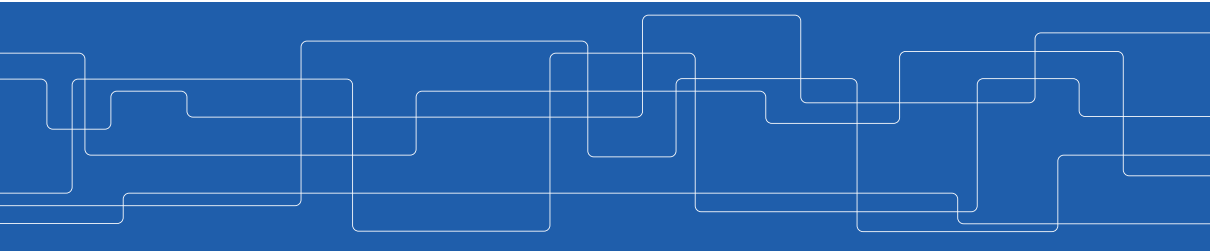
IEEE EuroS&P ACSW 2023

Vulnerability Analysis of Vehicular Coordinated Maneuvers

Konstantinos Kalogiannis,
Andreas Henriksson and Panos Papadimitratos
Networked Systems Security (NSS) group, www.eecs.kth.se/nss

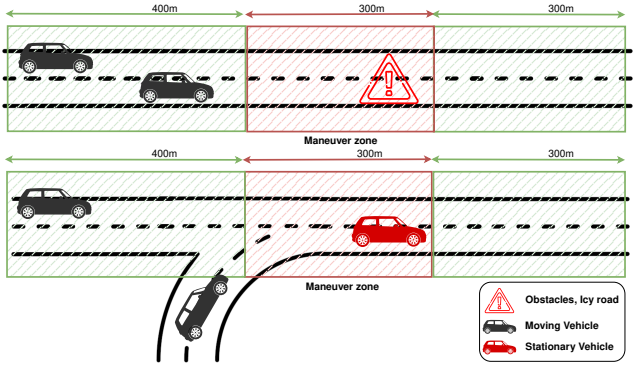


Overview

- Background
  - Maneuver Coordination Service (MCS)
  - Current Approaches
  - Protocols
- Setup
- Analysis
  - Collision Impact
  - Safety
  - Time Impact
  - Road Denial
  - Takeaway

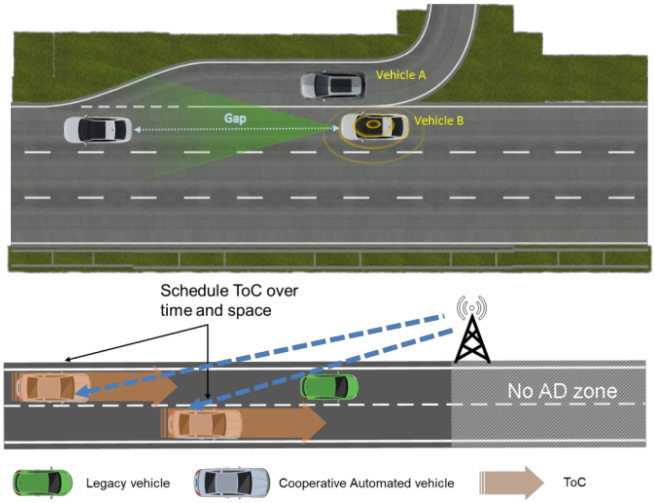
Background: Maneuver Coordination Service

- Why?
  - Safety
  - Traffic Management
- How?
  - Maneuver Coordination Messagess (MCMs)
- Where?
  - Transition Areas



Background: Current Approaches

- No universal "right way"
- Infrastructure assist?
- Trajectories or Perception?



Source: C2C Communication Consortium

Background: Protocols

- Common principles
  - Reserve Area
  - Send Trajectory
  - Receive "accept"
- Differences
  - Intervals
  - Conflict Detection
  - Response

Principle	Serial MCP[a]	STRP[b]	AutoMCM[c]	Opel Core[d]
Trajectory Structure	Frenet Frame	Reservation shape	Position in time	Gap in time
Transmission Frequency	Fixed interval	When needed	When needed	Fixed interval
Conflicts Detection	Check planned	Check vehicles' motion	Check planned	Check planned
Trajectory request	Attach desired	Send reservation shape	Scenario Advertisement	Send desired
Maneuver Acceptance	Send new planned	Send boolean commit	Send boolean message	Send new planned

[a] LehmannGW2018C: A generic approach towards maneuver coordination for automated vehicles

[b] NichtingHS2020C: Space time reservation procedure for v2x-based maneuver coordination of cooperative automated vehicles in diverse conflict scenarios

[c] MizutaniTE2021C: Automcm: Maneuver coordination service with abstracted functions for autonomous driving

[d] LizenbergBHEKK2021S: Simulation-based evaluation of cooperative maneuver coordination and its impact on traffic quality

Background: Protocols

- Common principles
  - Reserve Area
  - Send Trajectory
  - Receive “accept”
- Differences
  - Intervals
  - Conflict Detection
  - Response

Principle	Serial MCP[a]	STRP[b]	AutoMCM[c]	Opel Core[d]
Trajectory Structure	Frenet Frame	Reservation shape	Position in time	Gap in time
Transmission Frequency	Fixed interval	When needed	When needed	Fixed interval
Conflicts Detection	Check planned	Check vehicles' motion	Check planned	Check planned
Trajectory request	Attach desired	Send reservation shape	Scenario Advertisement	Send desired
Maneuver Acceptance	Send new planned	Send boolean commit	Send boolean message	Send new planned

[a] LehmannGW2018C: A generic approach towards maneuver coordination for automated vehicles

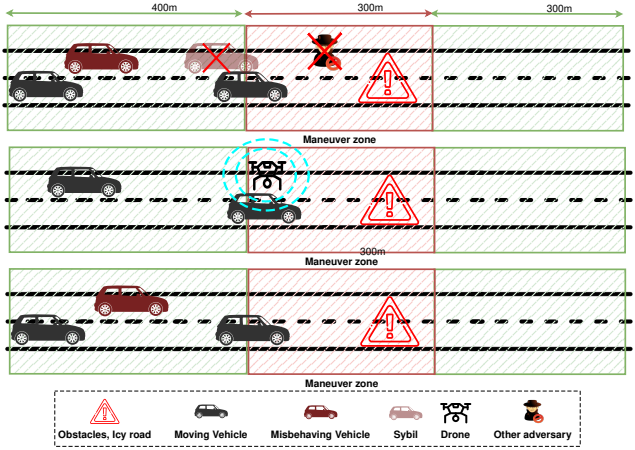
[b] NichtingHS2020C: Space time reservation procedure for v2x-based maneuver coordination of cooperative automated vehicles in diverse conflict scenarios

[c] MizutaniTE2021C: Automcm: Maneuver coordination service with abstracted functions for autonomous driving

[d] LizenbergBHEKK2021S: Simulation-based evaluation of cooperative maneuver coordination and its impact on traffic quality

Analysis: Adversary Model

- Secure & non-overlapping cryptographic primitives
- External Jammer
- Internal Attacker
- Rational Attacker
  - Self-preservation
  - Physical presence



Analysis: Setup

- Tools
  - SUMO
  - OMNeT++
  - Veins
- Scenarios
  - Sensor errors
  - Different lane speeds
  - Cost function
  - Vehicle spacing

Parameters	Value
Right lane	12.5, 25 m/s
Left lane (for right: 12.5)	16.5, 20.5, 24.5, 28.5, 32.5 m/s
Left lane (for right: 25)	29, 33, 37, 41 m/s
Sensor range	30 (backward) and 250 (forward) m
MCM Frequency	5 Hz
Spacing	10, 30, 50 m
Sensors	$\epsilon_p^{V2V} = 1m$, $\epsilon_s^{V2V} = 0.1m/s$, $\epsilon_a^{V2V} = 0.01m/s^2$, $\epsilon_p^{RAD} = 0.1m$, $\epsilon_s^{RAD} = 0.1m/s$
Car-following model	ACC
Cost Weights (V; A; Brakes)	1, 1, 0.5

Analysis: Setup (cont)

- Cost function
  $C_{\text{speed}} = w_{i1} \cdot (u_0(t) - u_{ref}(t))^2$
  $C_{\text{acc}} = w_2 \cdot a(t)^2$
  $C_{\text{total}} = C_{\text{speed}} + C_{\text{acc}}$

- Vehicle Insertion
  $t_l = t_r + \frac{l_R}{u_r} - \frac{l_R - spacing - l_v}{u_l}$

- w_{i1}: non-negative penalty for speed,
  u_0: current speed at time t,
  u_{ref}:new required speed for the maneuver.

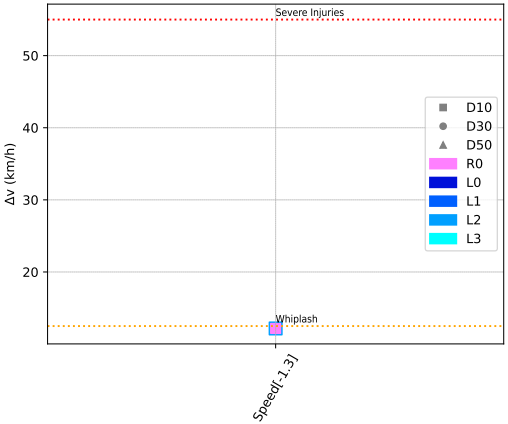
- t_l, t_r: insertion times for left/right lane
  l_R, l_v: length of initial road, length of the vehicle
  u_r, u_l: speeds for right/left lane
  spacing: distance between left/right lane vehicles

Analysis: Attack Setup

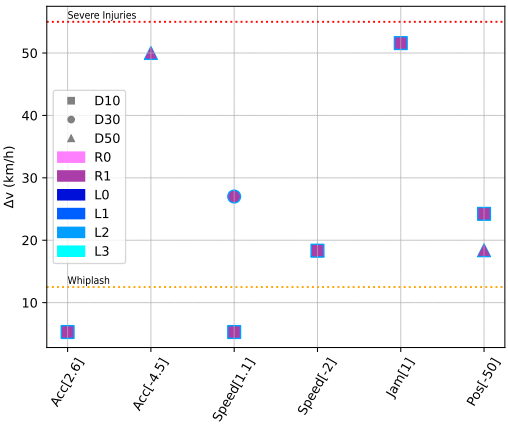
- Left lane attacker
- Falsification
  - Relative values
- Jamming
  - Targeted
  - Selective

Parameters	Value
Falsification Attacker	$L0$
Targeted Jamming	R_0
Selective Jamming / drop rate	0, 25, 50, 75 %
Position Attack (m)	10, -10, -30, -50, -100
Speed Attack (m/s)	1.1, 1.2, 1.3, 1.4, 1.5, 2
Acceleration Attack (m/s^2)	2.6, -4.5

Analysis: Collision Impact



(a) Single Maneuvering Vehicle



(b) Two Maneuvering Vehicles

Collision Impact: Moving at 25(R)/33(L) m/s.

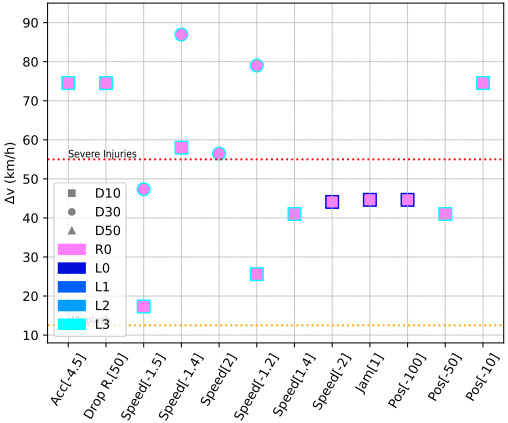
Analysis: Safety

- Multiple vehicles increase the potential for safety violations
- Sensors can be effective
- Position & Speed are critical

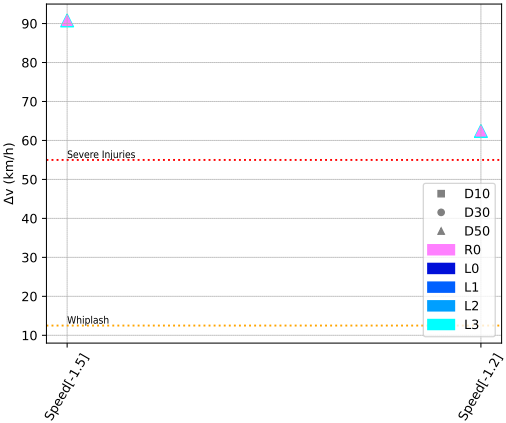
Safety violations due to misbehavior

Sensors	Maneuv. Vehicles	Jamming	Stealth Jamming	Position	Speed	Acceleration	Total
No	1	85%	69%	74%	78%	47%	74%
	2	96%	86%	90%	86%	92%	84%
Yes	1	48%	34%	17%	31%	25%	28%
	2	74%	53%	26%	48%	44%	43%

Analysis: Collision Impact with Sensors



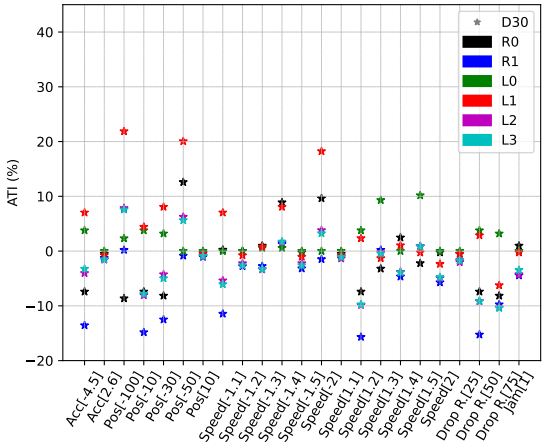
(a) No Sensor Usage

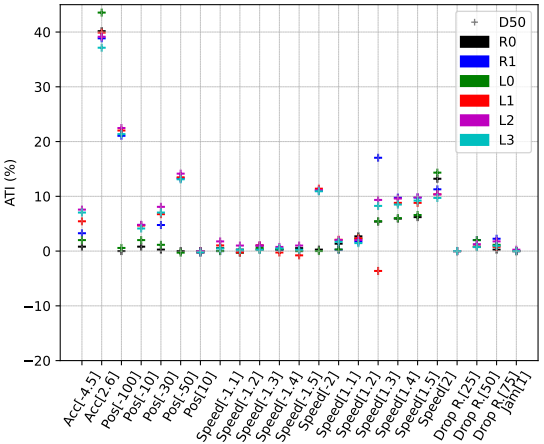


(b) Sensor Usage

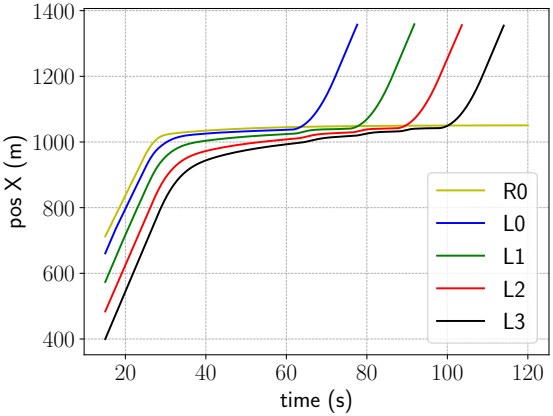
Collision Impact: Sensor Effectiveness at $25(R)/41(L)$ m/s.

Analysis: Attacks' Time Impact (ATI)

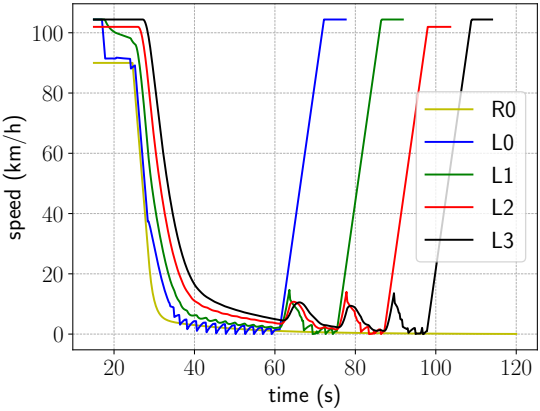




Analysis: Road Denial



(e) Vehicles Position



(f) Vehicles speed

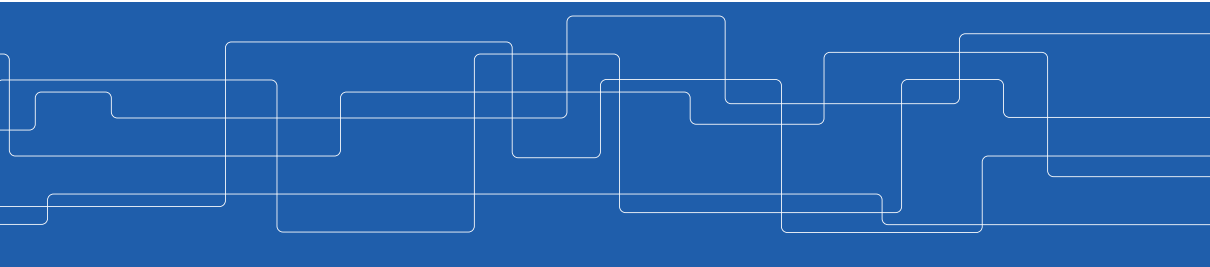
Analysis: Takeaways

- Mitigation Steps
  - Sensors
  - Misbehavior Detection
- Delayed maneuvers pose a safety threat
- Speed information is crucial
- Physical verification of maneuver
  - Not solved by cost functions

IEEE EuroS&P ACSW 2023

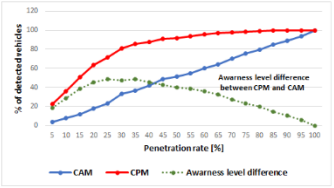
Vulnerability Analysis of Vehicular Coordinated Maneuvers

Konstantinos Kalogiannis,
Andreas Henriksson and Panos Papadimitratos
Networked Systems Security (NSS) group, www.eecs.kth.se/nss



Appendix - Related Work - Investigated

- RSU-assisted
  - Speed, Sybil Attacks
  - Fake object, Sensor blindness
- Macro-analysis
  - Attacker Model
  - Reproducibility, Impact, Stealthiness

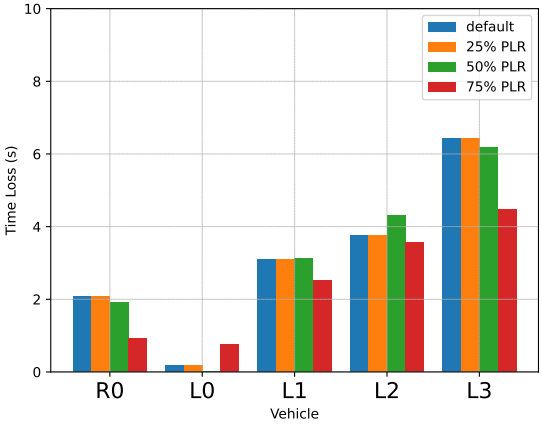


(g) Security attacks impact for collective perception based roadside assistance: A study of a highway on-ramp merging case

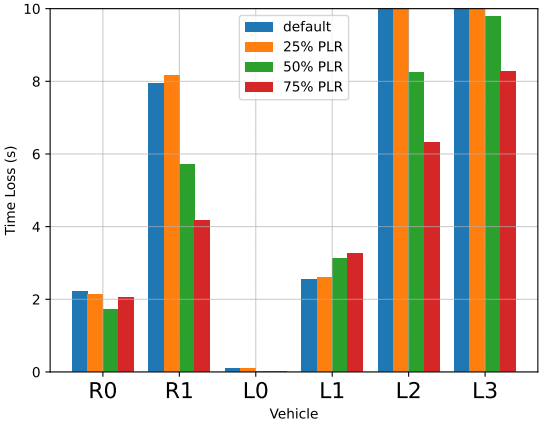
The attacker inserts an incorrect value in the MSCM-request	Set the *maximum speed* with a value way above speed limit (e.g., 200 km/h > 130 km/h)	The *maximum speed* is way above the average speed of surrounding vehicles or the speed limit displayed by the map or perceived by the camera.	**Overall: *High*.** • ***(High)* Reproducibility:** An attacker inserts a malicious value to the field *maximum speed* • ***(High)* Impact:** Maneuvering vehicles maneuver way above the speed limit (safety risk). • ***(Low)* Stealthiness:** speed value way above the maximal speed limit (implausible value).
	Attacker request a maneuver on a nonexistent lane by setting an incorrect *LaneOffset*	Check the number of lanes displayed by the map or perceived by the camera.	**Overall: *Medium*.** • ***(High)* Reproducibility:** An attacker inserts a malicious value to the field *LaneOffset* (located in the container *TRR Location*) • ***(Medium)* Impact:** Set the vehicle off the road (safety risk). • ***(Low)* Stealthiness:** An attacker is detectable through its certificate in the MSCM.

(h) V2X Misbehavior in Maneuver Sharing and Coordination Service: Considerations for Standardization

Trip Impact



(i) Single Maneuvering Vehicle



(j) Two Maneuvering Vehicle

Appendix - Future Work

- Setup
  - Generalized scenarios
  - Intersections
  - Penetration rates
- Attacks
  - Gradual & Combined
  - Collusion
- Misbehavior Detection