universität uulm

Institut für Verteilte Systeme
Institute of Distributed Systems

SecForCARs
security for connected automated cars

The Tenth International Conference on Advances in Vehicular Systems, Technologies and Applications
VEHICULAR 2021
July 18, 2021 to July 22, 2021 - Nice, France

IARIA

Security for Connected, Automated Vehicles: Securing Cooperative Adaptive Cruise Control

Frank Kargl, Ulm University, Institute of Distributed Systems
frank.kargl@uni-ulm.de
IARIA VEHICULAR 2021 | 2021-07-19

Presented by: Prof. Dr. Frank Kargl

Frank Kargl is a professor for Distributed Systems at Ulm University. Earlier, he held a tenured position as associate professor and full professor at University of Twente. For over 15 years, security and privacy of automotive systems are among his main research interests and he contributed substantially to research and standardization of Car-2-X communication as evidenced by over 100 publications in the field. For some years now, his focus extends towards the question how a combination of communication and automated driving in vehicles creates new challenges for their security. He is scientific lead of the German project SecForCARs, where a consortium of 14 partners from industry and academia addresses a broad range of related topics.

universität ulm

Institut für Verteilte Systeme
Institute of Distributed Systems

SecForCARs
security for connected automated cars

Abstract

In his talk, Frank Karg introduces the broad set of challenges for securing automated, connected driving and illustrates how the SecForCARs project is addressing them. He focusses on the use-case of Cooperative Adaptive Cruise Control and presents recent research that shows how CACC can effectively be attacked to even cause severe accidents, how misbehavior detection can help to identify such attacks, and what reaction strategies are available to then mitigate attack effects.

universität ulm

Institut für Verteilte Systeme
Institute of Distributed Systems

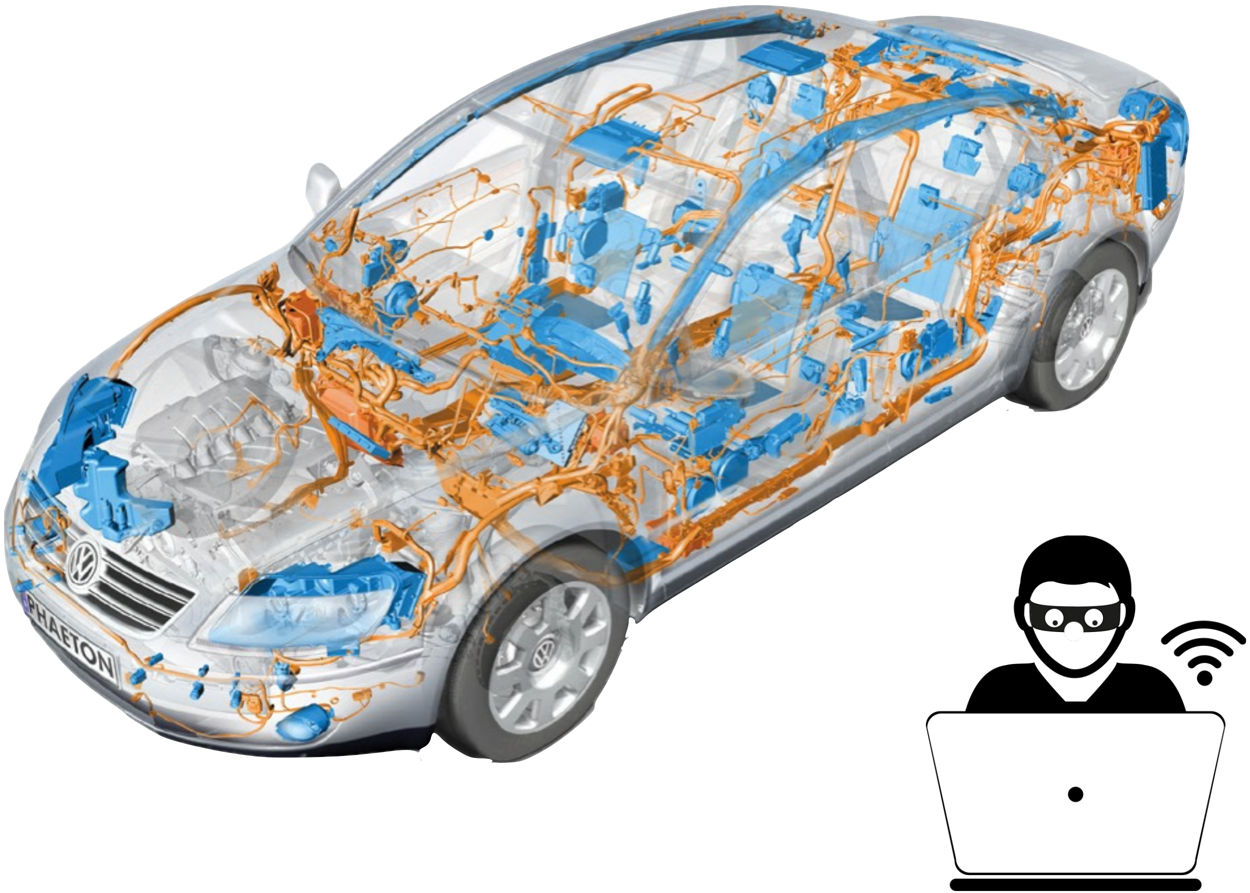
SecForCARs
security for connected automated cars

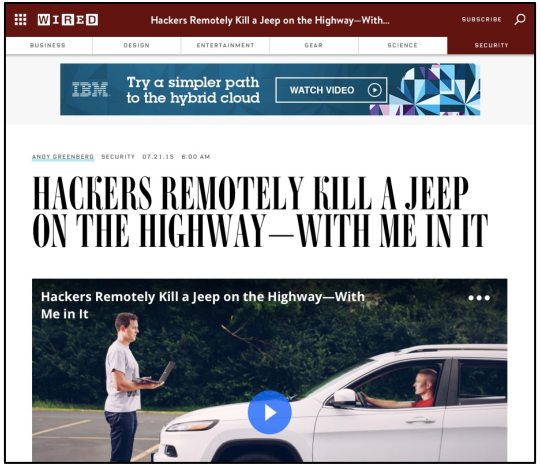
Security for Connected, Automated Vehicles:

Securing Cooperative Adaptive Cruise Control

Frank Kargl, Ulm University, Institute of Distributed Systems

IARIA VEHICULAR 2021 | 2021-07-19


PHAETON



Images:
Checkoway e.a., Comprehensive Experimental Analyses of Automotive Attack Surfaces, USENIX Security 2011
Koscher e.a., Experimental Security Analysis of a Modern Automobile, IEEE SSP 2010
ADAC, BMW Commbox

SEVECOM

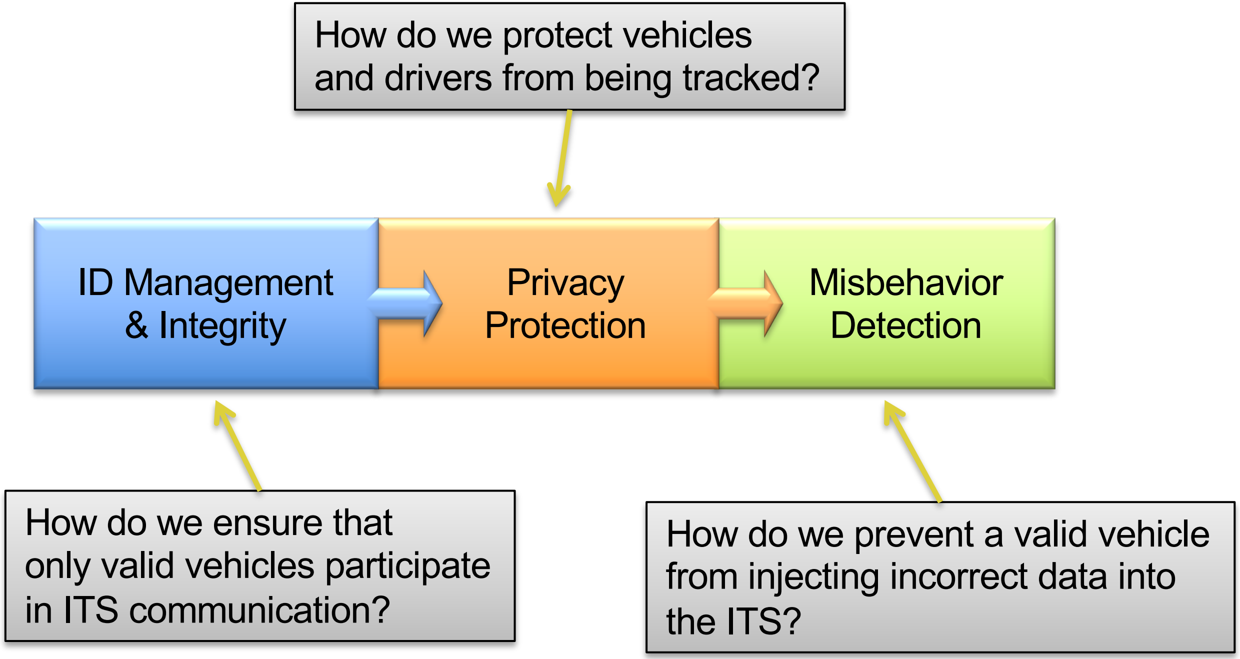
PRECIOSA

CONVERGE

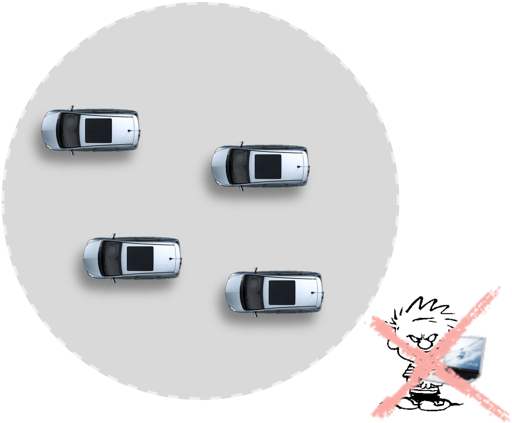
PRESERVE
preparing secure v2x communication systems

SecForCARs
security for connected automated cars

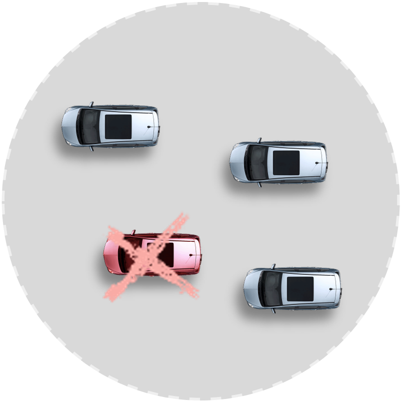
Central Elements of ITS Security



Pseudonym Schemes in Vehicular Networks: A Survey, IEEE Comm S&T, 17(1), 2015
Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems, IEEE Comm S&T, 21(1), 2019



External
Attacker



Insider
Attacker

Misbehavior Detection

IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 21, NO. 1, FIRST QUARTER 2019 779

Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems

Rens Wouter van der Heijden, Stefan Dietzel, Tim Leinmüller, and Frank Kargl, *Member, IEEE*

***Abstract*—Cooperative intelligent transportation systems (cITS) are a promising technology to enhance driving safety and efficiency. Vehicles communicate wirelessly with other vehicles and infrastructure, thereby creating a highly dynamic and heterogeneously managed ad-hoc network. It is these network properties that make it a challenging task to protect integrity of the data and guarantee its correctness. A major component is the problem that traditional security mechanisms like public key infrastructure (PKI)-based asymmetric cryptography only exclude outsider attackers that do not possess key material. However, because attackers can be insiders within the network (i.e., possess valid key material), this approach cannot detect all possible attacks. In this survey, we present misbehavior detection mechanisms that can detect such insider attacks based on attacker behavior and information analysis. In contrast to well-known intrusion detection for classical IT systems, these misbehavior detection mechanisms analyze information semantics to detect attacks, which aligns better with highly application-tailored communication protocols foreseen for cITS. In our survey, we provide an extensive introduction to the cITS ecosystem and discuss shortcomings of PKI-based security. We derive and discuss a classification for misbehavior detection mechanisms, provide an in-depth overview of seminal papers on the topic, and highlight open issues and possible future research trends.**

***Index Terms*—Vehicular ad hoc networks, intelligent vehicles, intrusion detection.**

I. Introduction

THROUGHOUT the field of computer science, securing systems against malicious attackers has become a fundamental requirement for safe, secure, and dependable operation of applications. Today, professional attacks against systems, which are mounted by large criminal organizations or even governments, are becoming increasingly common [1], [2]. At the same time, computer systems are increasingly intertwined with the real world, making them more appealing targets. The term cyber-physical systems (CPS) has been coined to encompass systems that are characterized by a large deployment of networked devices equipped with both sensors and actuators [3]. They are distinguished from traditional embedded systems, where individual nodes interact with the real world in strongly constrained environments. In contrast, CPS are highly networked, deployed in large regions, and may contain nodes with heterogeneous computational power. The content transferred in these networks is highly predictable, relating directly to real-world phenomena [3], [4], a fact that enables novel techniques to detect attacks, collectively referred to as *misbehavior detection*. A prominent example of such a system is a cooperative intelligent transportation systems (cITS), which consists of vehicles, road-side units and back-end systems, and which is the main focus of this survey. Attack detection in general is an essential second layer of security for networks, especially for widely deployed networked systems in potentially hostile environments, where attackers may have physical access to a subset of the system. Furthermore, the impact of such attacks is much greater, as they can easily be tailored to cause real-world harm or loss of life. Therefore, misbehavior detection in both CPS and cITS is essential for the secure and thus safe operation of these systems.

Cooperative Intelligent Transport Systems are networks designed to provide a variety of benefits [5], [6]. These include improved road-safety, greener driving through improved traffic management, support for partially autonomous vehicles, and infotainment services such as traffic information services. The characterizing communication paradigm of all these applications is that sensors are used to measure real world conditions, which are then communicated over a ubiquitous network. This network is built up by equipping each vehicle with a wireless interface, creating a dynamic ad-hoc network that can be accessed without further overhead, which is commonly referred to as a *vehicular ad-hoc network (VANET)*. The VANET can also include infrastructure components, referred to as road side unit (RSU), which are sparsely positioned along the road. The resulting network that includes sparse infrastructure is referred to as a *vehicular network*. Vehicles use the VANET to send and receive information, building a *world model* from received messages, which is used for the applications mentioned above. However, vehicles can also sense local information through a variety of sensors, especially with recent developments in partially autonomous driving. This information, communicated through vehicle-internal networks, is used for autonomous decision making by the vehicle, either in dedicated driving scenarios or with complete autonomy. These

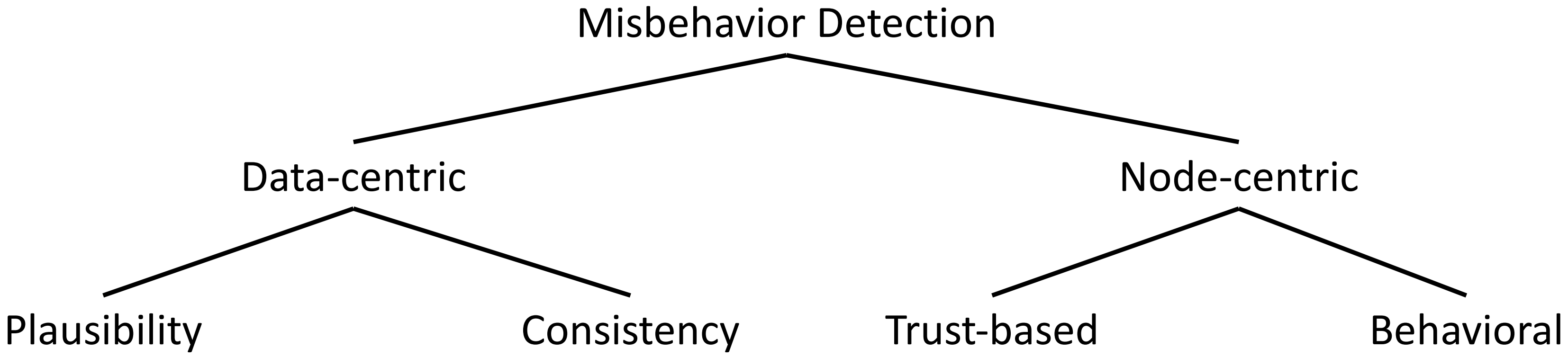
Manuscript received December 7, 2017; revised June 8, 2018 and August 2, 2018; accepted September 1, 2018. Date of publication October 1, 2018; date of current version February 22, 2019. This work was supported by the Baden-Württemberg Stiftung gGmbH Stuttgart as part of the Project IKT-05 AutoDetect of its IT Security Research Programme. *(Corresponding author: Rens W. van der Heijden.)*

R. W. van der Heijden and F. Kargl are with the Institute of Distributed Systems, Ulm University, 89073 Ulm, Germany (e-mail: rens.vanderheijden@uni-ulm.de).

S. Dietzel is with the Department of Computer Science, Humboldt-Universität Berlin, 10099 Berlin, Germany.

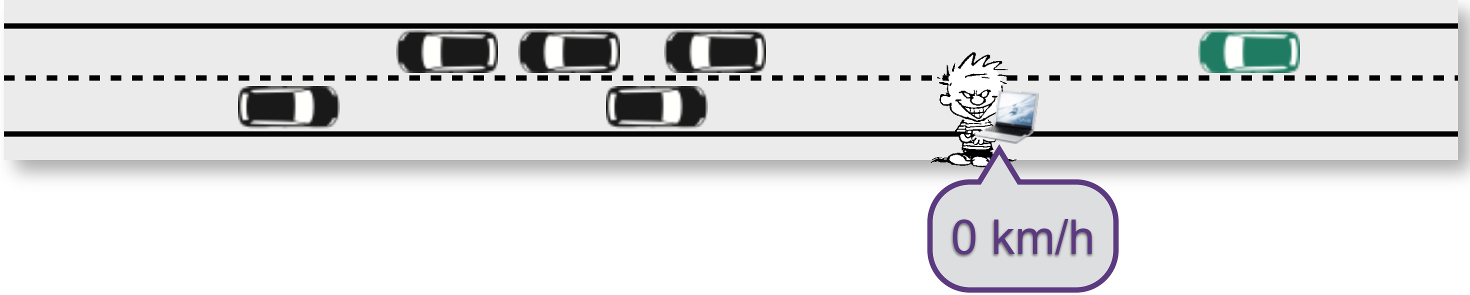
T. Leinmüller is with the InfoSafety Engineering, DENSO Automotive Deutschland GmbH, 85386 Eching, Germany.

Digital Object Identifier 10.1109/COMST.2018.2873088


Misbehavior Detection
Data-centric
Node-centric
Plausibility
Consistency
Trust-based
Behavioral

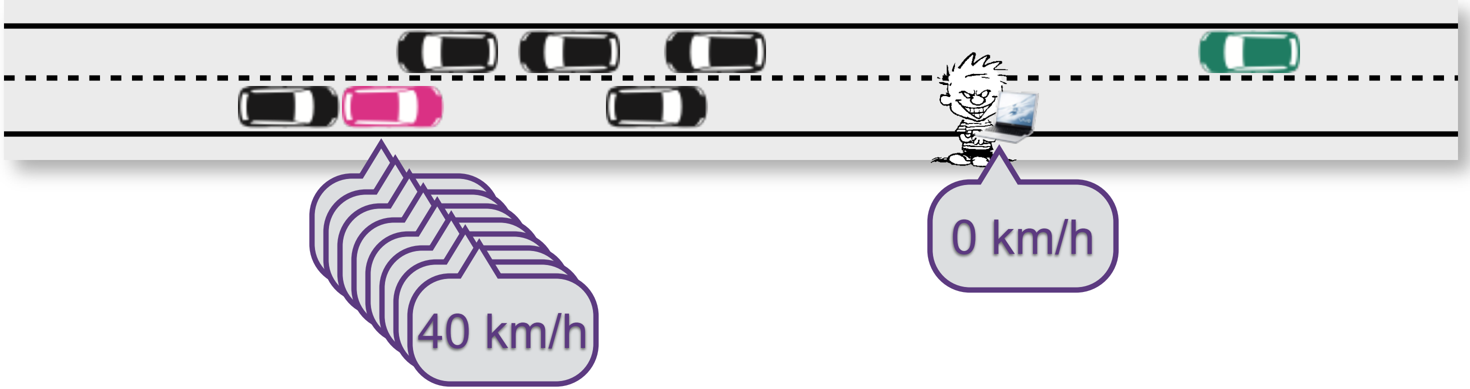
Misbehavior Detection

- Data-centric
  - Plausibility
  - Consistency
- **Node-centric**
  - **Trust-based**
  - Behavioral



No Certificate

- Misbehavior Detection
  - Data-centric
    - Plausibility
    - Consistency
  - **Node-centric**
    - Trust-based
    - **Behavioral**



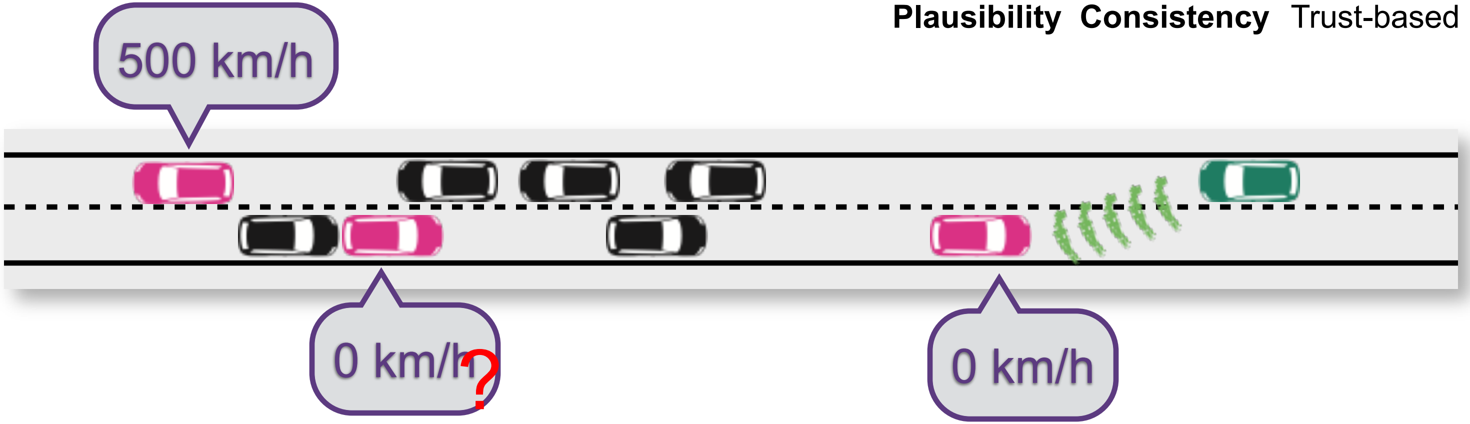
Flooding Attack

No Certificate

Misbehavior Detection

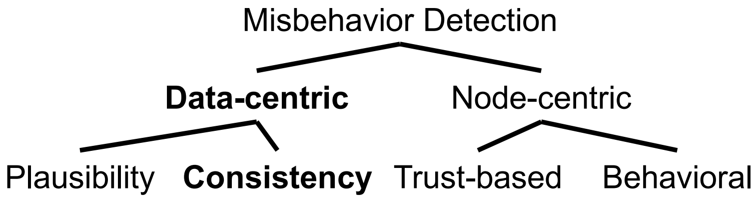
Data-centric Node-centric

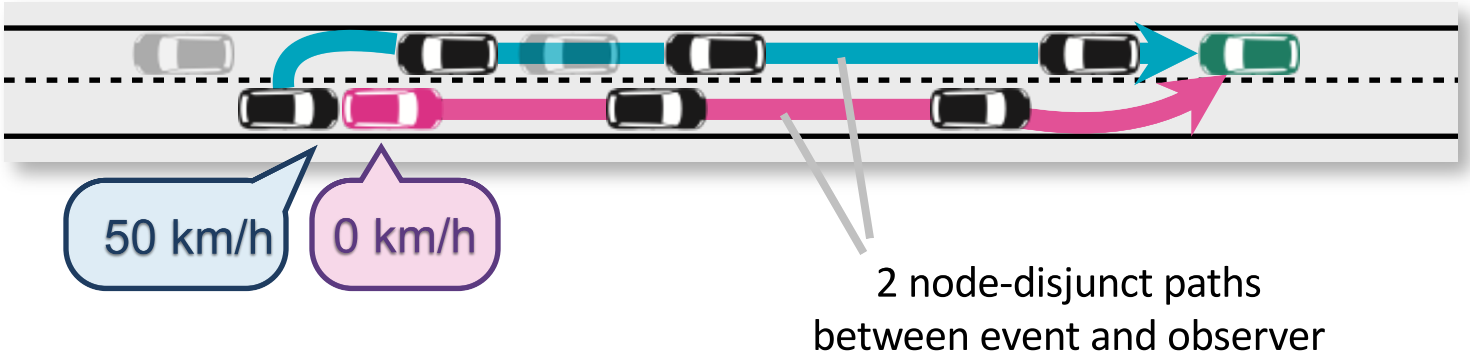
Plausibility **Consistency** Trust-based Behavioral



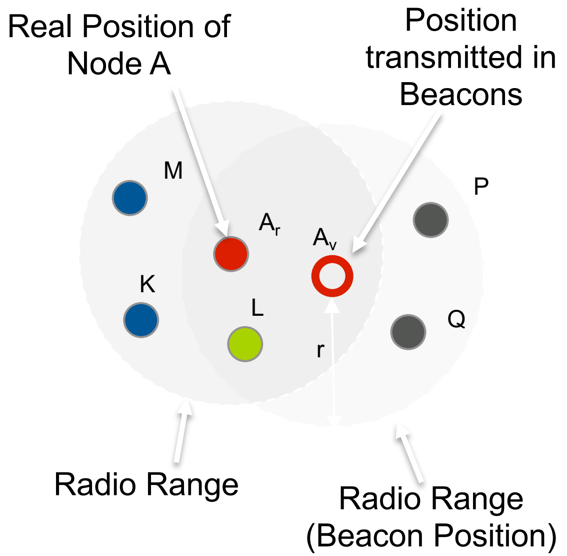
Conflicts with physical models

Conflicts with local sensors


Misbehavior Detection
Data-centric
Node-centric
Plausibility
Consistency
Trust-based
Behavioral

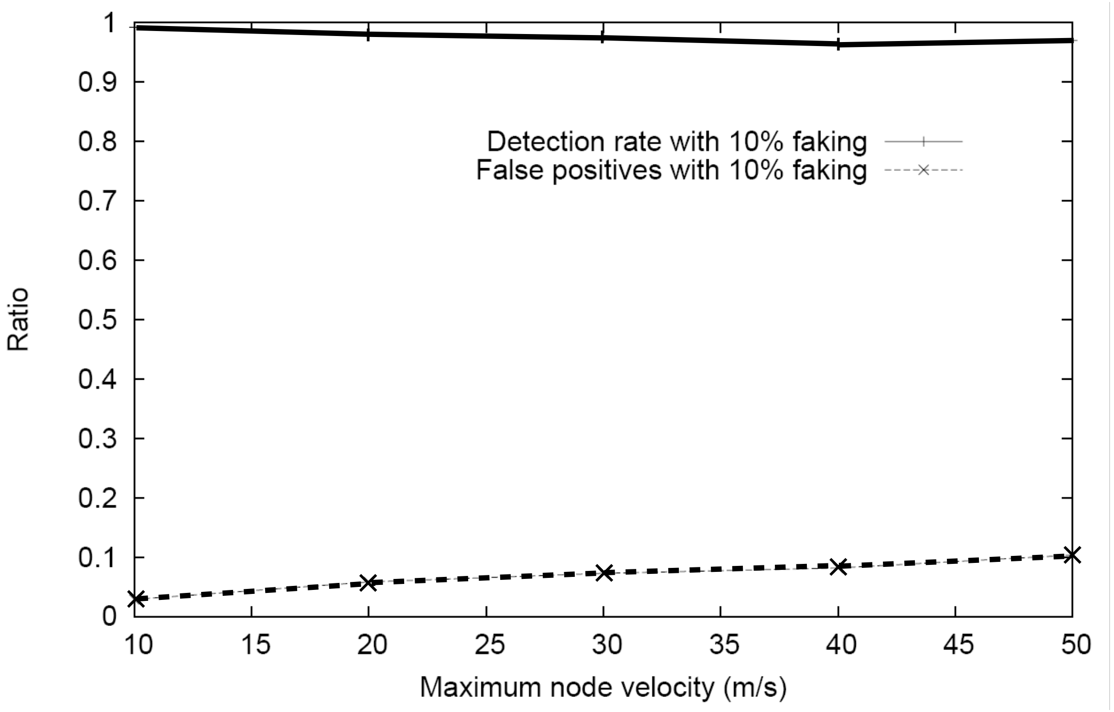

50 km/h
0 km/h
2 node-disjunct paths
between event and observer

Acceptance Range Threshold



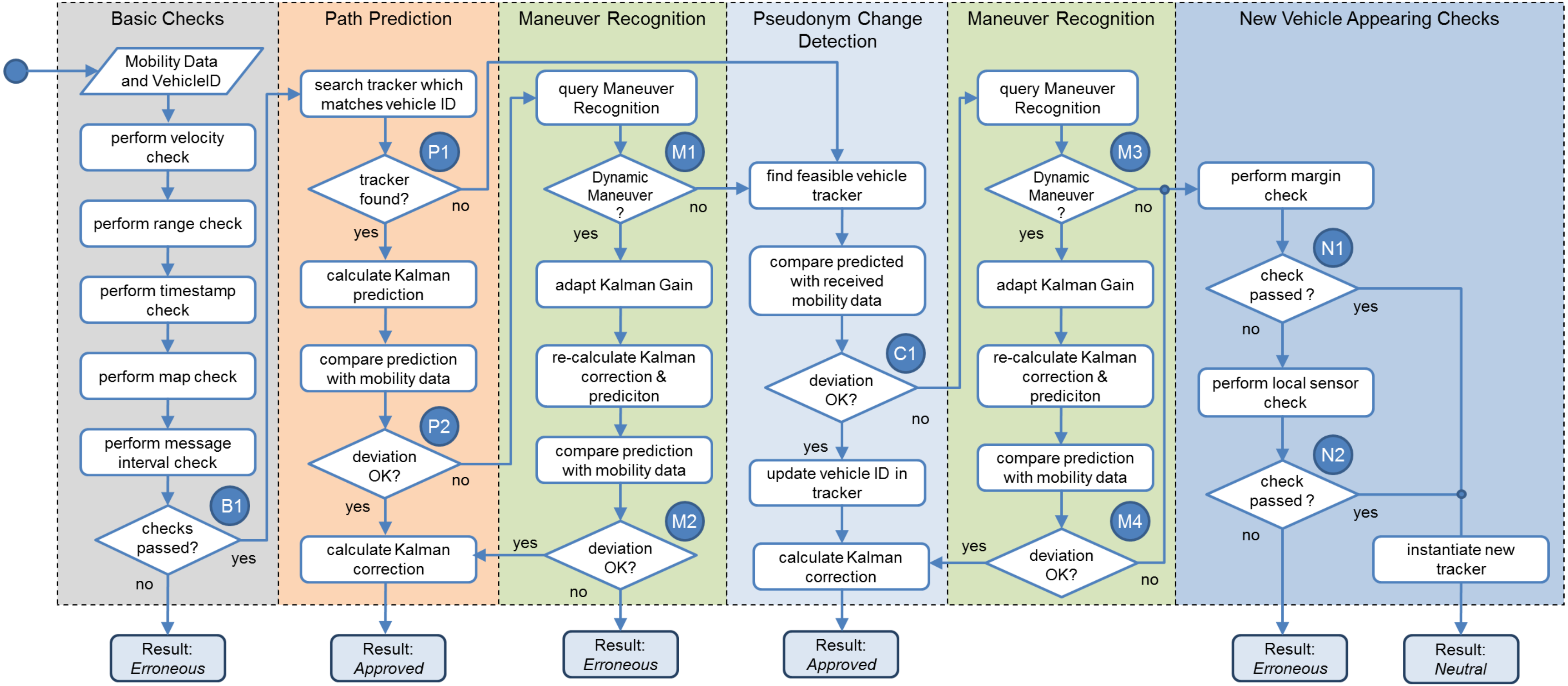
M,K: distance([M|K],A_v) > Δ_{max} -> ignore
L: distance([M|K],A_v) > Δ_{max}-> accept
Q,P: no beacon received

Detection rate ART & MGT



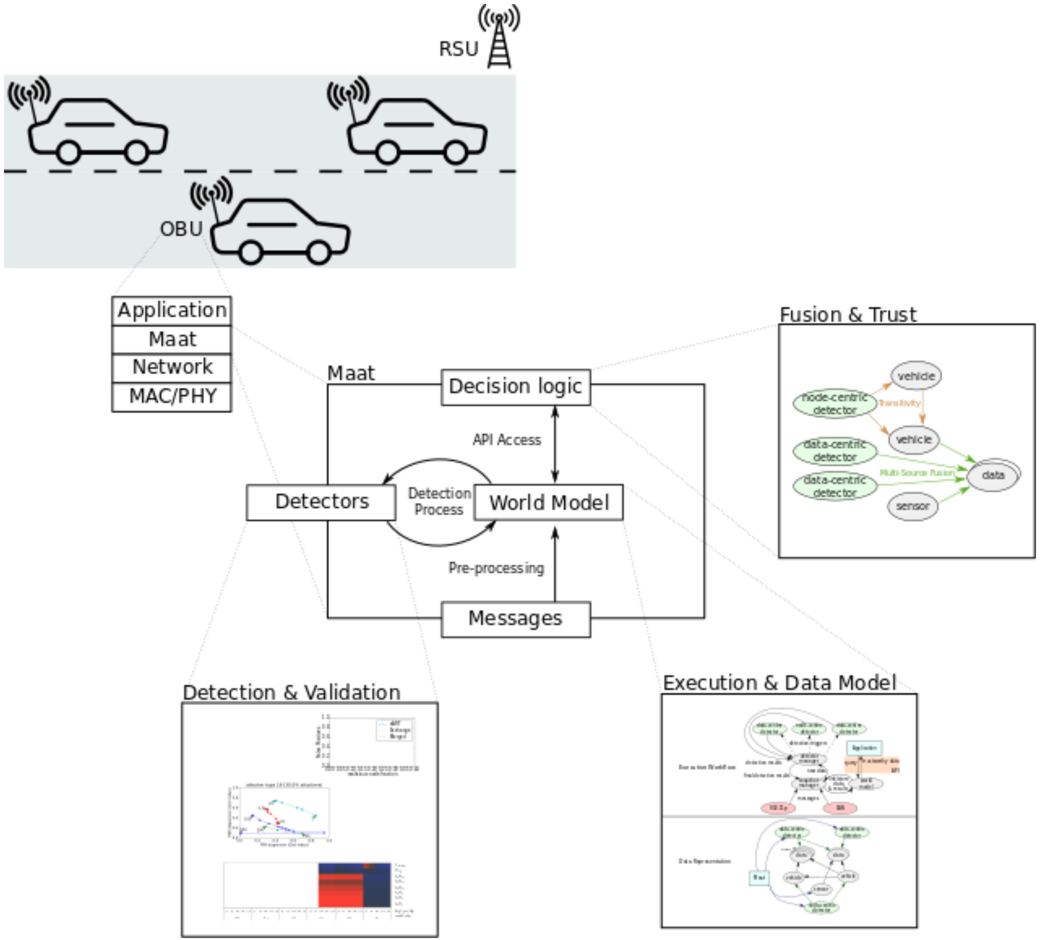
Detection rates larger than 96%
False positives between ~ 2% and 10%

Position Verification Scheme by Stübing e.a.



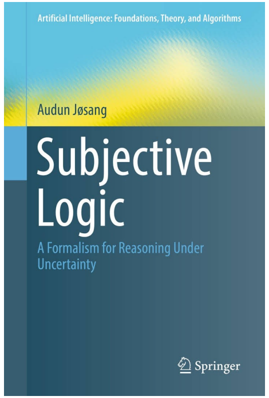
Hagen Stübing, „Multi-Layered Security and Privacy Protection in Cooperative Vehicular Networks“, PhD Thesis, TU Darmstadt, 2012

Maat MBD Framework: Flexibly Integrate many Different Detectors



Open Source:
https://github.com/vs-uulm/Maat

Subjective Logic Introduction



- Opinions:
  belief function **b(x)**, uncertainty value **u**, base rate **a(x)**
  - Representation of evidence for value **x**
  - Represent **u**ncertainty in decisions or trust
  - Separate a-priori (base rate) knowledge from belief

- Bijective relationship to Dirichlet/Beta distribution parameters
  - Simplification: binary domains (e,g., True/False)

- Fusion operators
  - BCF: Belief Constraint Fusion (equivalent to Dempster's Rule)
  - CBF: Cumulative Belief Fusion ("sum the evidence")
  - ABF: Averaging Belief Fusion ("average the evidence")
  - WBF: Weighted Belief Fusion ("confidence-weighted average")
  - CCF: Consensus & Compromise Fusion ("conflict --> vagueness")

Subjective Logic: Binary Domains

- Opinions over variable **X** with domain **D** have a belief function **b** and a base rate function **a** that map values of **D** to a value [0,1], and an uncertainty **u** from [0,1].

- For any opinion, **u + Σb(x) = 1** when summing over D.

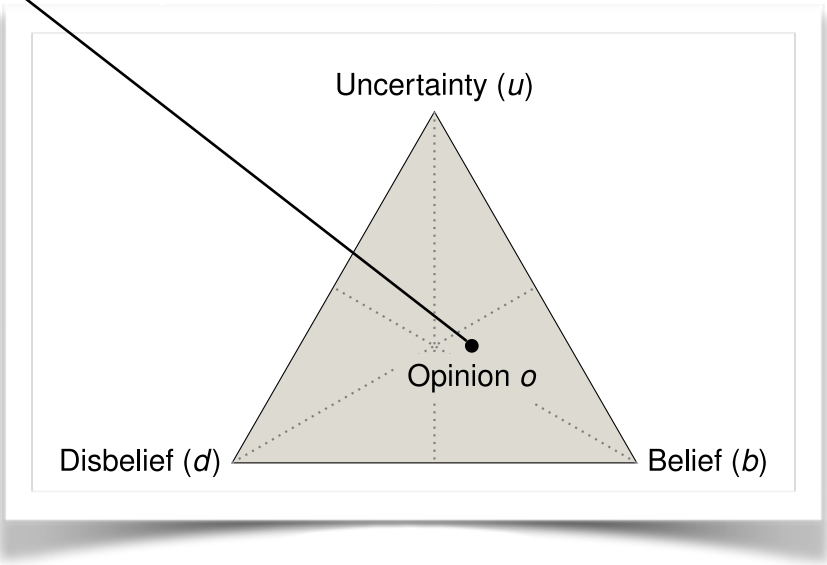
- The simplest domain contains **x** and the **inverse of x**; opinions over this domain are sometimes represented as a quadruplet **(b, d, u, a)**, where all four elements are values from [0,1] and b + d + u = 1.

- To compute the associated probability for a value x, one can project the opinion, resulting in: **P(X=x) = b + u • a** and **P(X=!x) = d + u (1 - a)**.

Subjective Logic Intuition for Binary Domains

(**b**elief,**d**isbelief,**u**ncertainty,b**a**serate)

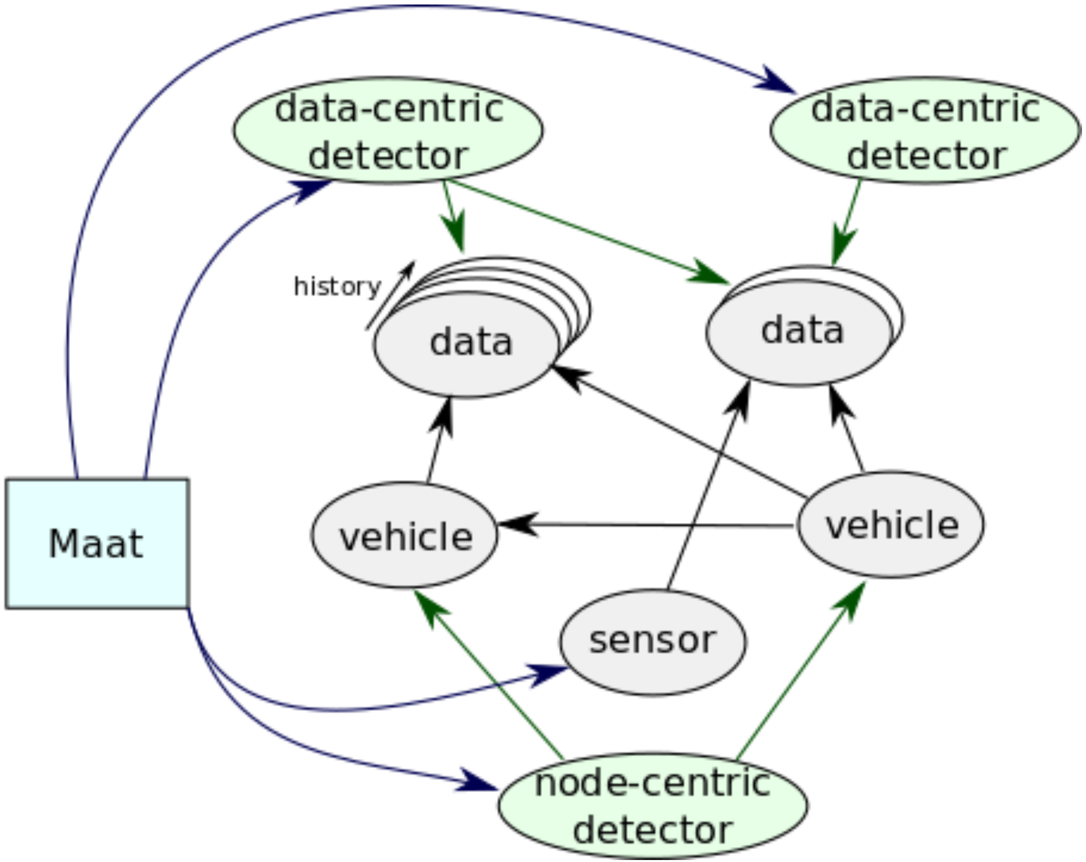
$A \xrightarrow{o} x$



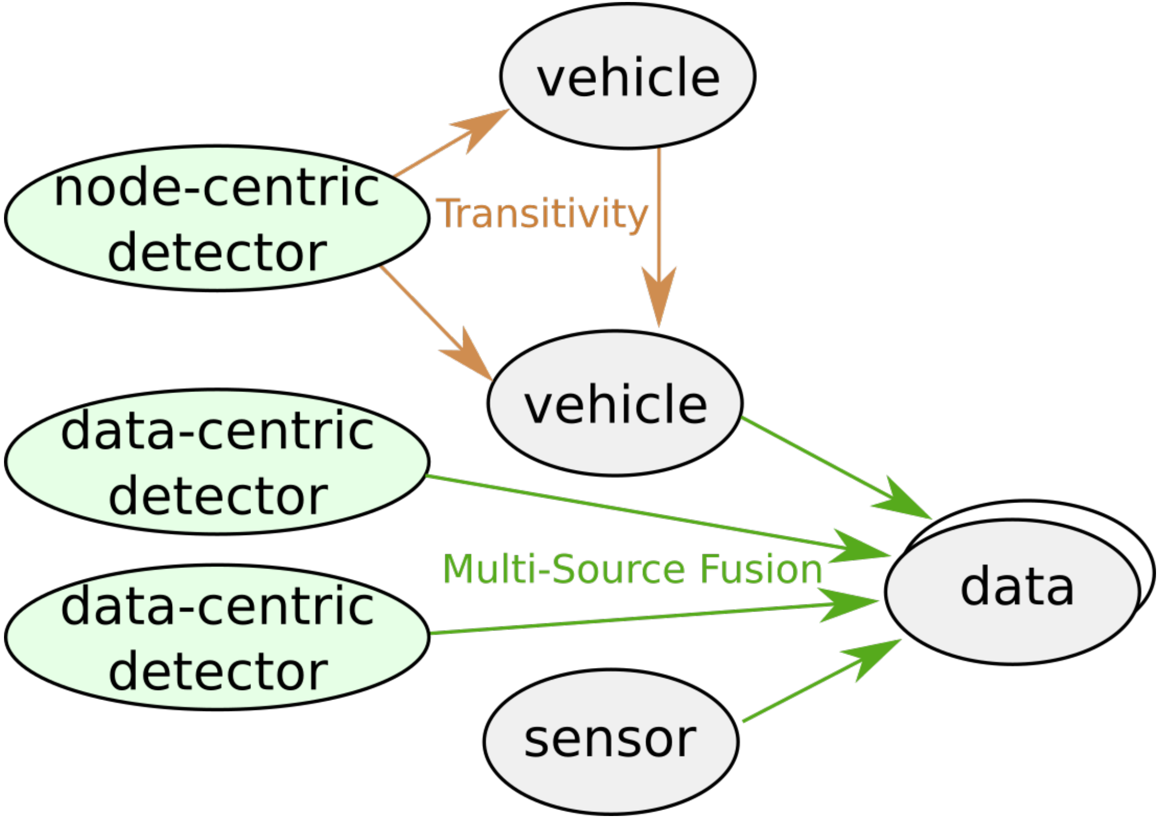
A: opinion holder
x: proposition / data value
o: opinion
b+d+u=1

Example:
o = (1,0,0,a) ≙ Boolean True

Maat: Data Model



Maat: Fusion & Trust




Communicating & Automated Cars
S 500 INTELLIGENT

universität ulm

Technische Universität Braunschweig

Fraunhofer IEM

Fraunhofer AISEC

Infineon technologies

Freie Universität Berlin

Hochschule Karlsruhe University of Applied Sciences HKA

SecForCARs
security for connected automated cars

Audi

escrypt
SECURITY. TRUST. SUCCESS.

SCHUTZWERK

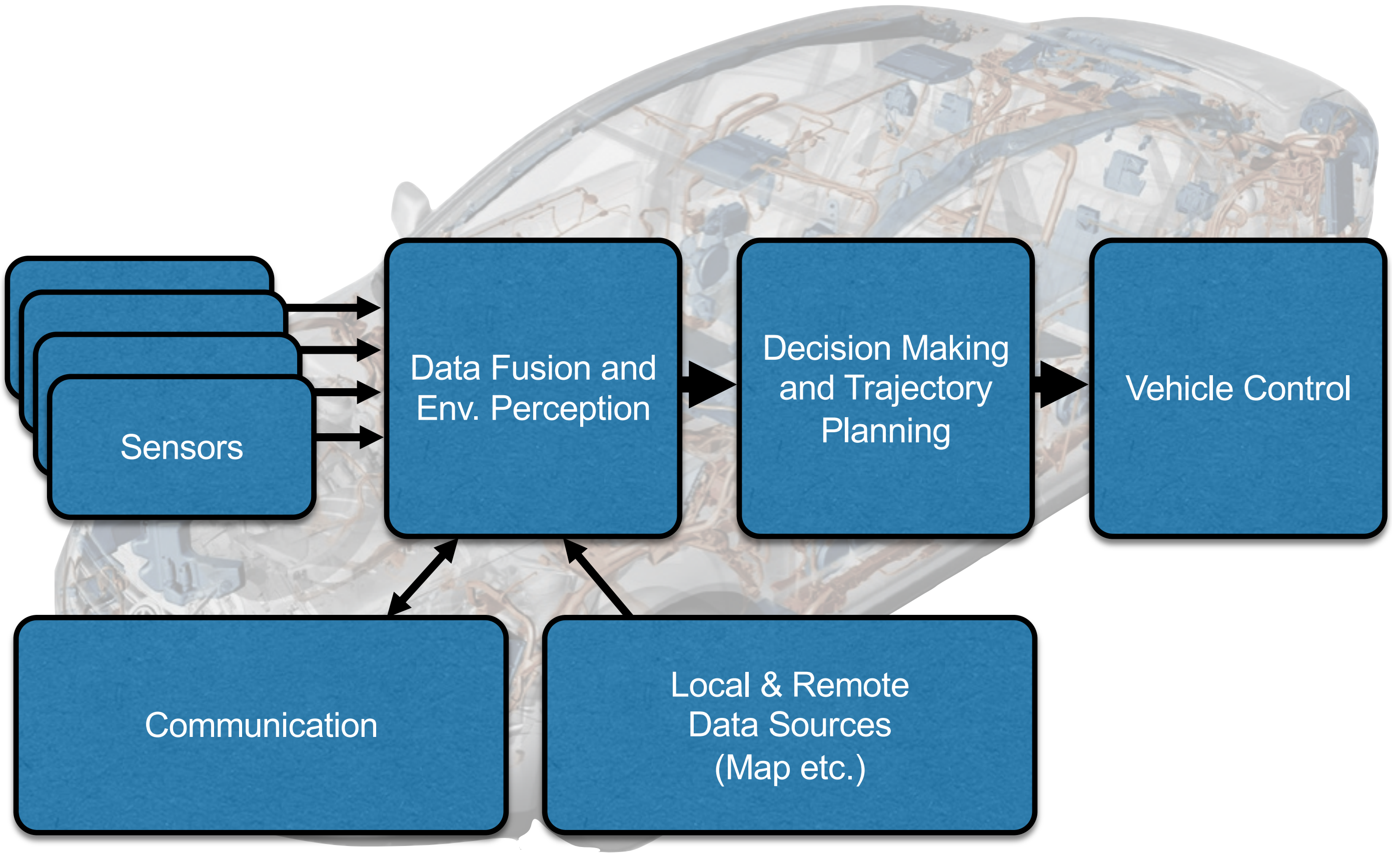
Technische Universität München TUM

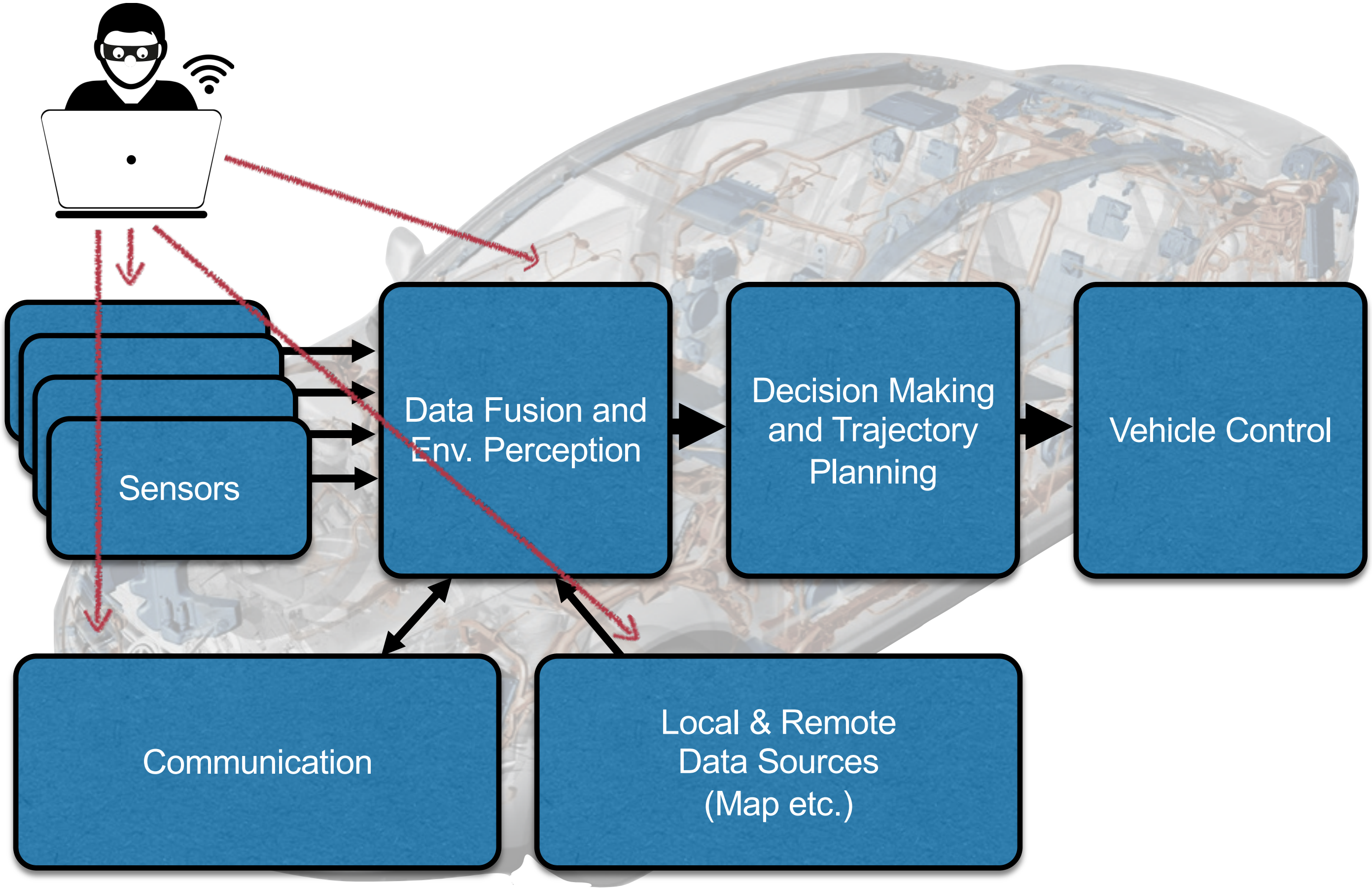
itemis

BOSCH

MIXED MODE
an Ingenics company

funding by:
Bundesministerium für Bildung und Forschung


Sensors
Data Fusion and Env. Perception
Decision Making and Trajectory Planning
Vehicle Control
Communication
Local & Remote Data Sources (Map etc.)


Sensors
Data Fusion and Env. Perception
Decision Making and Trajectory Planning
Vehicle Control
Communication
Local & Remote Data Sources (Map etc.)

2020 IEEE Vehicular Networking Conference (VNC)

Securing CACC: Strategies for Mitigating Data Injection Attacks

Michael Wolf*, Alexander Willecke†, Johannes-Christian Müller†, Keno Garlichs‡, Thomas Griebel†, Lars Wolf‡, Michael Buchholz†, Klaus Dietmayer†, Rens W. van der Heijden*, and Frank Kargl*
*Ulm University, Institute of Distributed Systems
†Ulm University, Institute of Measurement, Control and Microtechnology
‡TU Braunschweig, Institute of Operating Systems and Computer Networks

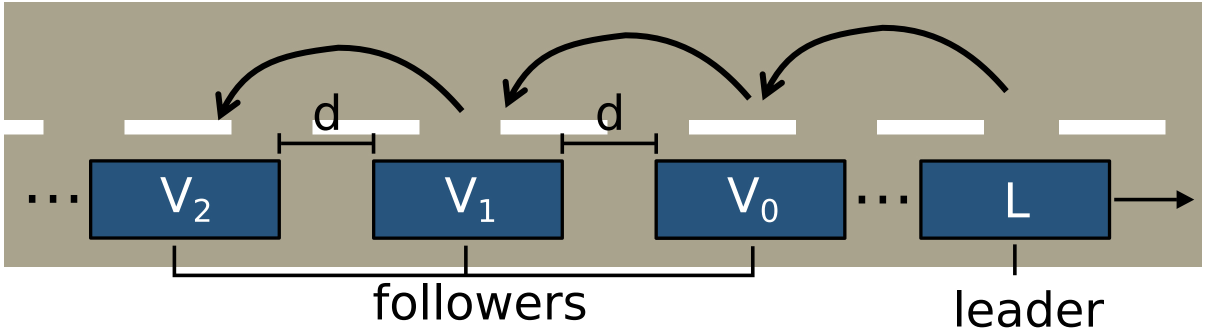
Abstract—Cooperative Adaptive Cruise Control (CACC) is a typical example for cooperative maneuvers of connected, automated vehicles. Safe operation of any such vehicle highly depends on information emitted by the surrounding vehicles as it is processed by the vehicle's longitudinal controller. This opens an attack surface affecting vehicle safety. This paper studies how CACC controllers can be protected against such attacks to ensure the safety of the vehicle and its passengers. This raises the question of how to mitigate injection of false data into the controller by attacks and other forms of vehicle misbehavior. Based on a literature analysis, this paper defines a new categorization for mitigation strategies, discussing their individual strengths, weaknesses and their potential for attack mitigation. This categorization can be used to derive novel ideas for mitigations, for example, an approach with a parameter-dependent reaction of the controller based on a suspiciousness parameter signaled by the Misbehavior Detection System (MDS). Through a simulation study, we show that this approach improves safety and efficiency of the platoon under attack but also identify a fundamental trade-off between these two design goals.

Index Terms—vehicular networking, automated driving, security, safety

I. INTRODUCTION

Misbehavior Detection

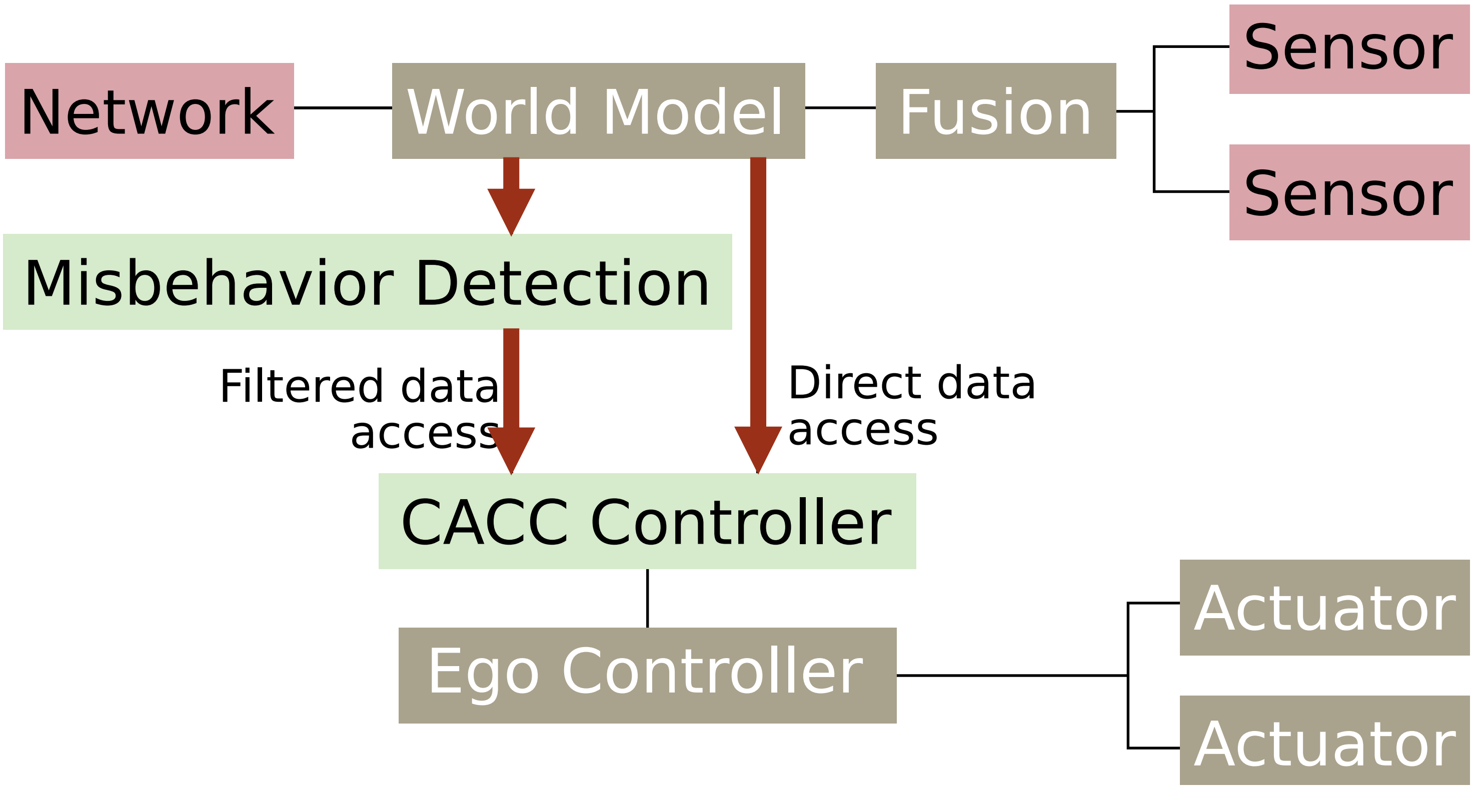
Cooperative Adaptive Cruise Control (CACC)

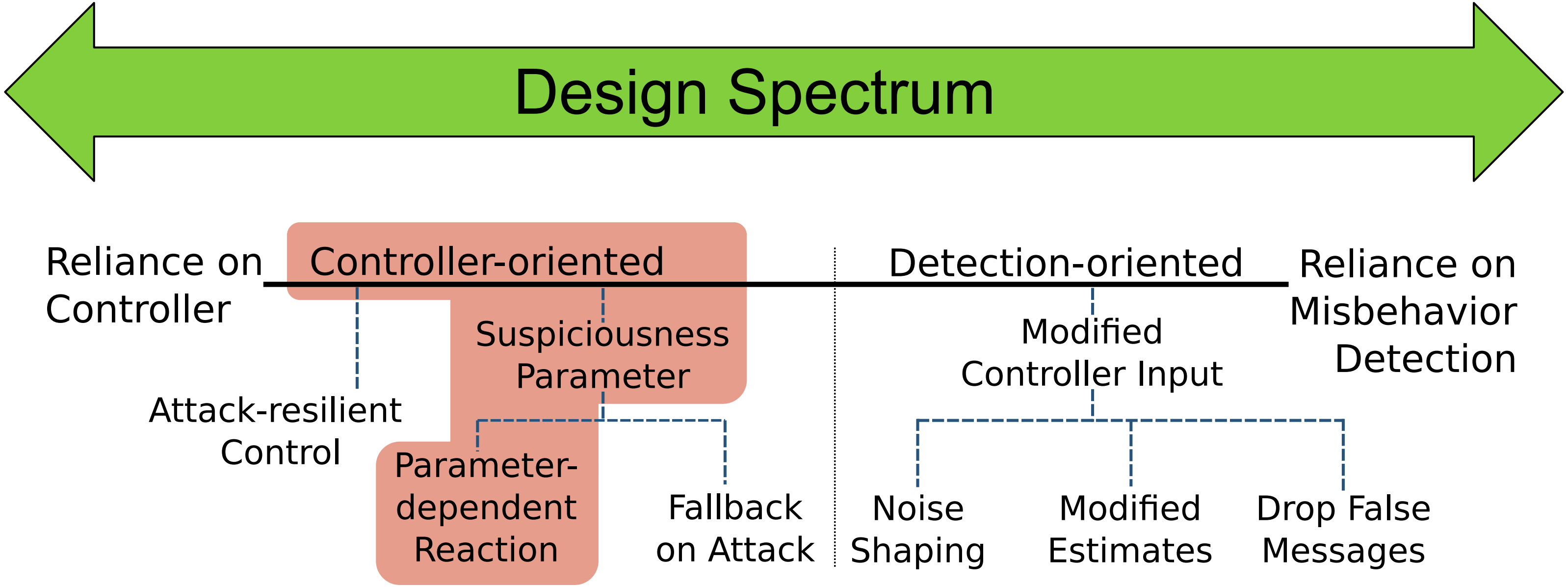



2017 IEEE Vehicular Networking Conference (VNC)

Analyzing Attacks on Cooperative Adaptive Cruise Control (CACC)

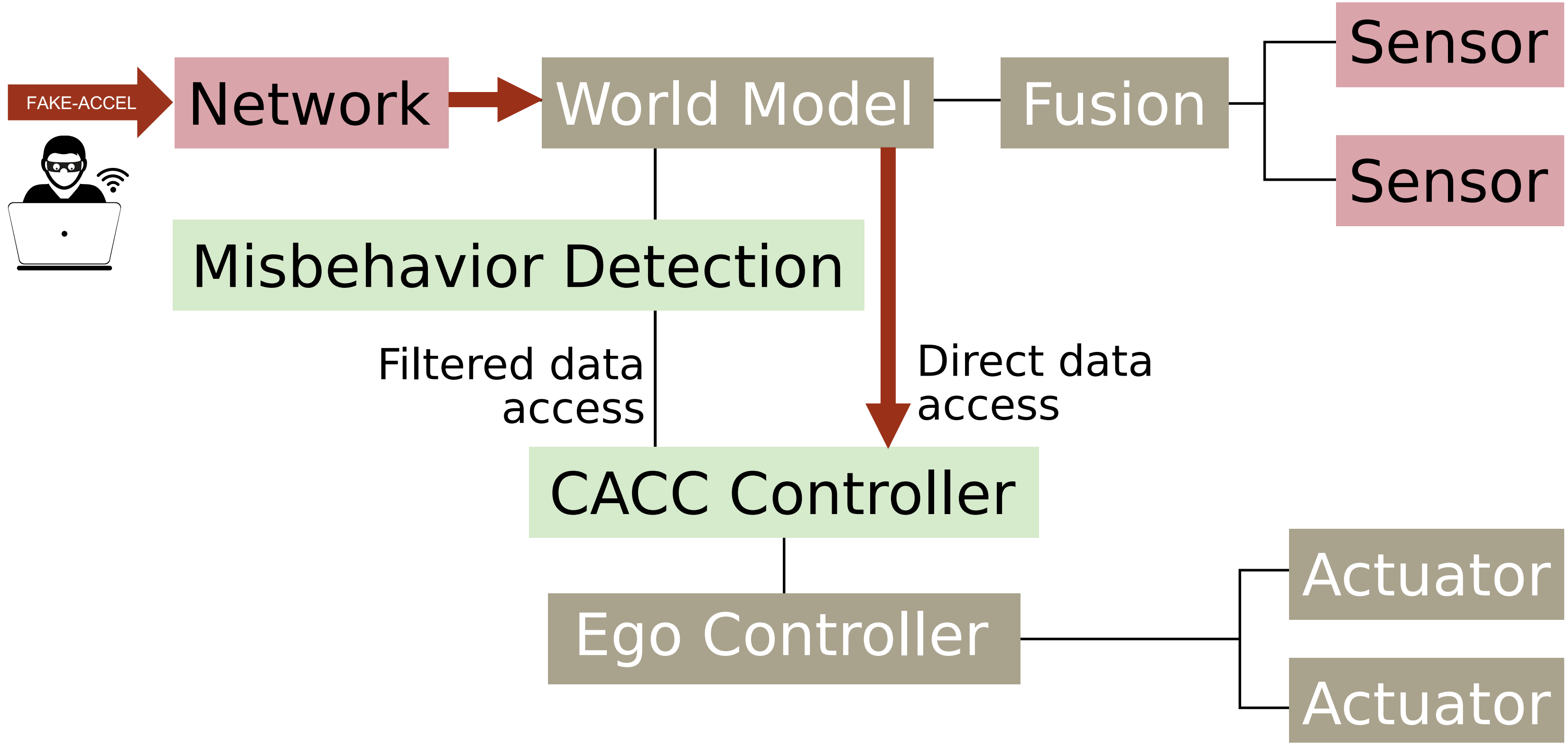
Rens van der Heijden, Thomas Lukaseder, Frank Kargl
Institute of Distributed Systems
Ulm University, Germany
rens.vanderheijden@uni-ulm.de, thomas.lukaseder@uni-ulm.de, frank.kargl@uni-ulm.de


Network
World Model
Fusion
Sensor
Sensor
Misbehavior Detection
Filtered data access
Direct data access
CACC Controller
Ego Controller
Actuator
Actuator


Design Spectrum
Reliance on Controller
Controller-oriented
Detection-oriented
Reliance on Misbehavior Detection
Attack-resilient Control
Suspiciousness Parameter
Parameter-dependent Reaction
Fallback on Attack
Modified Controller Input
Noise Shaping
Modified Estimates
Drop False Messages

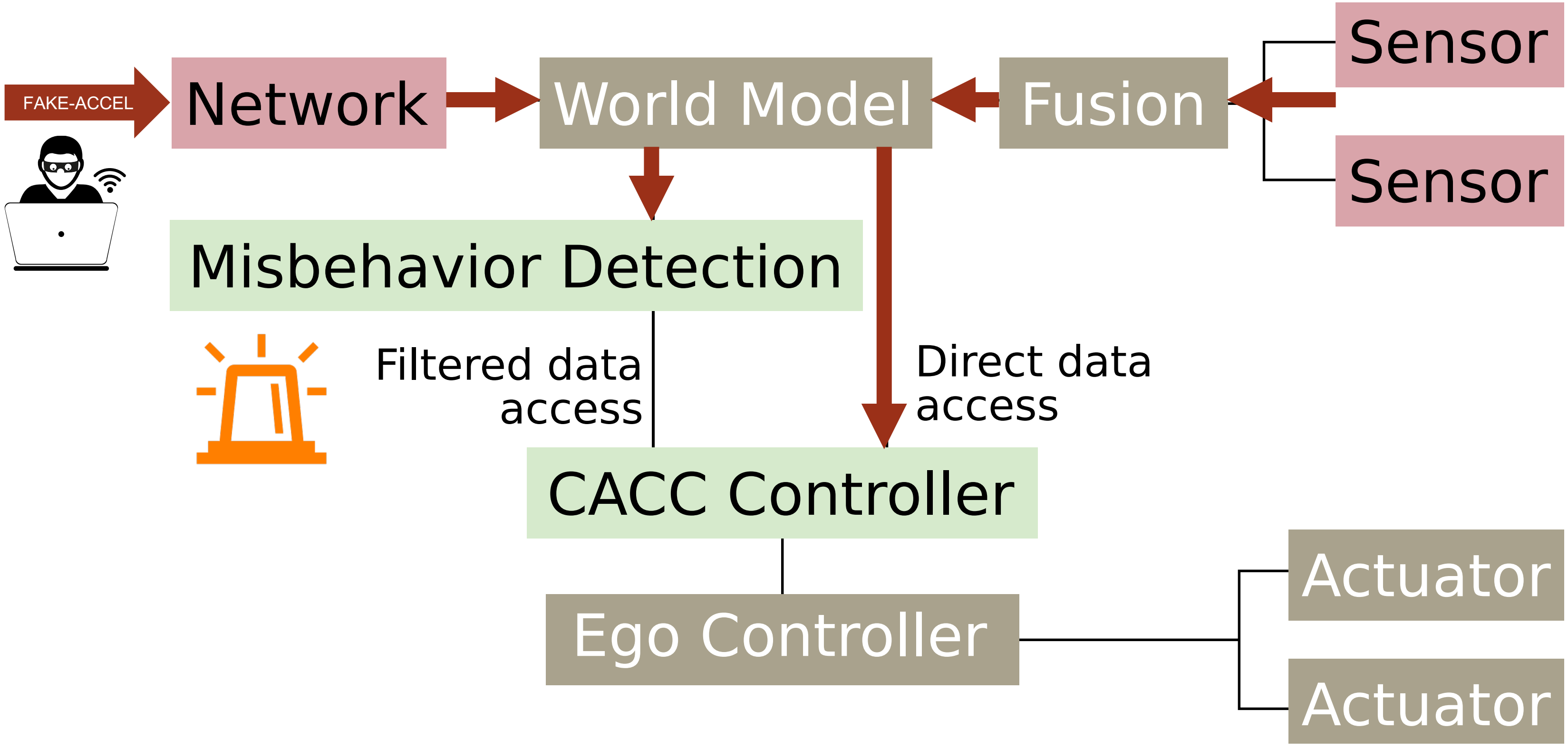
Mitigating Acceleration Attacks through MBD and Susp. Param.

Strategy 1: No MBD (Baseline)



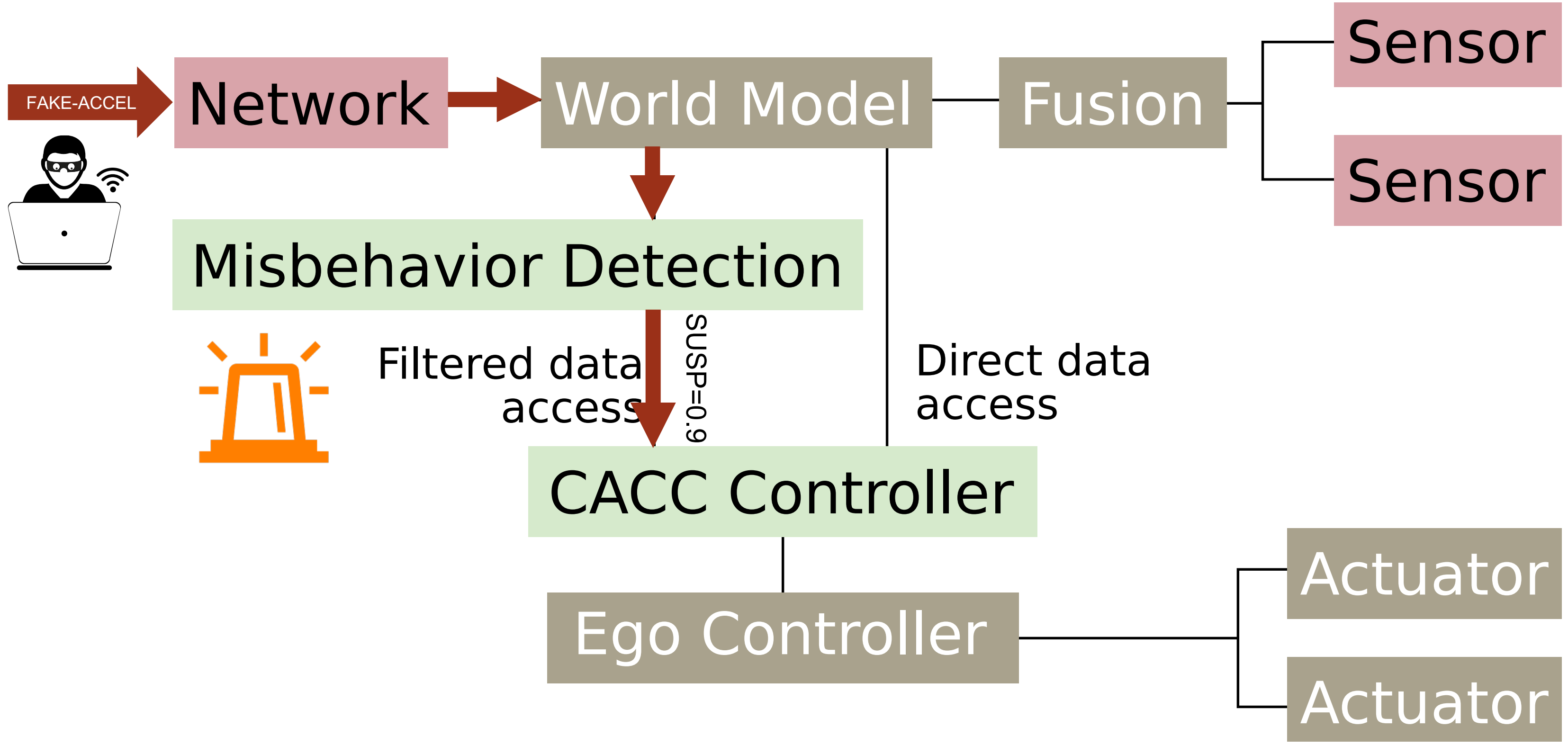
Mitigating Acceleration Attacks through MBD and Susp. Param.

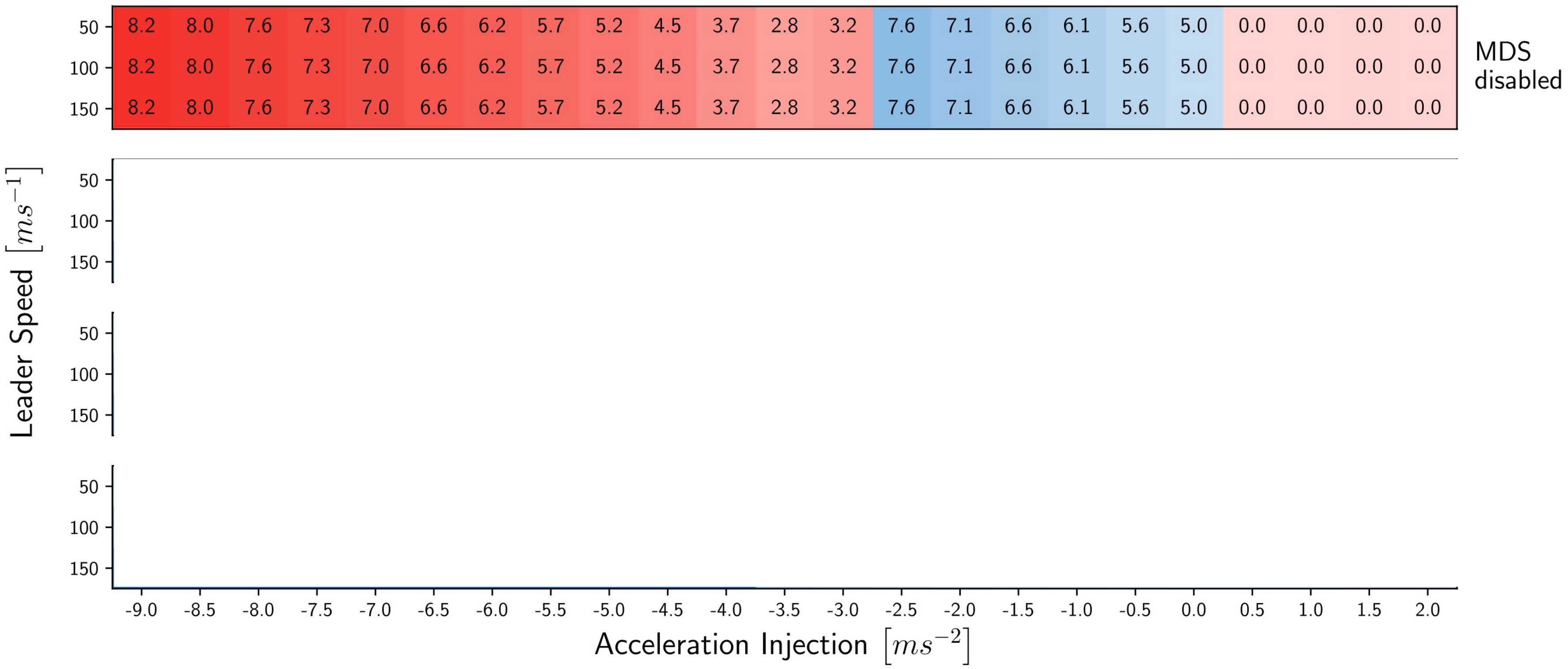
Strategy 2: Fallback to ACC



Mitigating Acceleration Attacks through MBD and Susp. Param.

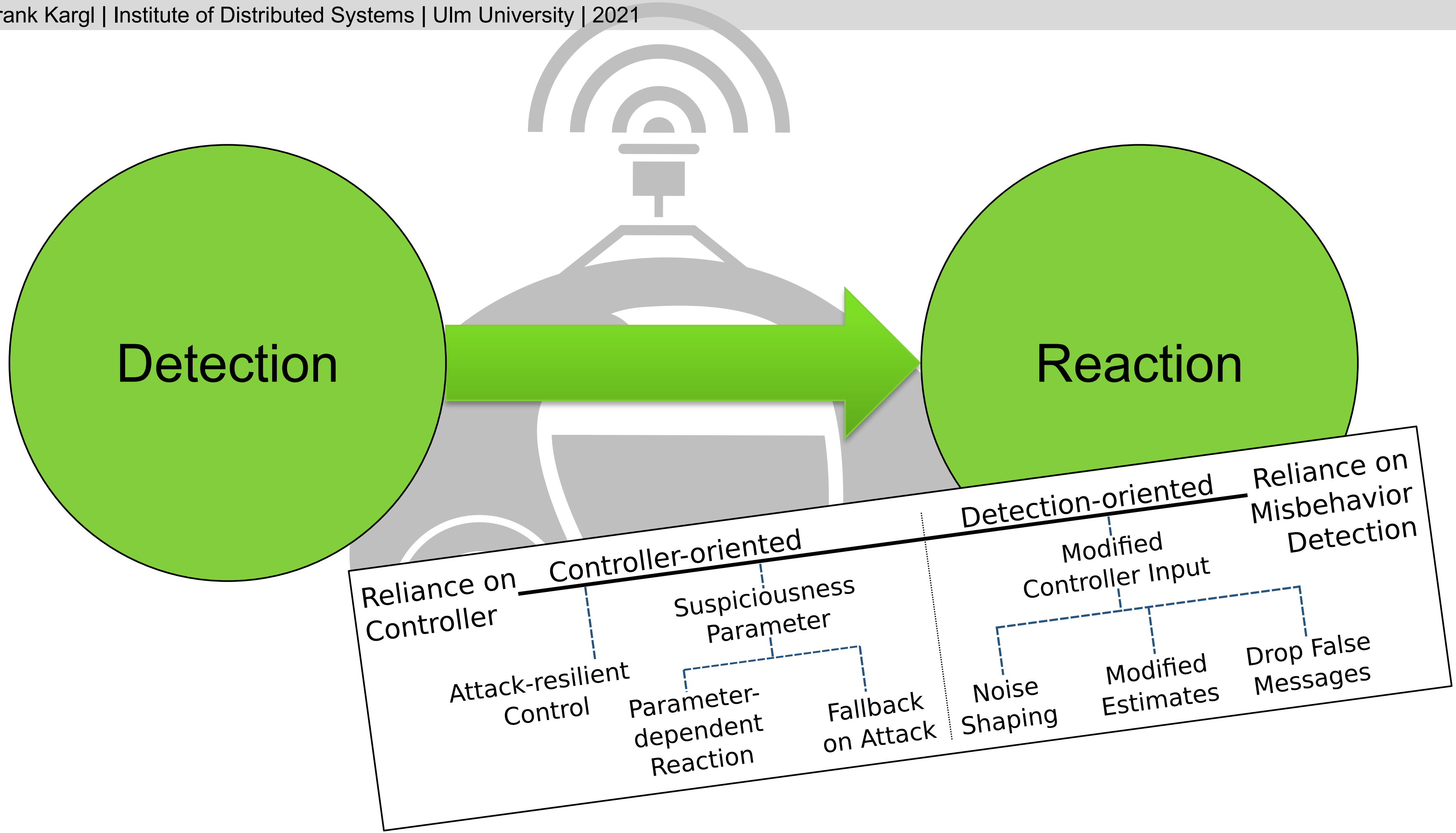
Strategy 3: Suspiciousness Param and Adjusted Controller Reaction




8.2 8.0 7.6 7.3 7.0 6.6 6.2 5.7 5.2 4.5 3.7 2.8 3.2 7.6 7.1 6.6 6.1 5.6 5.0 0.0 0.0 0.0 0.0
8.2 8.0 7.6 7.3 7.0 6.6 6.2 5.7 5.2 4.5 3.7 2.8 3.2 7.6 7.1 6.6 6.1 5.6 5.0 0.0 0.0 0.0 0.0
8.2 8.0 7.6 7.3 7.0 6.6 6.2 5.7 5.2 4.5 3.7 2.8 3.2 7.6 7.1 6.6 6.1 5.6 5.0 0.0 0.0 0.0 0.0
MDS disabled
50
100
150
Leader Speed $[ms^{-1}]$
-9.0 -8.5 -8.0 -7.5 -7.0 -6.5 -6.0 -5.5 -5.0 -4.5 -4.0 -3.5 -3.0 -2.5 -2.0 -1.5 -1.0 -0.5 0.0 0.5 1.0 1.5 2.0
Acceleration Injection $[ms^{-2}]$

Demonstrator : CACC “Carrerabahn”

CACC and Data Injection Attack

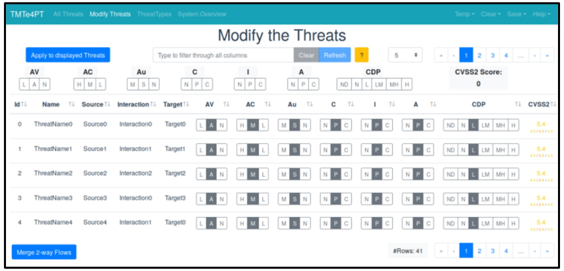


Google Car Created by James Mayle from the Noun Project

SecForCARs: More Topics and Results

SecForCARs security for connected automated cars

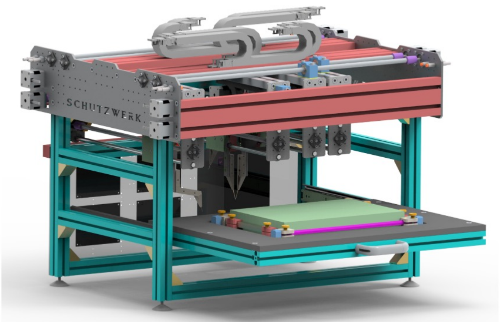
Methods and Tools for Safety/Security Modelling and Risk Analysis



Threat Modeling Tool Extension for Penetration Tester (TMTe4PT)

Attack Use-Case Visualization

Attacks and Penetration Testing



Automating ECU security testing

Attacks on RADAR

SOME/IP Fuzzing Framework

Automotive Responsible Disclosure FW

Security Mechanisms and Concepts

Secure ECU concepts, e.g., using PUFs

Secure Sensor Data Fusion

IDS / MBD Integration

SecForCARs Extension: Securing Automated Vehicles (SAVE)

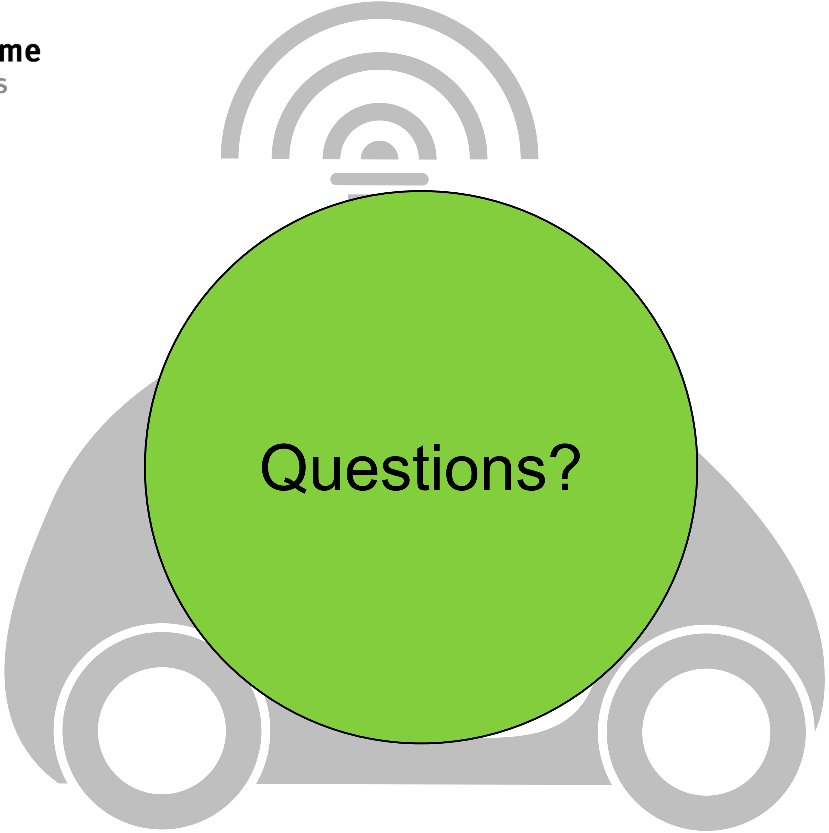
SIP NEDO
YNU YOKOHAMA National University pwc
TOYOTA

SecForCARs security for connected automated cars
Infineon Universität Ulm Fraunhofer IEM Fraunhofer AISEC
Hochschule Karlsruhe Technik und Wirtschaft UNIVERSITY OF APPLIED SCIENCES
escrypt SECURITY. TRUST. SUCCESS.
DENSO
Freie Universität Berlin

Joining Expertise

Institut für Verteilte Systeme
Institute of Distributed Systems

SecForCARs
security for connected automated cars



Email me at frank.kargl@uni-ulm.de or join a Slack discussion

Google Car Created by James Mayle from the Noun Project