universität ulm

Institut für Verteilte Systeme
Institute of Distributed Systems

SecForCARs
security for connected automated cars

Misbehavior Detection and Prevention in Connected, Automated Driving

Prof. Dr. Frank Kargl, Ulm University, Germany

SIP-adus Workshop 2021

Complexity of Connected & Automated Vehicles poses new challenges to S&P

© Steve Jurvetson, “hands-free Driving”, CC-BY-2.0

© Jaguar MENA, CC-BY-2.0

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

itemis

Technische Universität München

BOSCH

MIXED MODE

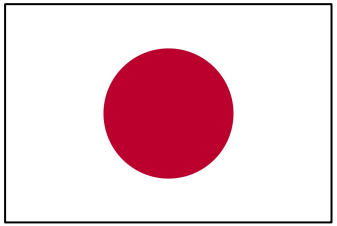
an Ingenics company

funding by:

Bundesministerium für Bildung und Forschung

SecForCARs
security for connected automated cars

joins expertise with Japan



SIP

NEDO

YNU
YOKOHAMA National University

pwc

TOYOTA

SecForCARs
security for connected automated cars

infineon

Fraunhofer IEM

Fraunhofer AISEC

Hochschule Karlsruhe
University of
Applied Sciences

HKA

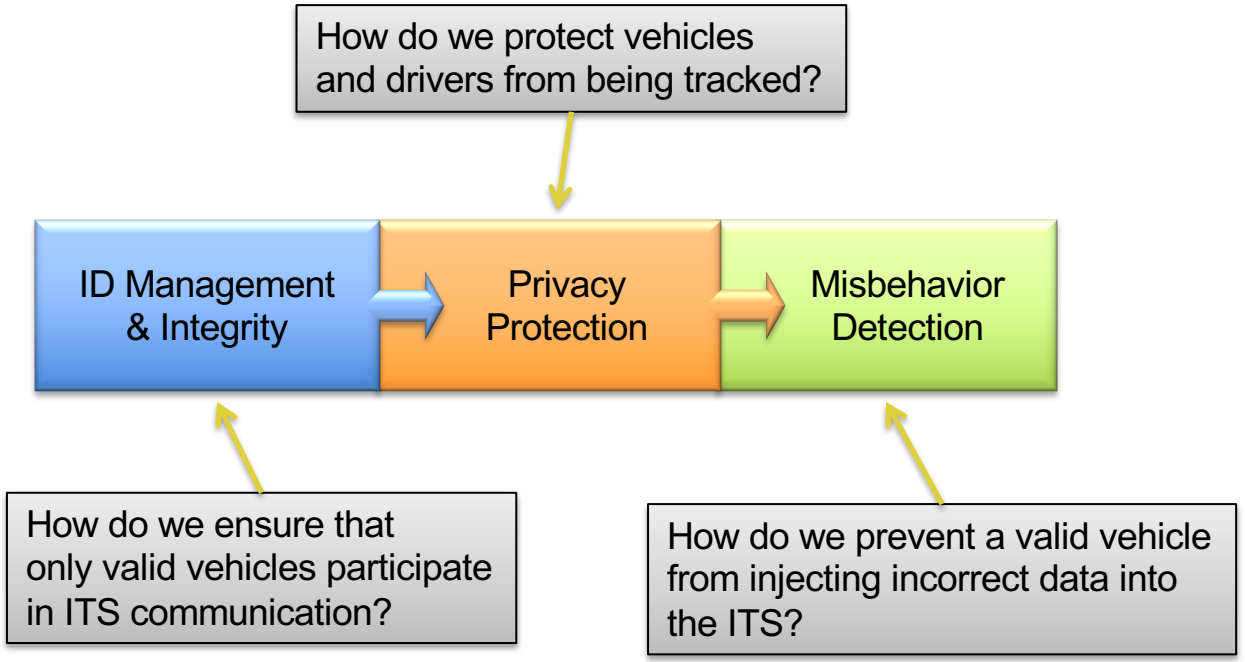
DENSO

escrypt
SECURITY. TRUST. SUCCESS.

Freie Universität Berlin

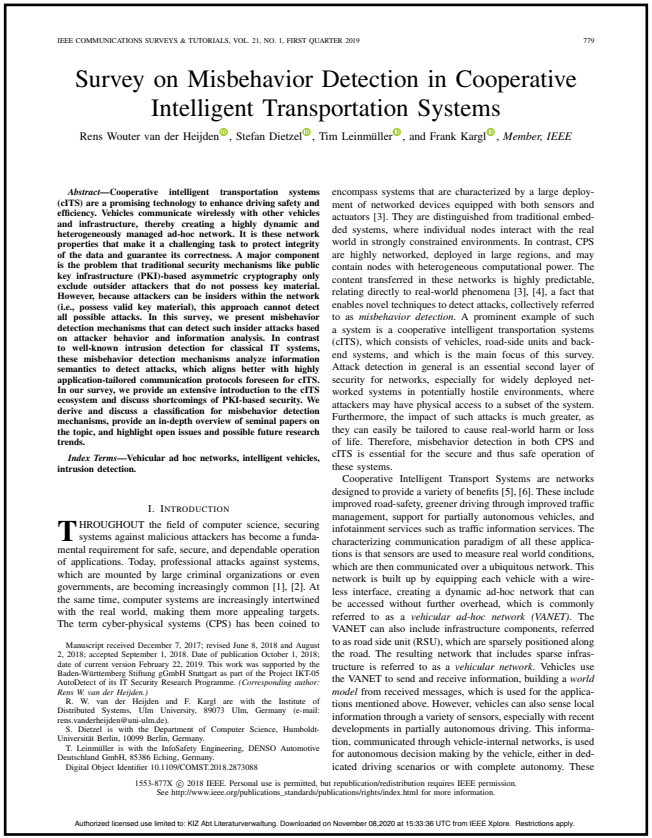
Securing Automated Vehicles
SAVE

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

Survey on 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.)*

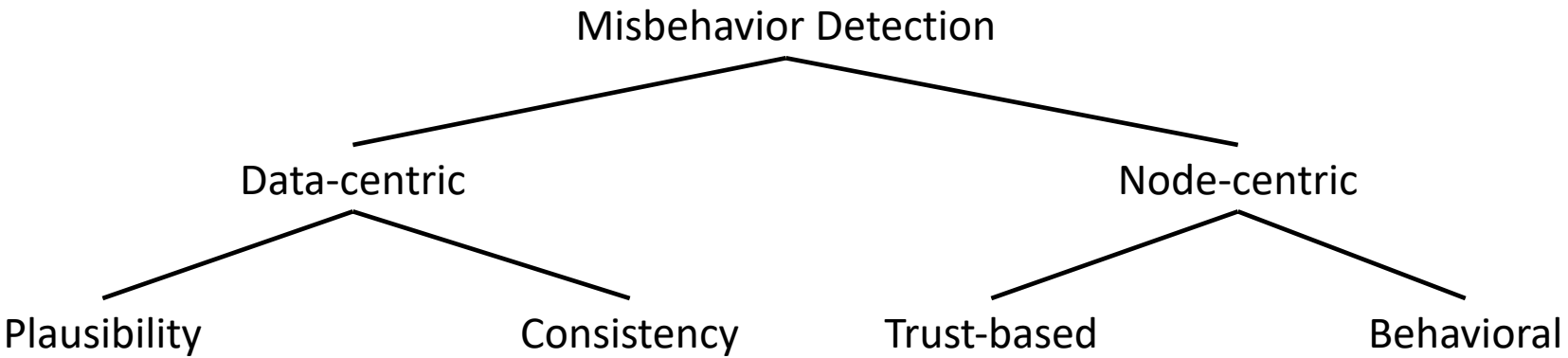
R. W. van der Heijden and F. Kargl are with the Institute of Distributed Systems, Ulm University, 89073 Ulm, Germany (e-mail: rens.vanderheijden@uni-ulm.de).

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.

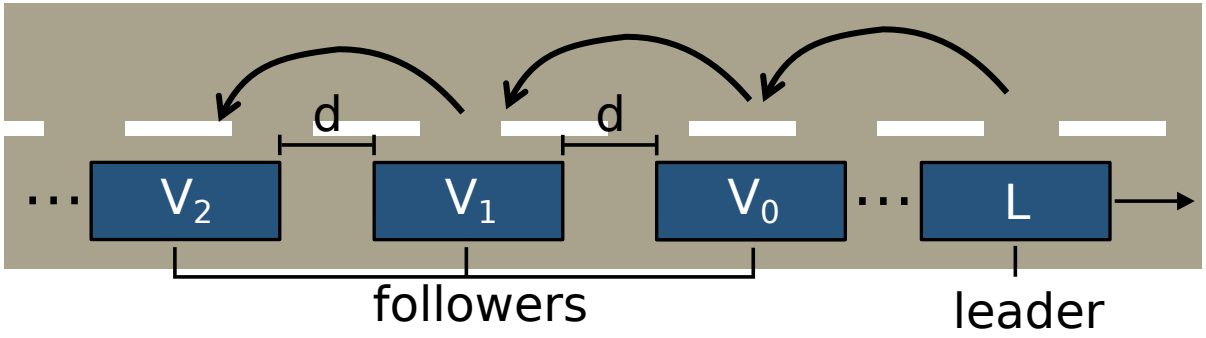
Digital Object Identifier 10.1109/COMST.2018.2873088

Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems, IEEE Comm S&T, 21(1), 2019


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

Cooperative Adaptive Cruise Control (CACC)

Cooperative Adaptive Cruise Control (CACC)




Analyzing Attacks on Cooperative Adaptive Cruise Control (CACC)

Analyzing Attacks on CACC, IEEE Vehicular Networking Conference (VNC) 2017

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

Increased mobility and trends for just-in-time delivery and online retail has led to an ever-increasing amount of road traffic. However, increasing traffic comes at a price, such as traffic congestion due to limited road capacity, huge energy consumption, air pollution, and the loss of life due to traffic accidents. According to one survey[1], each commuter in the city of Hamburg spent 113 hours in traffic congestion in 2019. It is estimated that 3.1 billion gallons of gasoline were wasted worldwide due to traffic congestion in 2014 [1]. It is estimated that 11.7 billion liters of gasoline were wasted worldwide due to traffic congestion in 2014 [1]. Furthermore, according to the statistics in [2], more than 30,000 people were killed on U.S. highways during accidents in 2014.

Cooperative intelligent transport system (C-ITS) use communication between vehicles to make driving safer or more efficient. One specific application of C-ITS is cooperative adaptive cruise control (CACC) which uses vehicular communication to coordinate platoons of self-driving cars following each other at short distance. There, all driving actions are communicated from the leading vehicle to its following vehicles, decreasing the reaction time compared to simple adaptive cruise control (ACC), which relies only on local sensors like radar. As a result of the tight coordination, the safety distances between the participating connected automated vehicles (CAVs) can be decreased, leading to an increase in road capacity and reduced fuel consumption. This reduction of fuel consumption is estimated to reach up to 30% [3]. Market introduction of CACC is being prepared, e.g., through the pre-standardization efforts of European telecommunications standards institute (ETSI), the standards body responsible for cooperative intelligent transport system in Europe [4], [5].

While CACC has been studied intensively for decades, and various surveys exist on both the control [1], [6], [7] and communication [7], [8] aspects, the security aspect came into focus only recently [9], [10]. However, in the wider setting of C-ITS and vehicular ad-hoc networks, security in general [11] and misbehavior detection in particular [12], [13] have received significant attention. Misbehavior detection refers to the detection of attacks in which authenticated vehicles transmit incorrect values (i.e., values that do not match the real world situation) in otherwise legitimate and correctly signed messages. Such misbehavior attacks typically origin either from malfunctioning cars or from attackers which have the goal to reduce the quality of service or even cause crashes. Although many of the security and misbehavior detection mechanisms developed in C-ITS are applicable also to CACC, in this paper we discuss a challenge that is specific to CACC: the short-term mitigation of detected misbehavior.

There are many approaches to detect misbehavior [12], mainly by checking plausibility or consistency of received data or by identifying anomalous behavior of sending vehicles. We illustrate this by an example shown in Figure 1. On top, a typical CACC platoon is illustrated, with a leader and some followers. The bottom shows an example of a false data injection attack: the dark red vehicle A transmits a faked (*claimed*) negative acceleration and corresponding false position shown in light red as if it would break sharply. This would put it in a dangerous position in front of vehicle V_1 which would have to react by braking itself. Here, it is assumed that the messages are cryptographically signed and that the signatures and certificates are valid as the attacker's vehicle possesses

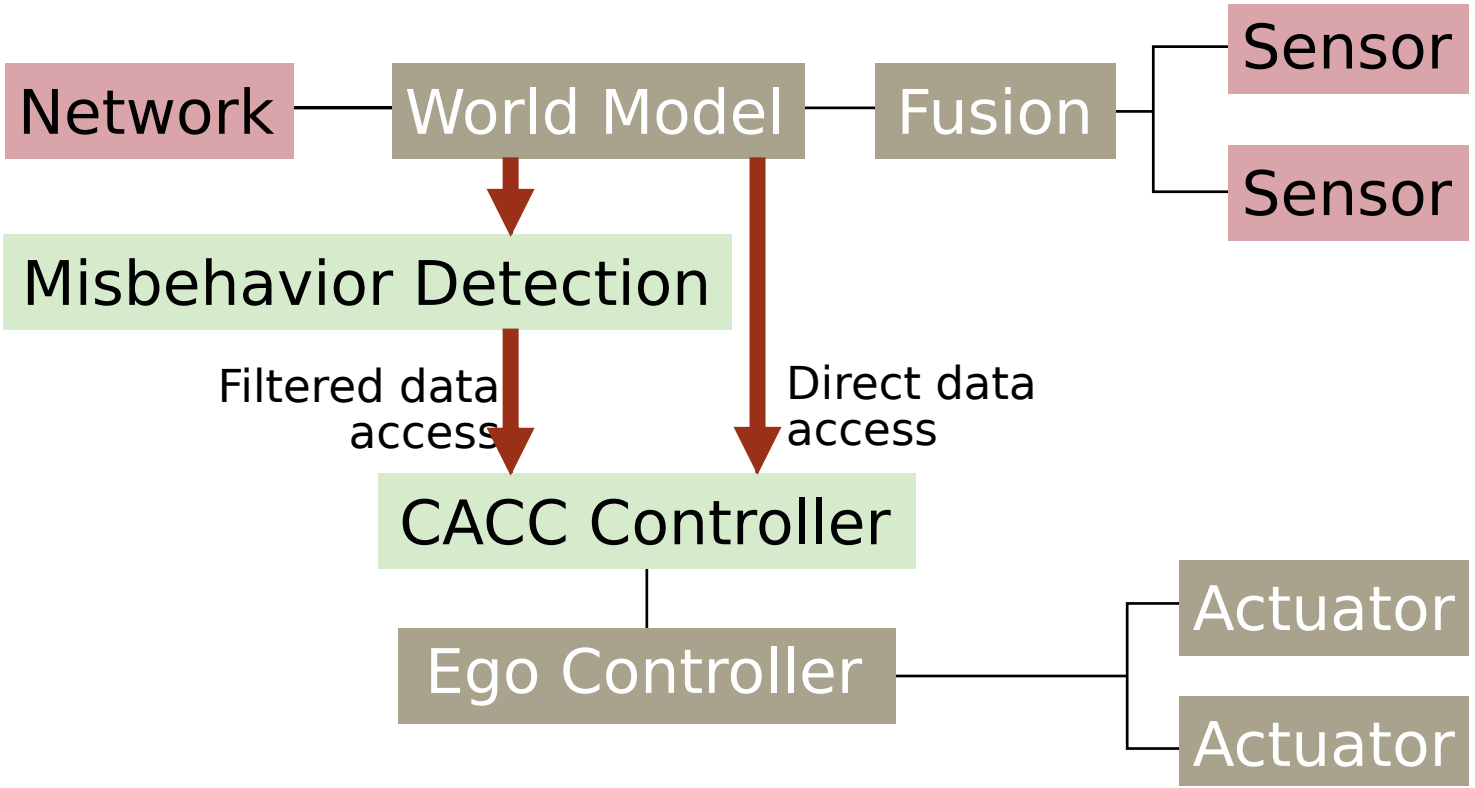
[1] https://www.openpr.de/news/1051162/

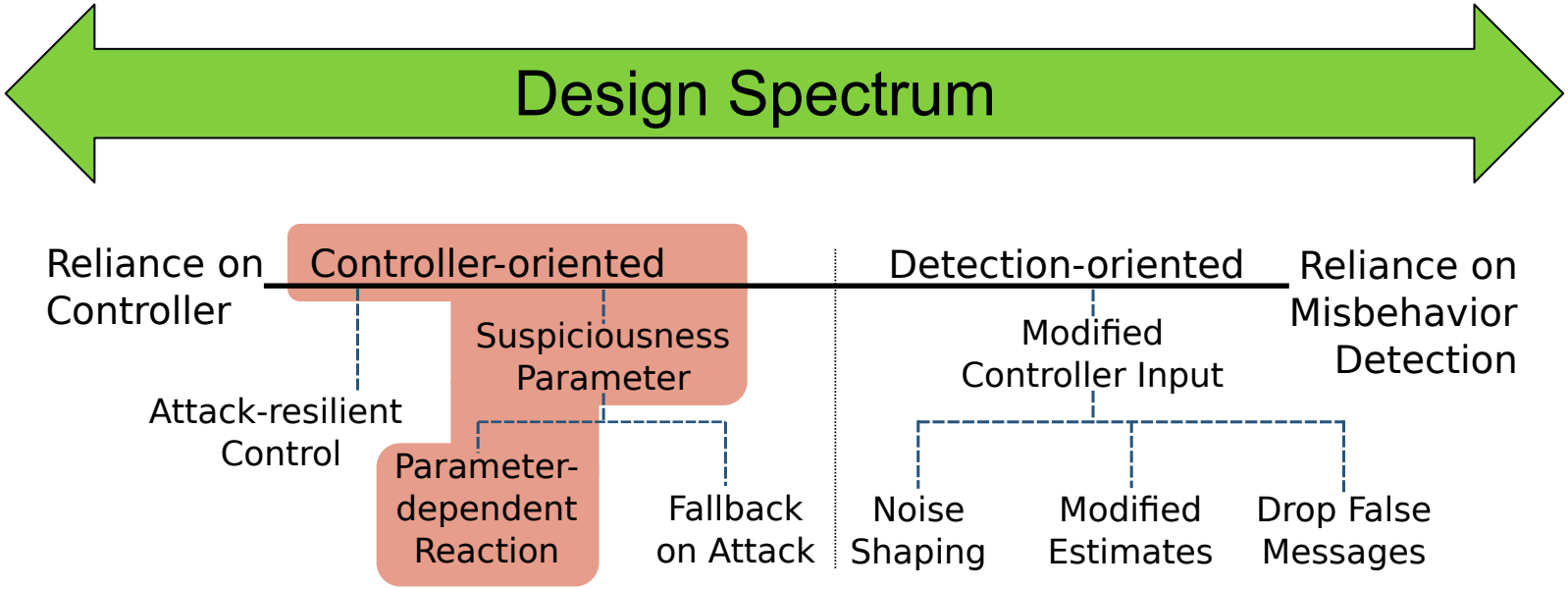
2020 IEEE Vehicular Networking Conference (VNC) | 978-1-7281-9221-5/20/$31.00 ©2020 IEEE | DOI: 10.1109/VNC51378.2020.9318396

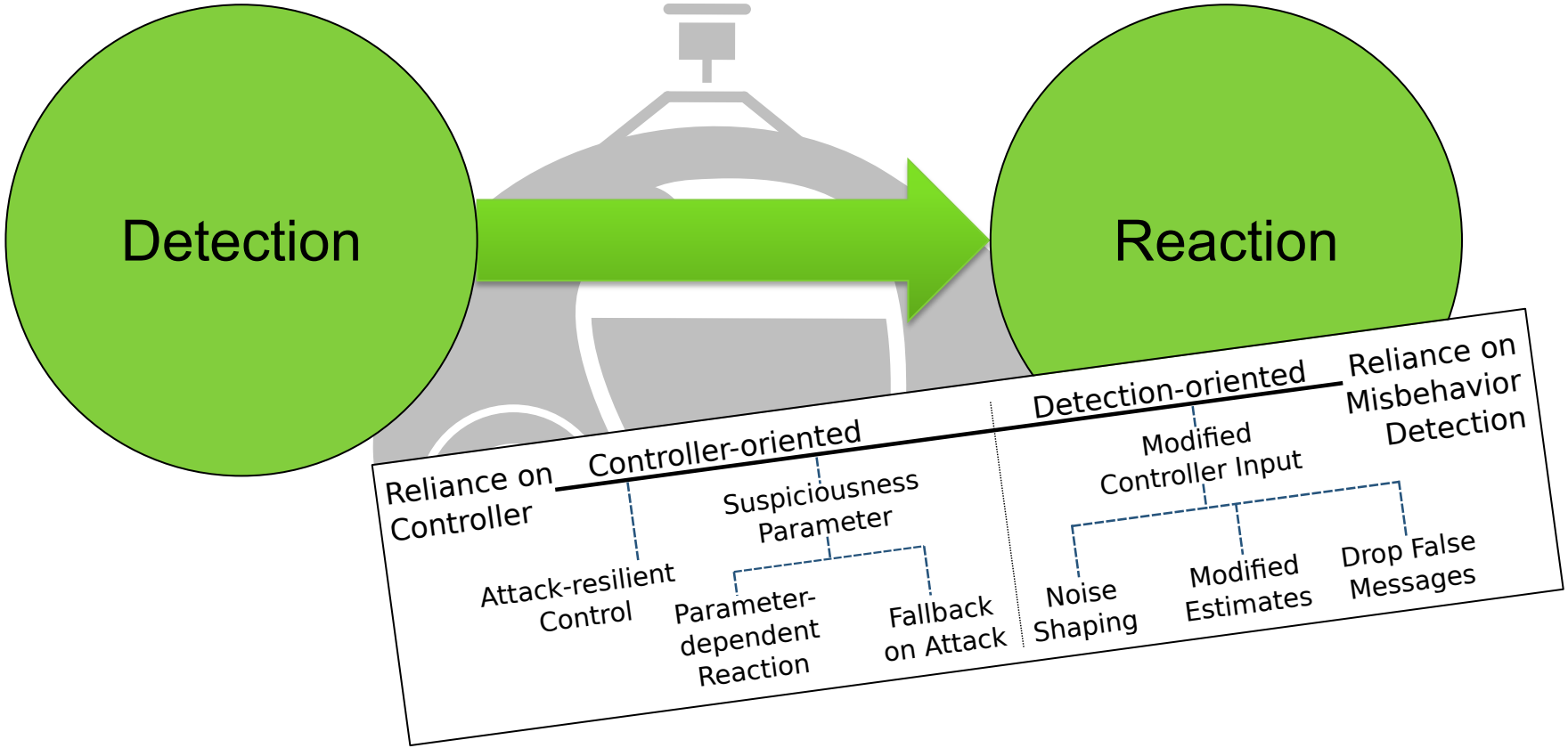
978-1-7281-9221-5/20/$31.00 ©2020 IEEE

Misbehavior Detection

Securing CACC: Strategies for Mitigating Data Injection Attacks, IEEE Vehicular Networking Conference (VNC) 2020


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



Google Car Created by James Mayle from the Noun Project

SecForCARs
security for connected automated cars

I am looking forward to the discussion in the breakout-session

Google Car Created by James Mayle from the Noun Project