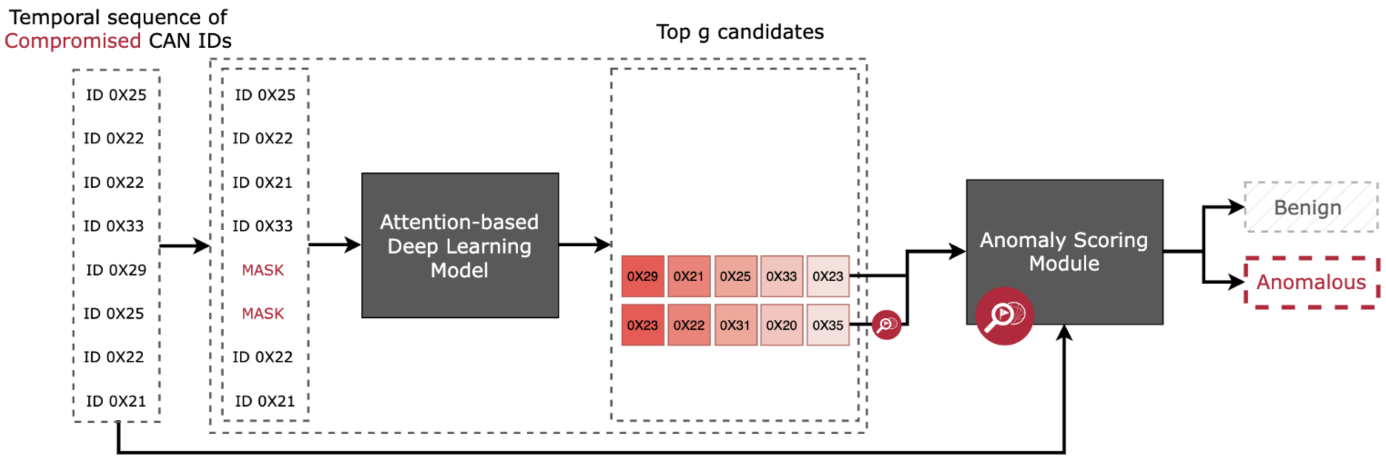
- Model trained on normal data → ↗ **accuracy on predicting masked CAN IDs for normal test sample.**

- Randomly **replace** a ratio of CAN IDs in a sequence with a specific **MASK** token

- Predict the **masked CAN IDs** in CAN sequence

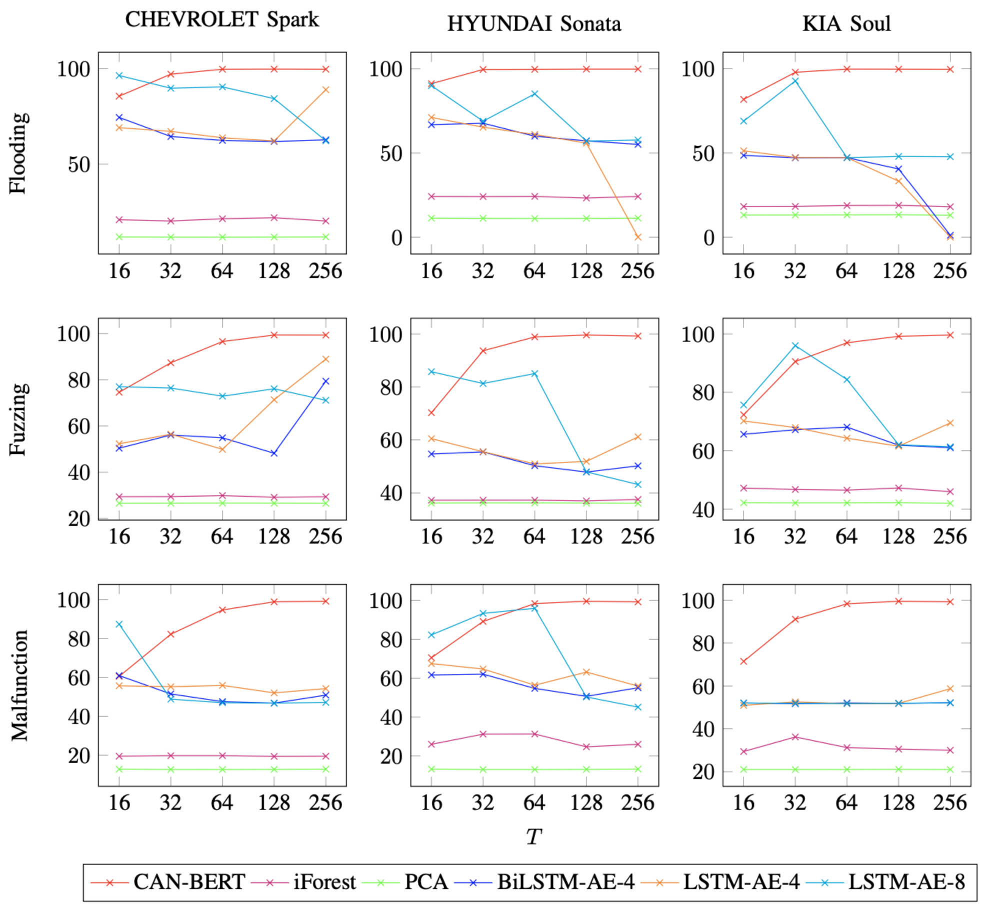
- **Anomalous CAN ID**
  → observed CAN ID is **not in the top-g candidate** set predicted by attention-based model

- **Anomalous CAN ID sequence**
  → > ***r*** anomalous CAN IDs



Anomaly detection stage

Comparison of the attention-based model with other baselines



- Sequence length variation: {16,32,64,128,256}
- **Target:** Identify a message injection attack as soon as possible
- **Takeaways:**
  - **ML algorithms** perform poorly and maintain the same F1- score metric w.r.t sequence length.
  - **DL based models** outperformed the traditional anomaly detection models w.r.t sequence length.
  - **Attention-based** obtains respectable F1 scores ∈ [0.85, 0.99]
    - BERT-based models are better at capturing the patterns of CAN ID sequences

AI as a force multiplier in automotive cybersecurity

Other use cases

- AI technologies for:
  - automotive threat intelligence in the VSOC
  - fuzzing and penetration testing
  - investigation
  - research
  - report

Conclusion

- Toward explainability and interpretability of deep learning-based IDS
- Quantization of deep learning-based IDS

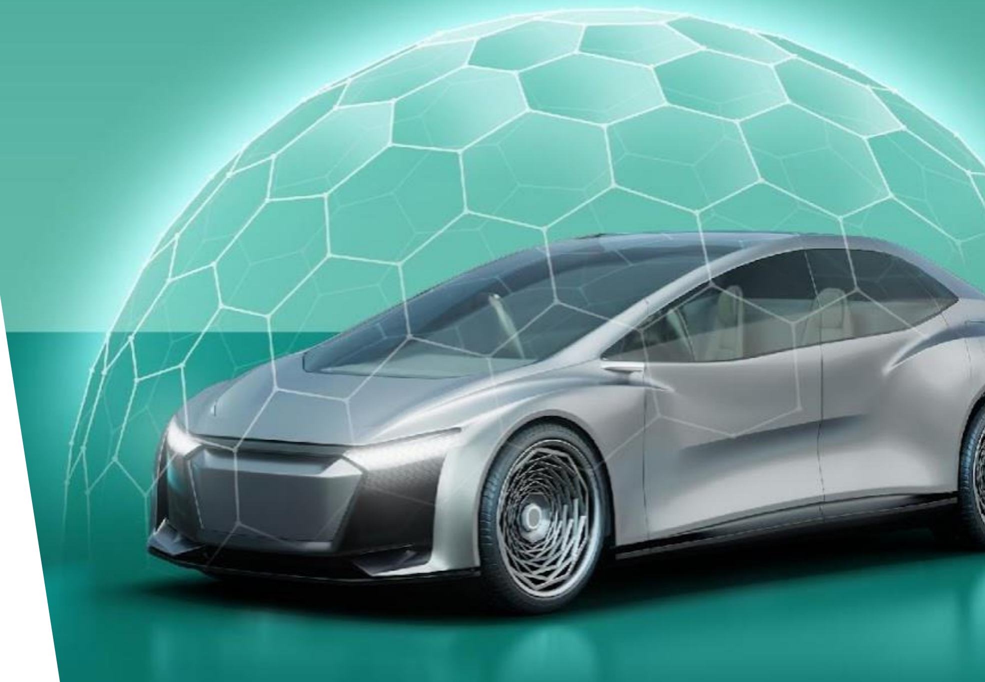
- End-to-end framework for overall intrusion detection

Key Takeaways

- *AI as a force multiplier for automotive cybersecurity*
- *Revolutionization in the automotive Intrusion Detection Field*
- *Benefits: Improved detection rates, faster response times, proactive defense*
- *Considerations: Data security & privacy, explainability of AI models*

ETAS Infineon

Join the next cybersecurity webinar to get more expert insights!



Upcoming Webinar: Securing the automotive industry in the quantum computing era

Date & Time: 23. October 2024, 9am (EST)

Infineon