Investigating Attacks on Vehicular Platooning and Cooperative Adaptive Cruise Control (CACC)

Konstantinos Kalogiannis
Supervisor: Mohammad Khodaei
Examiner: Panos Papadimitratos
Networked Systems Security (NSS) Group
KTH Royal Institute of Technology

ITS

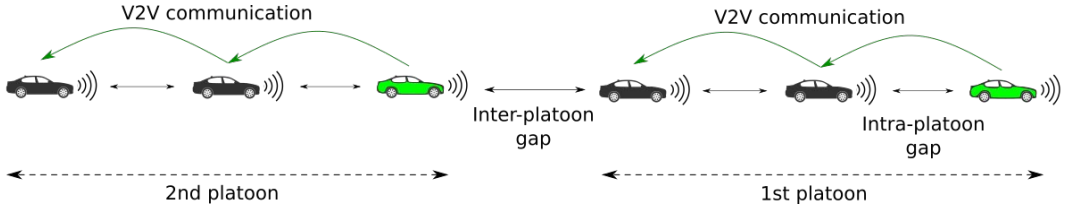
- Components
  - Vehicles
  - Road Side Units
  - Service Centers

- Cooperative Awareness Message (CAM)
  vs
  Decentralized Environmental Notification Message (DENM)
  - DIfferent dissemination frequencies
  - Different goals

- Applications[1,2]
  - Road safety
  - Traffic efficiency

Platooning

- Properties
  - Intra-platoon gaps
  - Inter-platoon gaps
  - Platoon size



- Vehicular Public Key Infrastructure[3]
  - Beacon validation
  - Identity management

- CACC controllers
  - Constant Vehicle Spacing
  - Constant Headway Time

Radar Measurements: R V2V Communication: Top precedence:

Controller	Policy	Predecessor			Leader			Topology
		d	s	a	p	s	a	
ACC	CTH	R	R					-
PATH	CVS	R	R					PL Following
Consensus	Both	R						PL Following
Flatbed	CVS	R	R					PL Following
Ploeg	CTH	R	R					Predecessor Following

Problem Statement

Investigating attacks on vehicular platooning and its maneuvering capabilities with the goal of decreasing its efficiency and degrading the formation stability.

- What is the effect of falsification attacks when perpetrated during a maneuver?
- How is the platoon's stability affected by attacks originating from within, regardless of position?
- What is the severity of the attacks' induced collisions?
- Can misbehavior detection function in such a scenario?

Novelty

- Attacks during platoon maneuvering
  - Middle-Join
  - Exit
- Systematic review of attacks
  - Combined kinematic properties - positive and negative injections
  - Different platoon speeds - all positions
- Evaluation of Flatbed
  - Jamming
  - Falsification attacks

Contributions

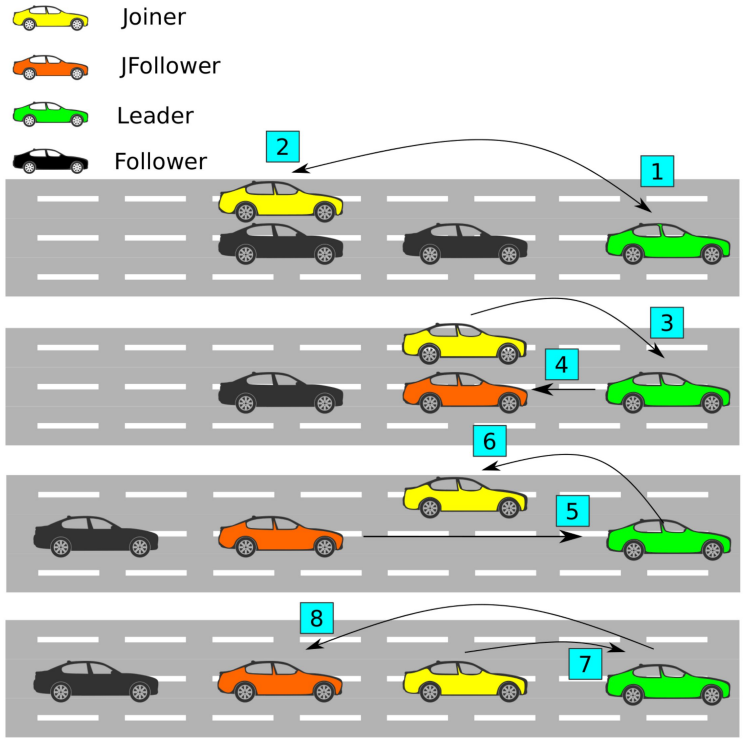
- Maneuvers
  - Support all controllers in a Join
  - Support dynamic positioning in a Join
  - Faster Exit

- Unified Attack Framework
  - Attacker(s) position
  - Attack type and payload
  - Maneuvering

- Tools Used
  - Plexe-Veins[6]: Platoon network simulator
  - OMNeT++[8]: Event Simulation Framework
  - SUMO[7]: Urban Mobility Simulator

Join Protocol

A. Approach (1-2-3)
   a. Join index
   b. Reach position
B. Increase Gaps (4-5-6)
   a. Increase policy margins (JFollower)
   b. Maintain position(Joiner)
      i. Threshold
      ii. Abort
C. Join Formation (6-7-8)
   a. Change lane
   b. Update formation
   c. Update policy margins



System Model

- Assumptions
  - Same vehicle characteristics (engine, brakes, car length)
  - All vehicles have valid pseudonyms
  - Cars on the road know the platoon leader

- Adversary Model
  - Internal member or Leader Attacker
  - Only CAM and DENM falsifications allowed
  - Collusion between misbehaving vehicles

Attacks

- Simple attacks
  - Replace nominal value with a malicious one
  - Always falsified with the same value
  - Position, Speed, Acceleration
- Gradual attacks
  - Relative values
  - Increase by step
  - Limit range of values
- Smart attacks
  - Relative values - increase by step
  - Falsify one property - relate the rest based on kinematic equations
  - Stricter limits
- Jamming attack
  - Drop all packets

Simulation setup

Configuration	Attack Values	Attack Position	Maneuver
JammingDetail	[30-35] s	1	[no,Join,Exit]
PosInjectionAttack	[3, 5, 7, 9, 11] m	[0,2]	[no,Join,Exit]
SpeedInjectionAttack	[-50, 0, 50, 100, 150] km/h	[0,2]	[no,Join,Exit]
AccInjectionAttack	[-30, -10, 0, 10, 30] m/s^2	[0,2]	[no,Join,Exit]
GradualPosFalsificationAttack	[-10,40] m	[0,2]	[no,Join,Exit]
GradualSpeedFalsificationAttack	[-10,17] m/s	[0,2]	[no,Join,Exit]
GradualAccFalsificationAttack	[-10,10] m/s^2	[0,2]	[no,Join,Exit]
SmartPosFalsificationAttack	[-10,10] m	[0,2]	[no,Join,Exit]
SmartSpeedFalsificationAttack	[-10,10] m/s	[0,2]	[no,Join,Exit]
SmartAccFalsificationAttack	[-10,10] m/s^2	[0,2]	[no,Join,Exit]

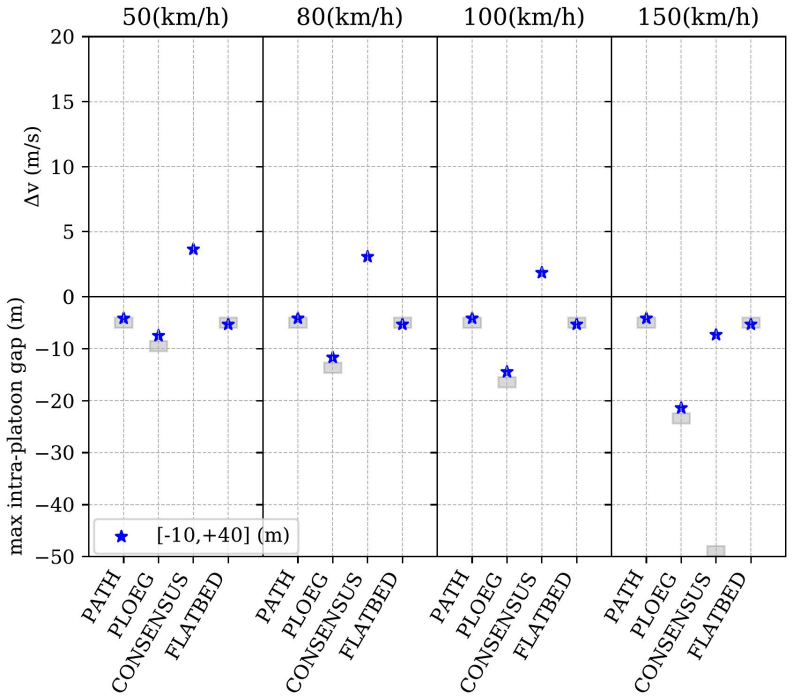
Property	Value
Controller	PATH, Ploeg, Consensus, Flatbed
Spacing	5m, 0.5s, 0.8s, 5m
Platoon Length	6 / 7 (Join)
Leader speed	50, 80, 100, 150 kmph
Sensors	ϵ_p^{V2V} = 1 m, ϵ_s^{V2V} = 0.1 m/s, ϵ_a^{V2V} = 0.01 m/s^2 ϵ_p^{RAD} = 0.1 m, ϵ_s^{RAD} = 0.1 m/s

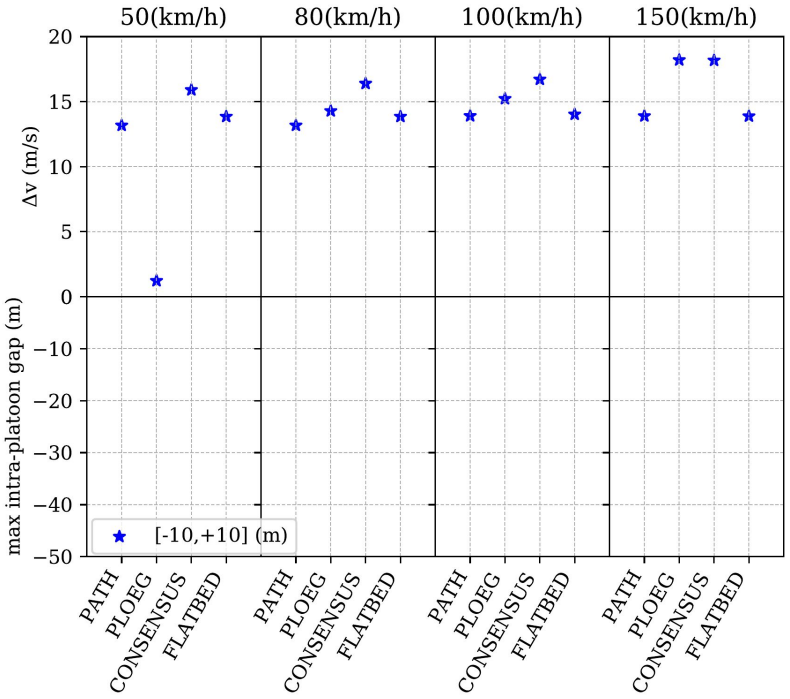
General Parameters	Value
Simulation length	120s
Warm-Up period	30s
Area Size	5 KM x 50 M (4 lanes)
Repetitions	10
Carrier Frequency	5.89 GHz
Max TX Power	100mW
Physical Layer Bitrate	6Mbps
Sensitivity	-94dBm
Thermal Noise	-95dBm
Physical Layer Propagation Delay	true
Network Layer Propagation Delay	true

Metrics

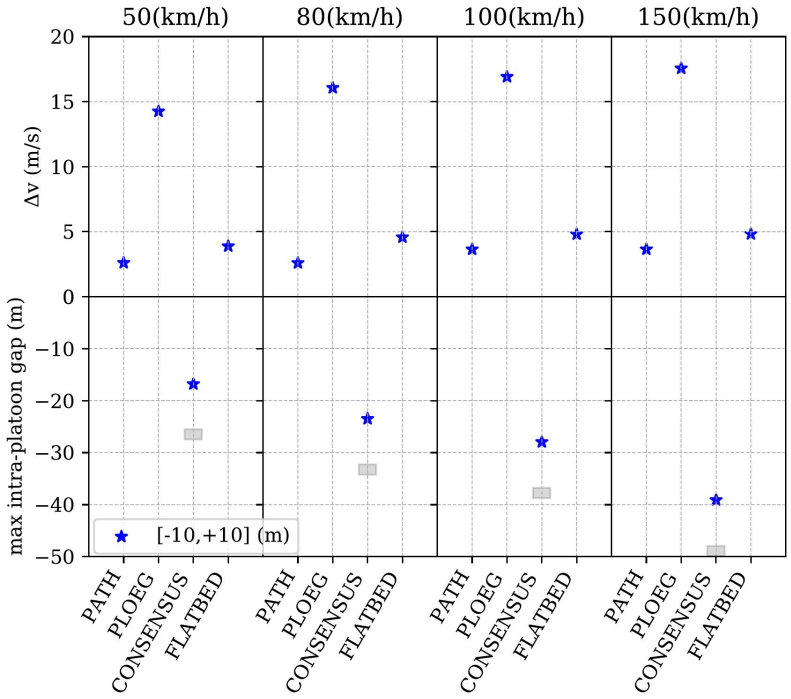
- Controllers behavior
  - Distance between each vehicle
  - Speed, Acceleration, Controller Acceleration, Position
- Platoon instability
  - Nominal gaps
  - Maximum error distance from nominal gaps
- Collision Severity
  - ΔV between colliding cars

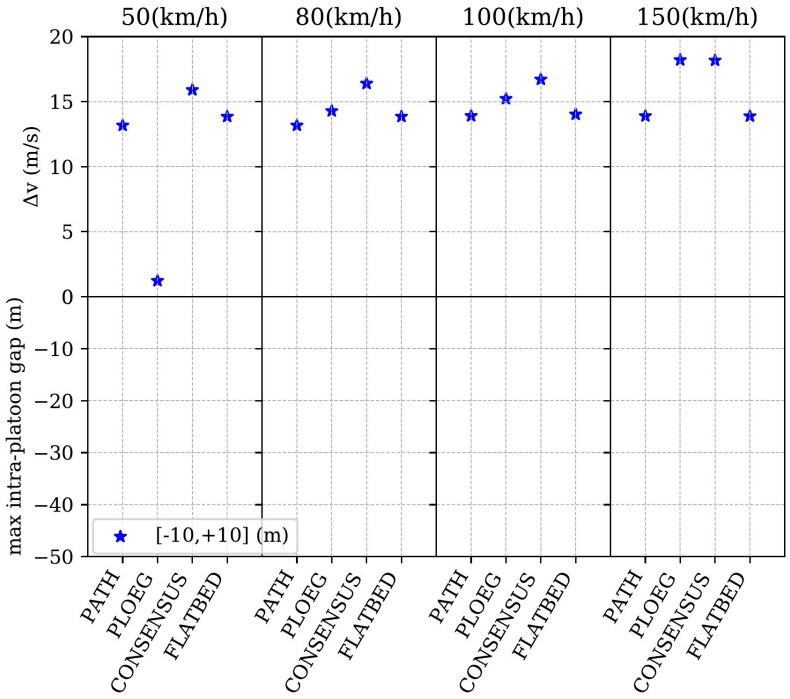
Gradual vs Smart Pos Leader Attack



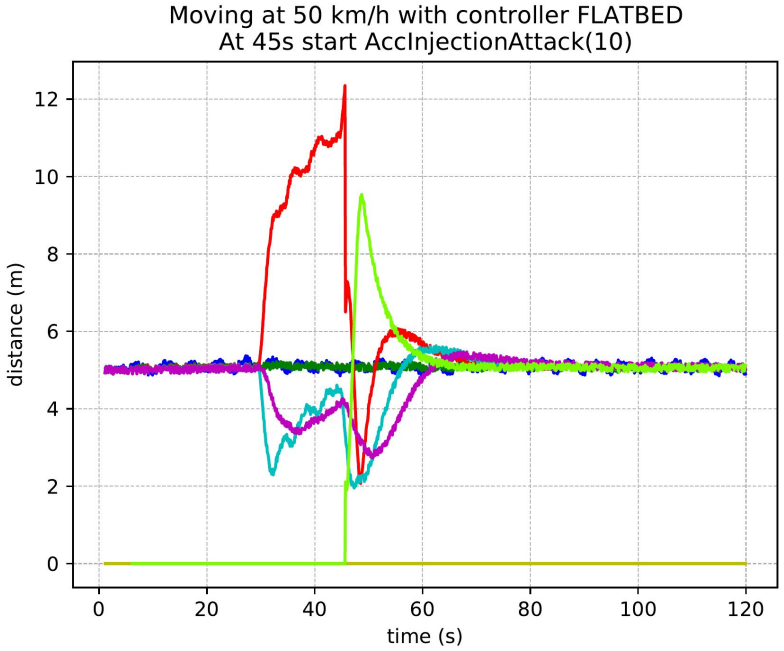


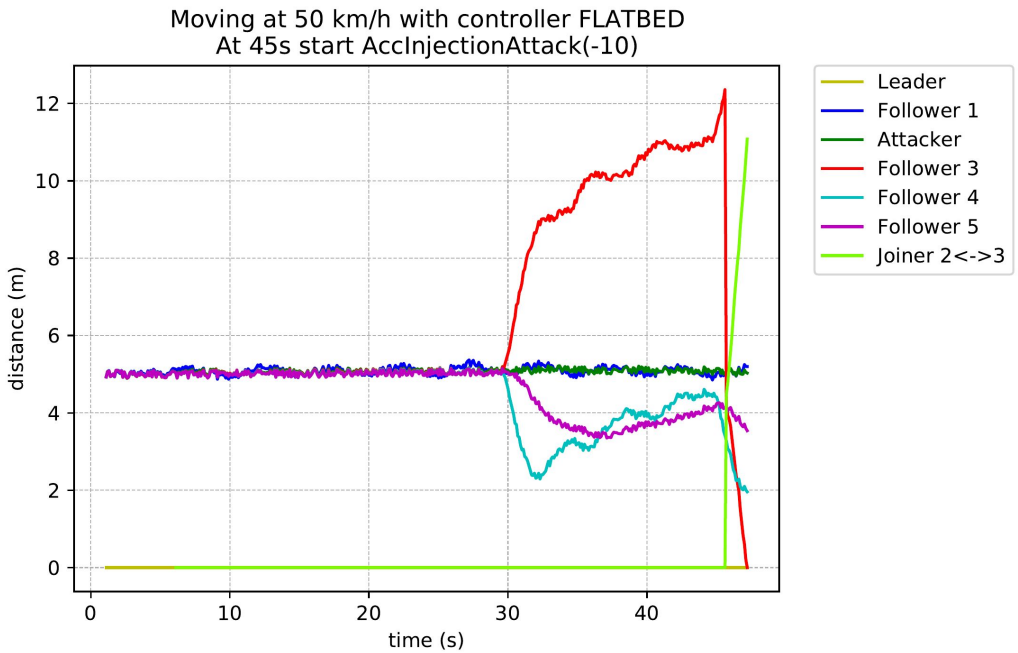
Smart Pos: Follower vs Leader





Acceleration Attack - Flatbed Join





Hitmap

Attack		No Maneuver				Join Maneuver				Exit Maneuver			
		50 (km/h)	80 (km/h)	100 (km/h)	150 (km/h)	50 (km/h)	80 (km/h)	100 (km/h)	150 (km/h)	50 (km/h)	80 (km/h)	100 (km/h)	150 (km/h)
Position (m)	PATH	-	-	-	-	-	-	-	-	-	-	-	-
	Consensus	LF {3,5,7,9,11}	LF {3,5,7,9,11}	LF {3,5,7,9,11}	LF {3,5,7,9,11}	{3,5,7,9,11}	{3,5,7,9,11}	{3,5,7,9,11}	{3,5,7,9,11}	{3,5,7,9,11}	{3,5,7,9,11}	{3,5,7,9,11}	{3,5,7,9,11}
	Flatbed	-	-	-	-	-	-	-	-	-	-	-	-
	Ploeg	-	-	-	-	-	-	-	-	-	-	-	-
Speed (km/h)	PATH	LF {-50,0}	LF {-50,0} F +50	LF {-50,0,50}	LF {-50,0,50,100}	{-50,0}	{-50,0,50}	{-50,0,50}	{-50,0,50,100}	{-50,0}	{-50,0,50}	{-50,0,50}	{-50,0,50,100}
	Consensus	L {100,150}	L 150	L 150	-	-	-	-	-	-	-	-	-
	Flatbed	L {100,150}	L {100,150}	L 150	-	{-50,0}	{-50,0}	{-50,0}	{-50,0,50,100}	-	-	-	-
	Ploeg	-	-	-	-	-	-	-	-	-	-	-	-
Acceleration (m/s^2)	PATH	F {-30,-10}	F {-30,-10}	F {-30, -10}	F {-30, -10}	{-30,-10}	{-30,-10}	{-30,-10}	{-30,-10}	{-30,-10}	{-30,-10}	{-30,-10}	{-30,-10}
	Consensus	-	-	-	-	-	-	-	-	-	-	-	-
	Flatbed	-	-	-	-	-	-	-	-	-	-	-	-
	Ploeg	LF {-10,-30}	LF -30	LF -30	LF -30	-30	-30	-30	{10,30}	-30	-30	-30	{10,30}
Gradual Position (m)	PATH	-	-	-	-	-	-	-	-	-	-	-	-
	Consensus	LF -10/+40	LF -10/+40	-	-	-10/+40	-10/+40	-	-	-10/+40	-10/+40	-	-
	Flatbed	-	-	-	-	-	-	-	-	-	-	-	-
	Ploeg	-	-	-	-	-	-	-	-	-	-	-	-
Gradual Speed (m/s)	PATH	LF {-10/+17}	LF {-10/+17}	LF {-10/+17}	LF {-10/+17}	-10/+17	-10/+17	-10/+17	-10/+17	-10/+17	-10/+17	-10/+17	-10/+17
	Consensus	L -10/+17	L -10/+17	L -10/+17	L -10/+17	-	-	-	-	-	-	-	-
	Flatbed	L -10/+17	L -10/+17	L -10/+17	L -10/+17	-	-	-	-	-	-	-	-
	Ploeg	-	-	-	-	-	-	-	-	-	-	-	-
Gradual Acceleration (m/s^2)	PATH	F -10/+10	F -10/+10	F -10/+10	F -10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10
	Consensus	-	-	-	-	-	-	-	-	-	-	-	-
	Flatbed	-	-	-	-	-10/+10	-	-	-10/+10	-	-	-	-
	Ploeg	LF -10/+10	LF -10/+10	LF -10/+10	LF -10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10
Smart Position (m)	PATH	F* -10/+10	F* -10/+10	F* -10/+10	F* -10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10
	Consensus	L -10/+10	L -10/+10	L -10/+10	L -10/+10	-	-	-	-	-	-	-	-
	Flatbed	F -10/+10	F -10/+10	F -10/+10	F -10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10
	Ploeg	L -10/+10	LF -10/+10	-10/+10	LF -10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10
Smart Speed (m/s)	PATH	F -10/+10	F -10/+10	F -10/+10	F -10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10
	Consensus	L -10/+10	L -10/+10	-	-	-	-	-	-	-	-	-	-
	Flatbed	L -10/+10	L -10/+10	L -10/+10	L -10/+10	-10/+10	-	-	-	-	-	-	-
	Ploeg	LF -10/+10	LF -10/+10	L -10/+10	L -10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10
Smart Acceleration (m/s^2)	PATH	F -10/+10	F -10/+10	F -10/+10	F -10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10
	Consensus	-	-	-	-	-	-	-	-	-	-	-	-
	Flatbed	L -10/+10	L -10/+10	L -10/+10	L -10/+10	-	-	-	-	-	-	-	-
	Ploeg	LF -10/+10	LF -10/+10	LF -10/+10	LF -10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10	-10/+10

Remarks

- Controllers
  - Consensus - most resilient
  - CVS - susceptible to jamming during acceleration
- Attacks on Maneuvers
  - Exit: minimal differences
  - Join:
    - Denied entry
    - CVS susceptibility
- Attack potency comparison
  - Follower better than Leader - no maneuver scenarios
- Kalman Filter
  - Detects Attacks
  - 100% False positives during maneuvering

Future Work

- Maneuvers
  - Security & Privacy of current maneuvers?
  - Susceptible to smarter attacks?
    - Selective jamming
    - False controller dissemination
- Colluding attackers
  - Easier/Harder to detect?
  - Leader + Follower? Two middle-formation leavers?
- Defense mechanisms
  - Misbehavior detection models?
  - Can they detect all the attacks?
  - Actual cost (cpu) of deploying them?
- Evaluate more realistic scenarios
  - Different lengths, engine capabilities

References

1. T. ETSI, “Intelligent transport systems (its); vehicular communications;basic set of applications; definitions,” Tech. Rep., 6 2009.
2. P. Papadimitratos, A. D. La Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza, “Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation,” IEEE Communications Magazine, vol. 47, no. 11, pp. 84–95, November 2009. doi: 10.1109/MCOM.2009.5307471.
3. M. Khodaei, H. Jin, and P. Papadimitratos, “Secmace: Scalable and robust identity and credential management infrastructure in vehicular communication systems,” IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 5, pp. 1430–1444, April 2018. doi: 10.1109/TITS.2017.2722688
4. R. van der Heijden, T. Lukaseder, and F. Kargl, “Analyzing attacks on cooperative adaptive cruise control (cacc),” in 2017 IEEE Vehicular Networking Conference (VNC), November 2017. doi: 10.1109/VNC.2017.8275598 pp. 45–52.
5. M. Iorio, F. Risso, R. Sisto, A. Buttiglieri, and M. Reineri, “Detecting injection attacks on cooperative adaptive cruise control,” in 2019 IEEE Vehicular Networking Conference (VNC), December 2019. doi: 10.1109/VNC48660.2019.9062798 pp. 1–8.
6. M. Segata, S. Joerer, B. Bloessl, C. Sommer, F. Dressler, and R. Lo Cigno, “PLEXE: A Platooning Extension for Veins,” in 6th IEEE Vehicular Networking Conference (VNC 2014). Paderborn, Germany: IEEE, 12 2014. Doi: 10.1109/VNC.2014.7013309. ISBN 978-1-4799-7660-7. ISSN 2157-9857 pp. 53–60.
7. P. A. Lopez, M. Behrisch, L. Bieker-Walz, J. Erdmann, Y. Flötteröd, R. Hilbrich, L. Lücken, J. Rummel, P. Wagner, and E. Wiessner,82 | REFERENCES “Microscopic traffic simulation using sumo,” in 2018 21st International Conference on Intelligent Transportation Systems (ITSC). IEEE, November 2018. doi: 10.1109/ITSC.2018.8569938 pp. 2575–2582.
8. A. Varga and R. Hornig, “An overview of the omnet++ simulation environment,” 01 2008. doi: 10.1145/1416222.1416290 p. 60.

Investigating Attacks on Vehicular Platooning and Cooperative Adaptive Cruise Control (CACC)

Konstantinos Kalogiannis
Supervisor: Mohammad Khodaei
Examiner: Panos Papadimitratos
Networked Systems Security (NSS) Group
KTH Royal Institute of Technology

Appendix

1. Controller Comparison
2. Jamming
3. Kalman Filter
4. Intelligent Attacks
    a. Gradual Acceleration
    b. Smart Acceleration + Details
    c. Gradual Speed
    d. Smart Speed + Details
5. Maneuvers
    a. Acceleration - Join
    b. Gradual Acceleration - Join
    c. Gradual Speed Denied Entry - Join
    d. Smart Speed - Join
    e. Smart Position - Join
    f. Smart Position - Exit
    g. Acceleration - Exit
    h. Without Abort Crashes
6. Speed

Controller Comparison

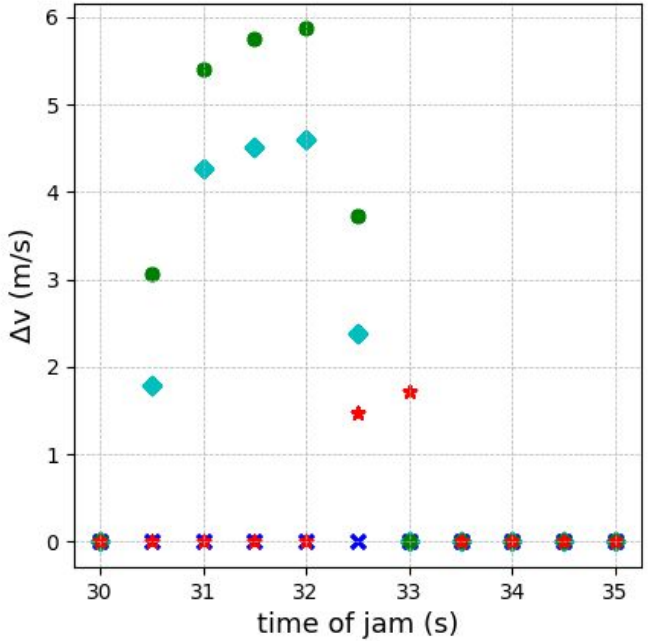
- Effective combined attacks
  - Ploeg - Acceleration
  - Consensus - Position
  - Flatbed - Speed
- Instability
  - Minimal difference Simple vs Gradual (1st table)
  - Consensus on combined attacks
- Crashes
  - Consensus is resilient
  - Ploeg always crashes

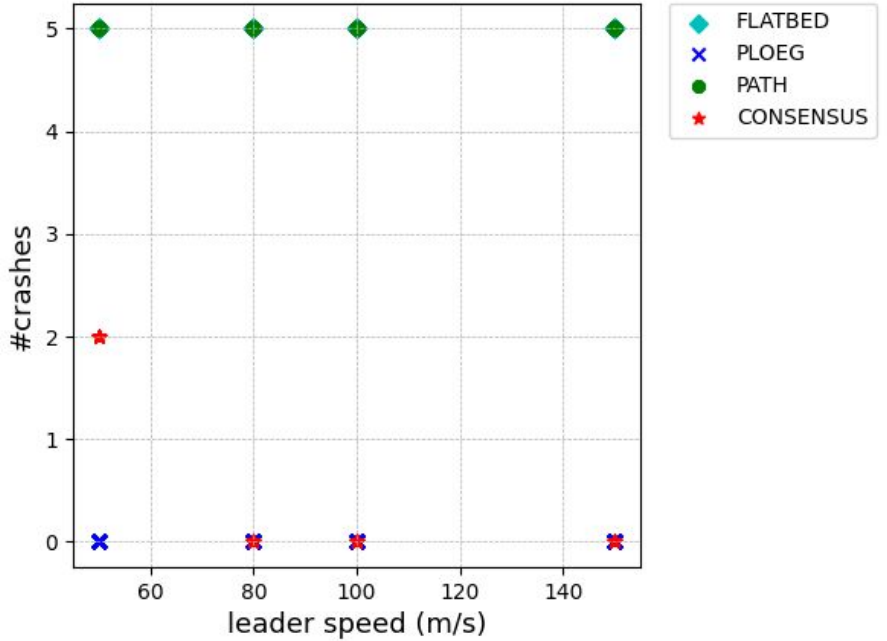
Controller	Simple			Gradual			Combined		
	P	S	A	P	S	A	P	S	A
PATH	100	—	20	100	—	—	—	—	—
Ploeg	100	100	20	100	100	—	—	—	—
Consensus	—	75	100	—	75	100	—	—	20
Flatbed	100	—	68.75	100	—	62.5	—	—	75

Controller	Simple			Gradual			Combined		
	P	S	A	P	S	A	P	S	A
PATH	—	1.47	10	—	—	—	—	—	—
Ploeg	—	—	20	—	—	—	—	—	—
Consensus	—	19.11	—	43.75	—	—	75	87.5	75
Flatbed	—	77.95	20	—	75	25	—	68.75	—

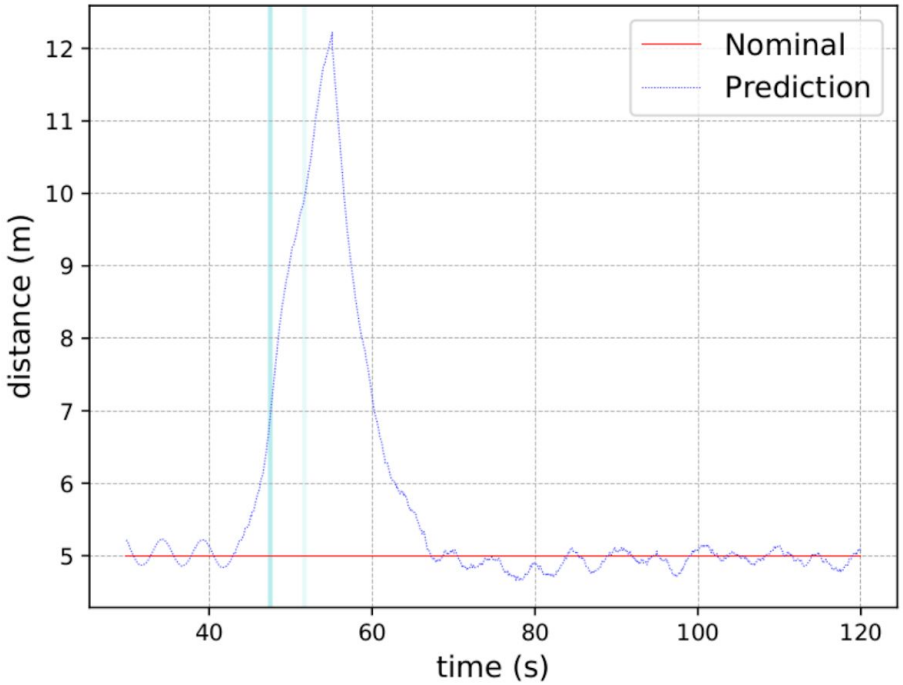
Controller	Simple			Gradual			Combined		
	P	S	A	P	S	A	P	S	A
PATH	—	98.53	70	—	100	100	100	100	100
Ploeg	—	—	60	—	—	100	100	100	100
Consensus	100	5.88	—	56.25	25	—	25	12.5	—
Flatbed	—	22.05	11.25	—	25	12.5	100	31.25	25

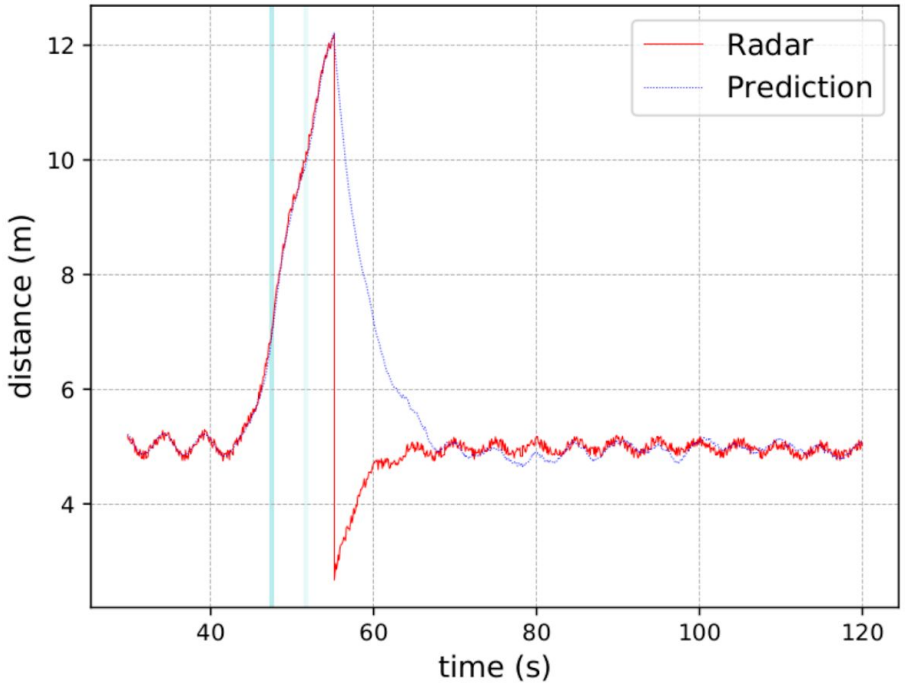
Jamming


Δv (m/s)
time of jam (s)
0
1
2
3
4
5
6
30
31
32
33
34
35


#crashes
leader speed (m/s)
0
1
2
3
4
5
60
80
100
120
140
FLATBED
PLOEG
PATH
CONSENSUS

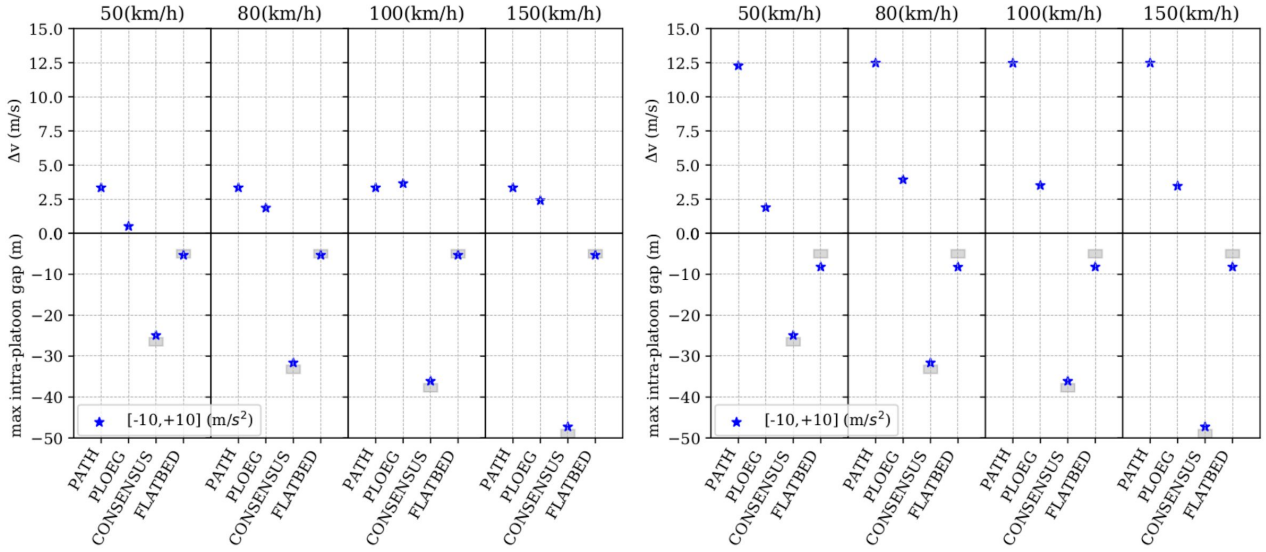
Kalman Filter Comparison: V2V - Radar





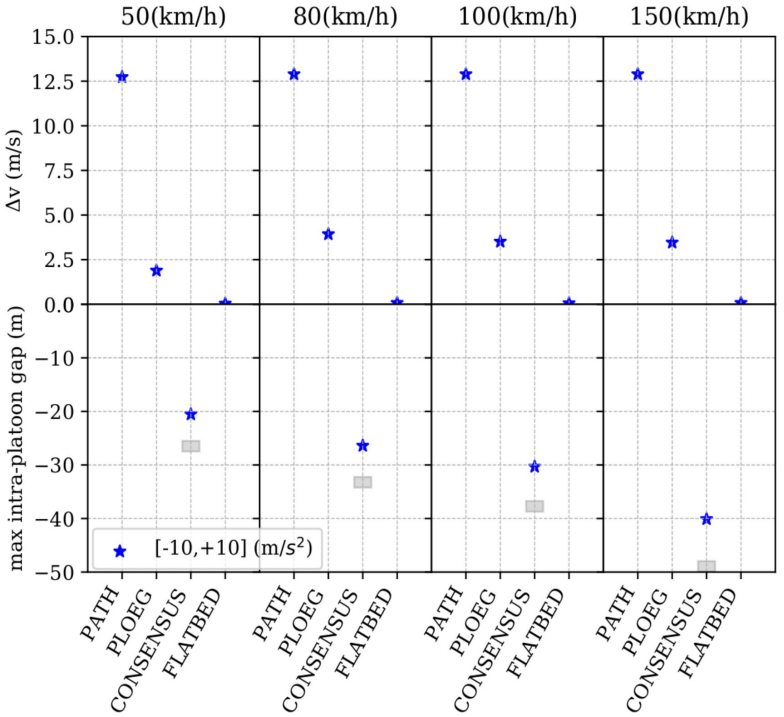
Gradual Acceleration: Follower vs Leader Attacker

- Rear vs Front Collision
  - PATH Follower is Better
  - Ploeg 50 km/h is Better

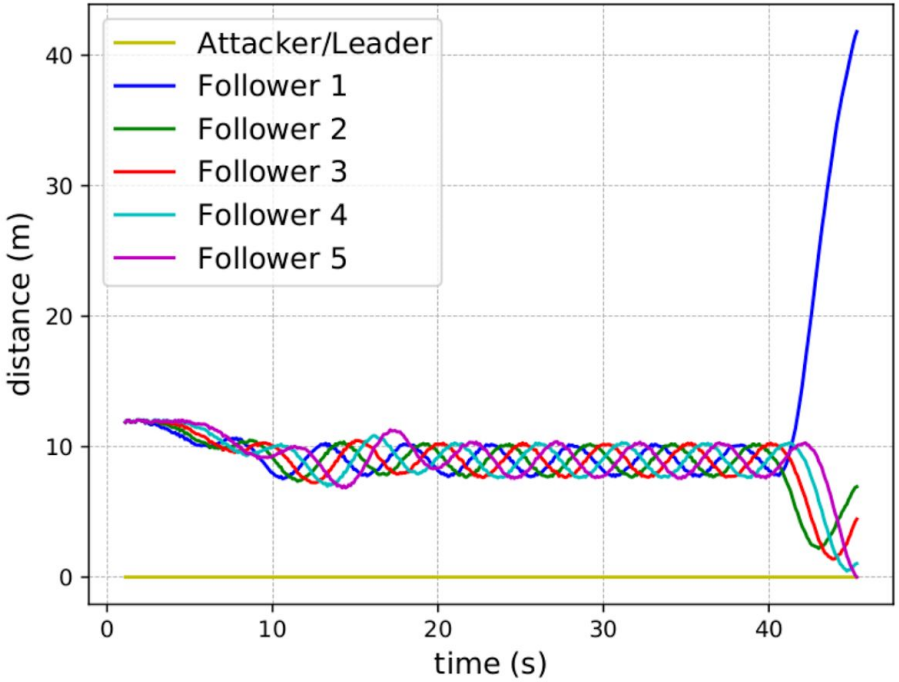


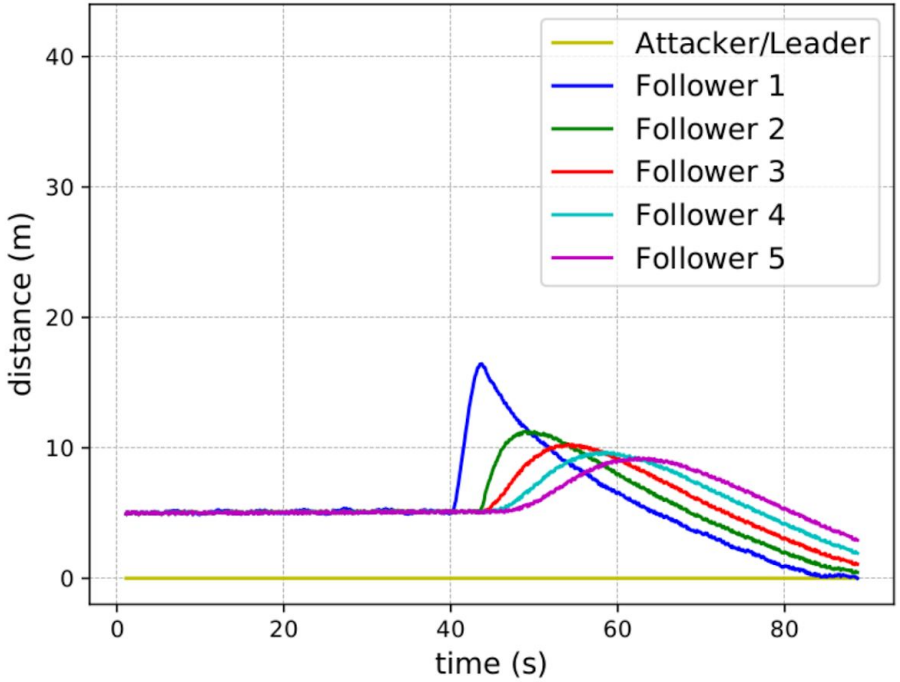
Leader Smart Acceleration

- Follower
  - Similar to Gradual Acceleration
- Leader
  - Flatbed closes the distance very slowly
  - Acceleration attack improves the least



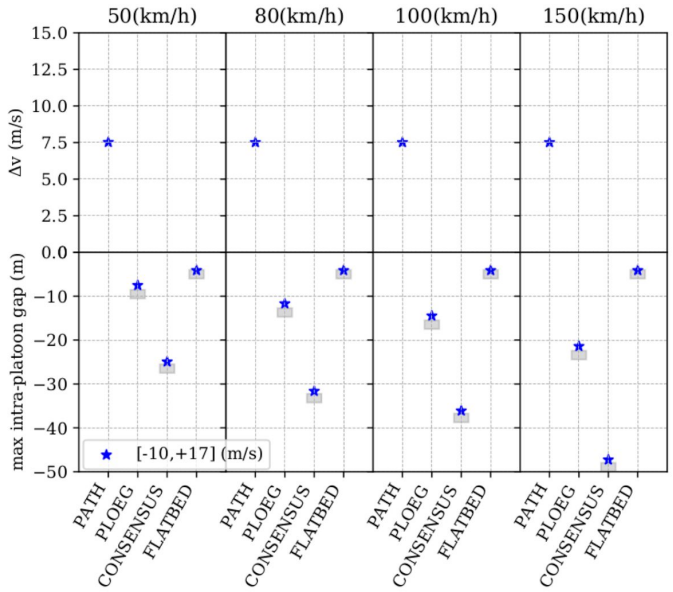
Smart Acceleration: Ploeg vs Flatbed

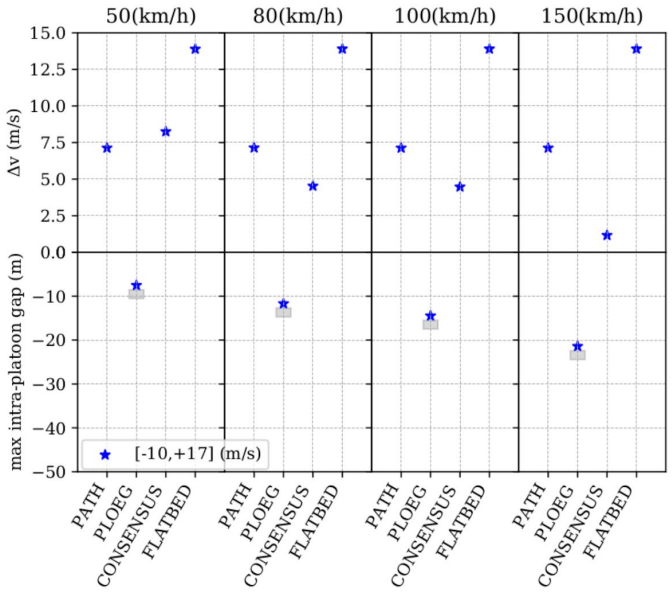




Gradual Speed: Follower vs Leader

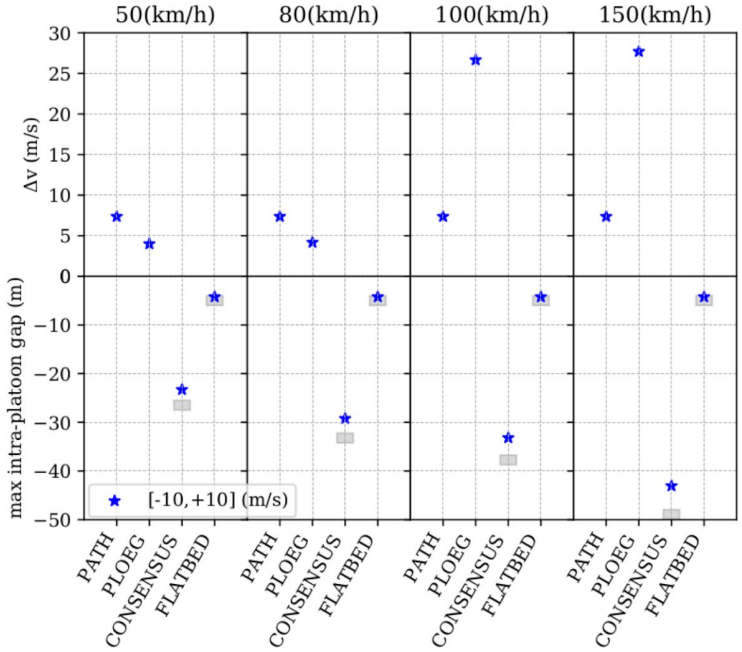
- Consensus
  - Increasingly Smaller difference between current speeds (thus gaps) and falsified speed

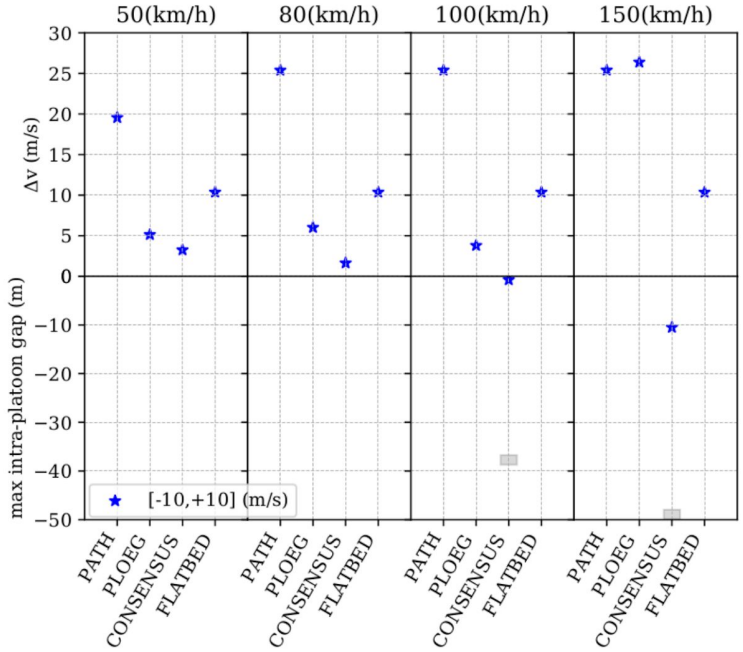




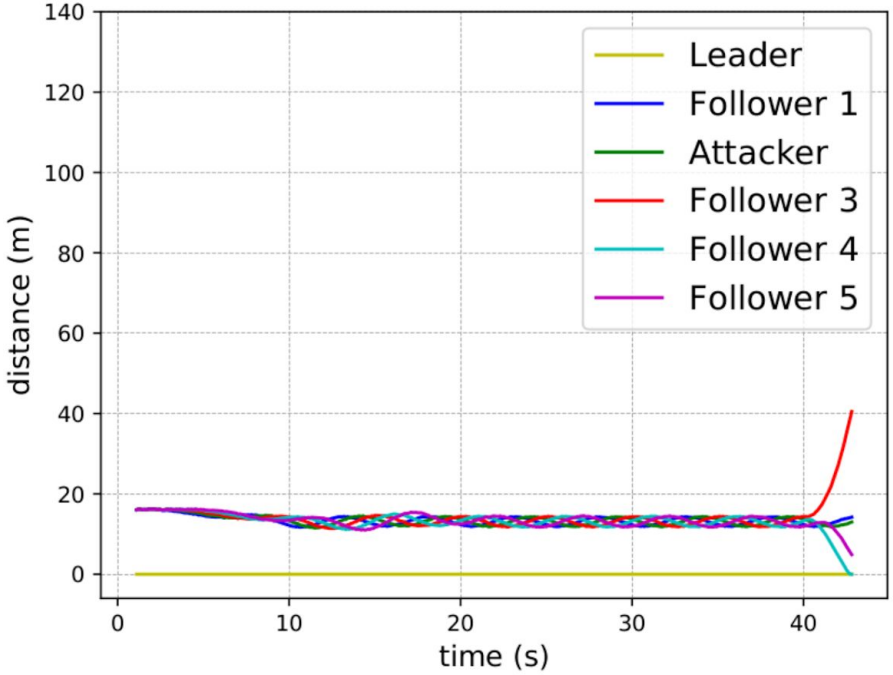
Smart Speed: Follower vs Leader Attacker

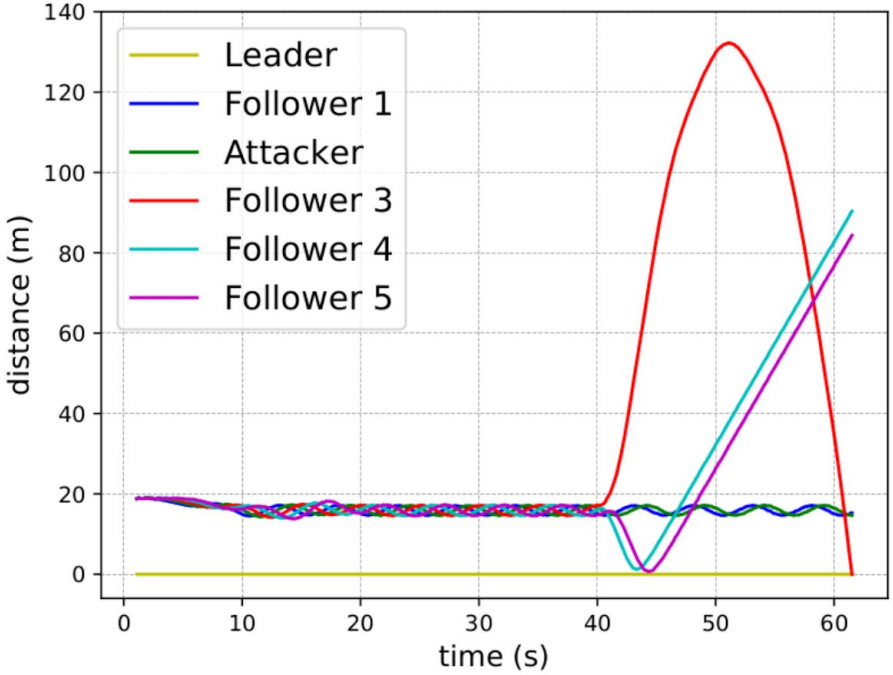
- PATH/Ploeg: Rear vs Front Collision
- Consensus: Bigger speed => Bigger gaps





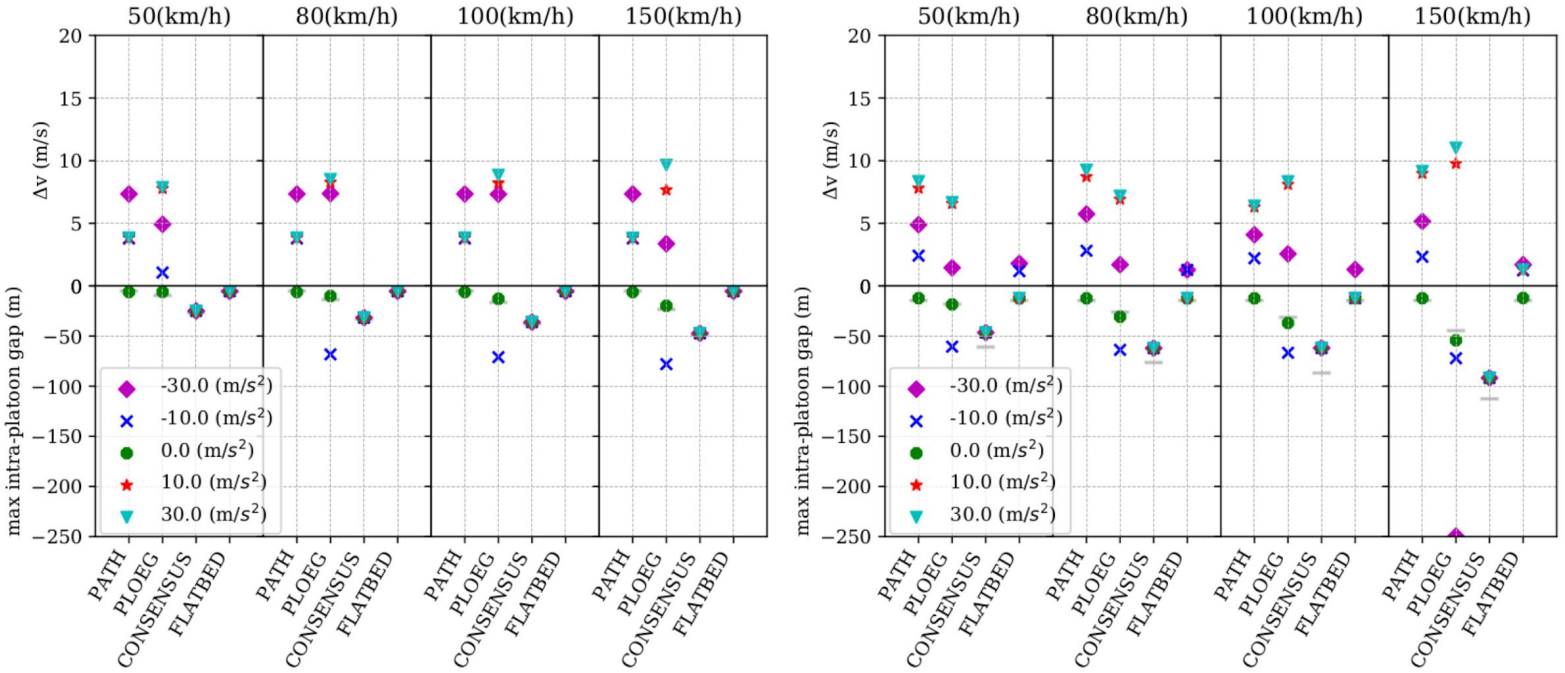
Smart Speed Ploeg 80 vs 100 km/h



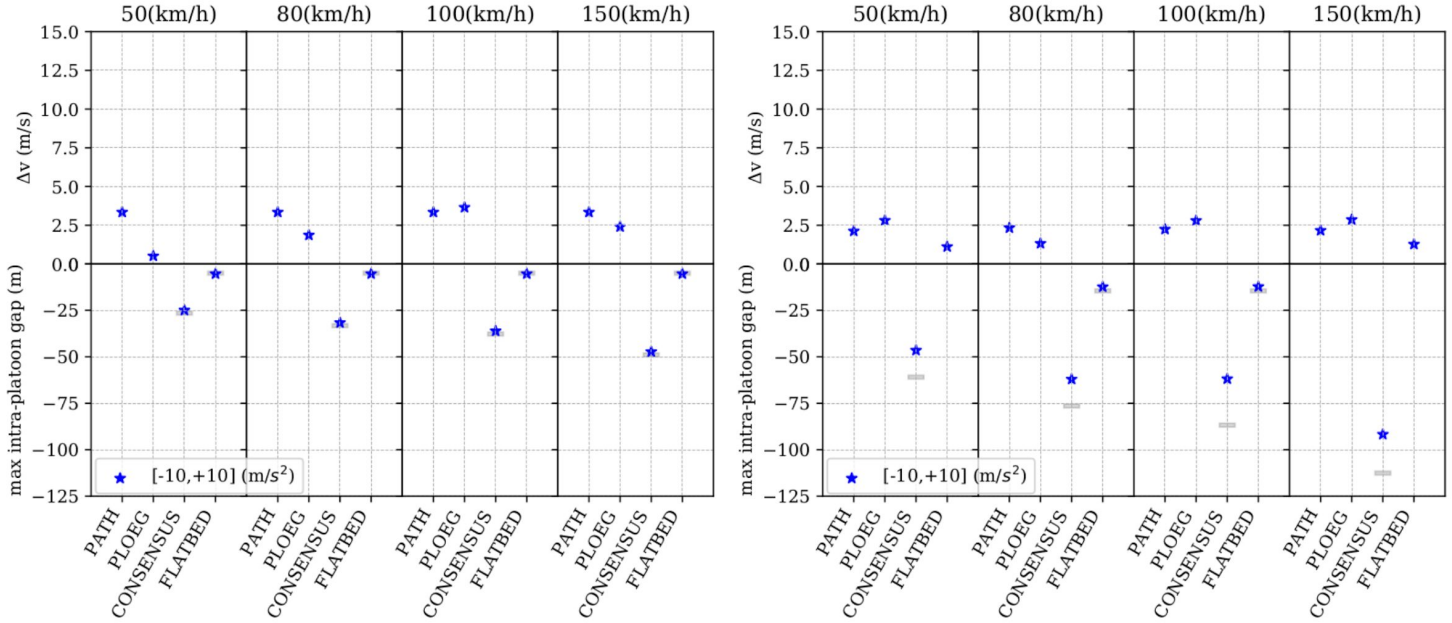


Acceleration: Static vs Join

- PATH: Positive values => better crashes (due to bigger gaps)

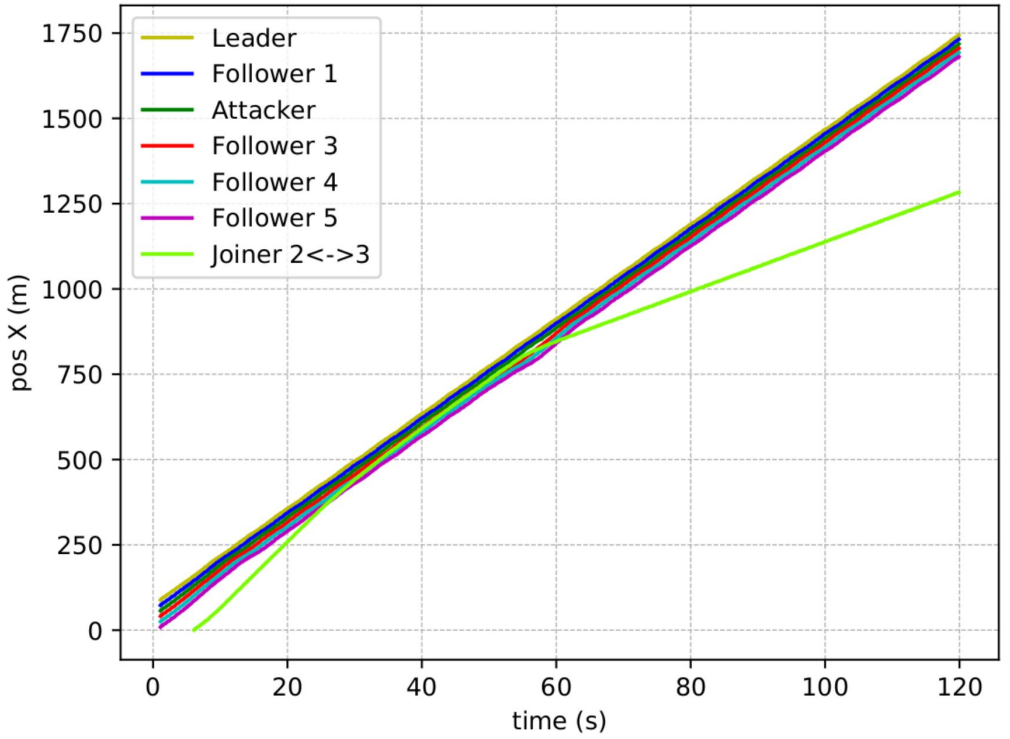


Gradual Acceleration: Static vs Join

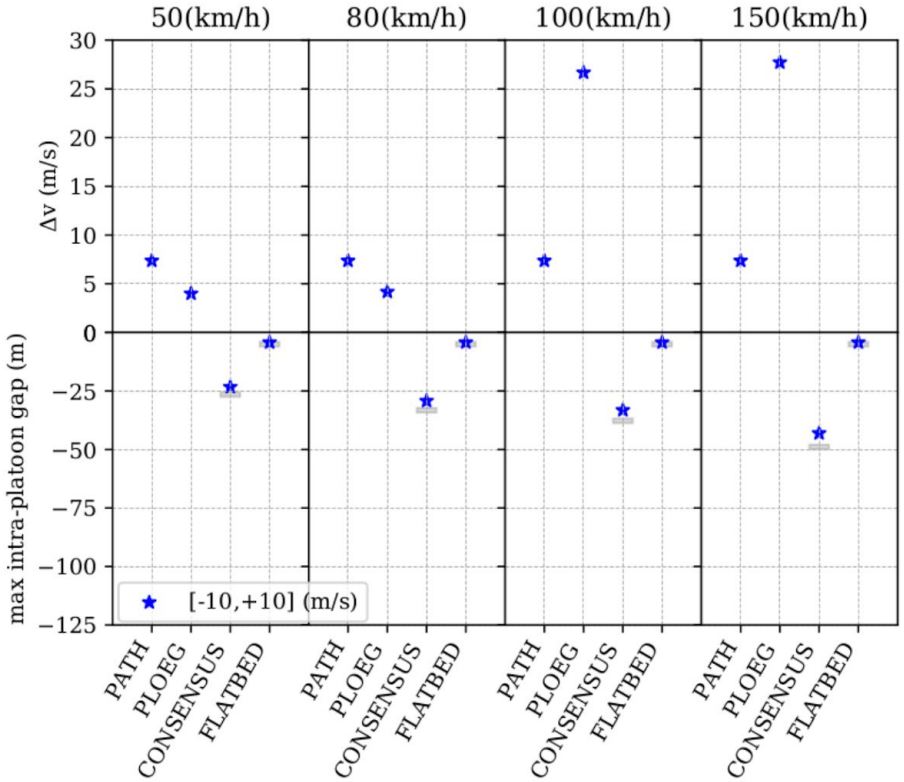


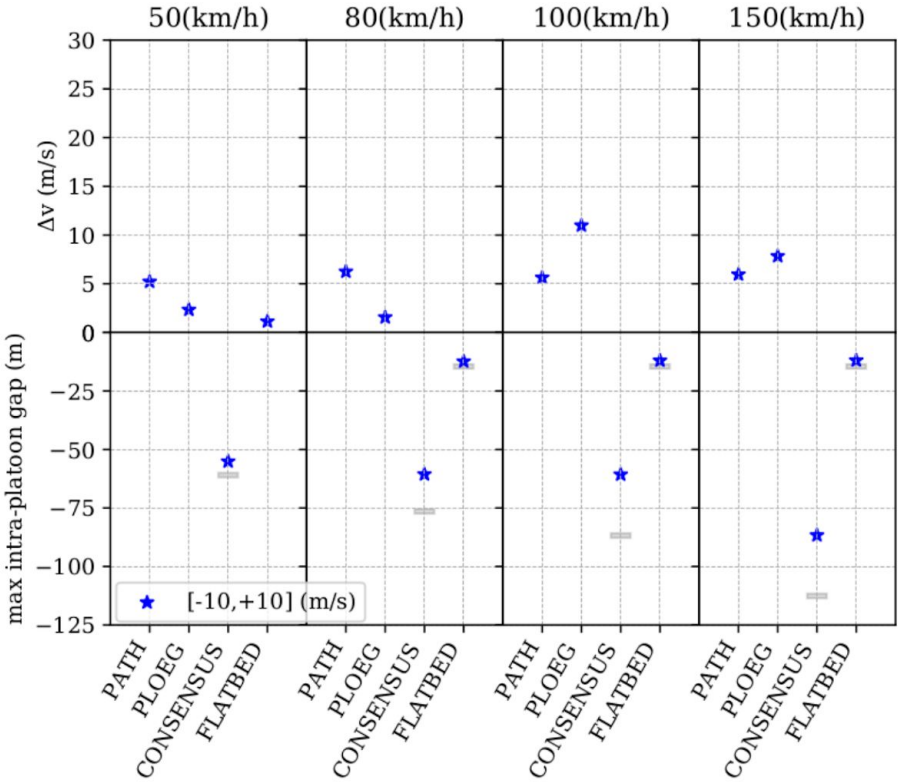
Gradual Speed Entry Denial: Ploeg

- Ploeg ignores speed data
- The Joiner does not
- Entry is aborted

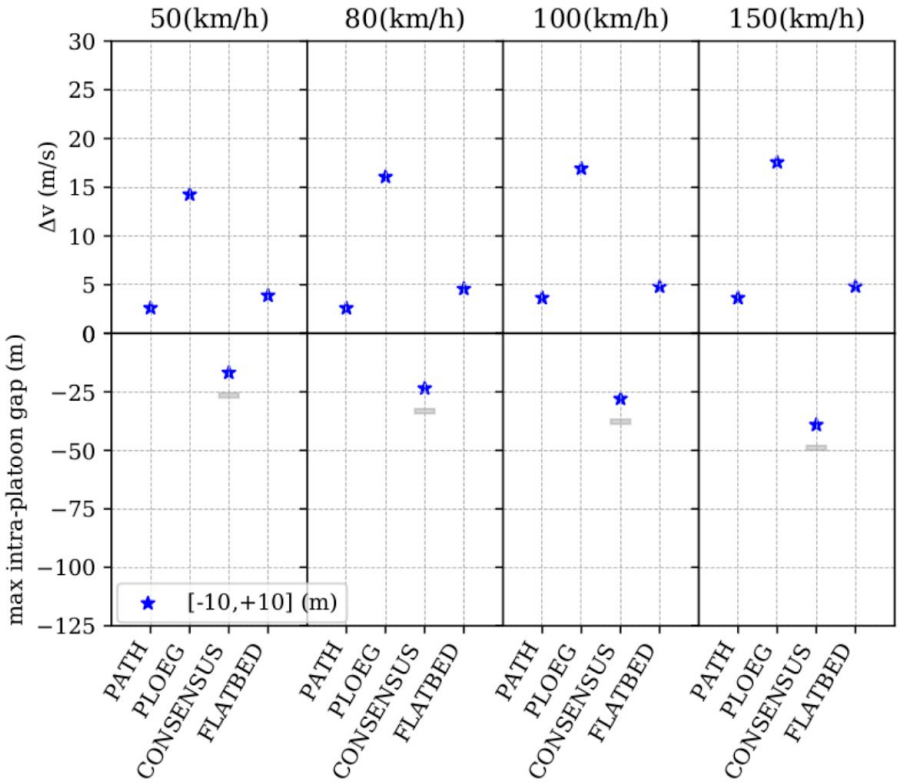


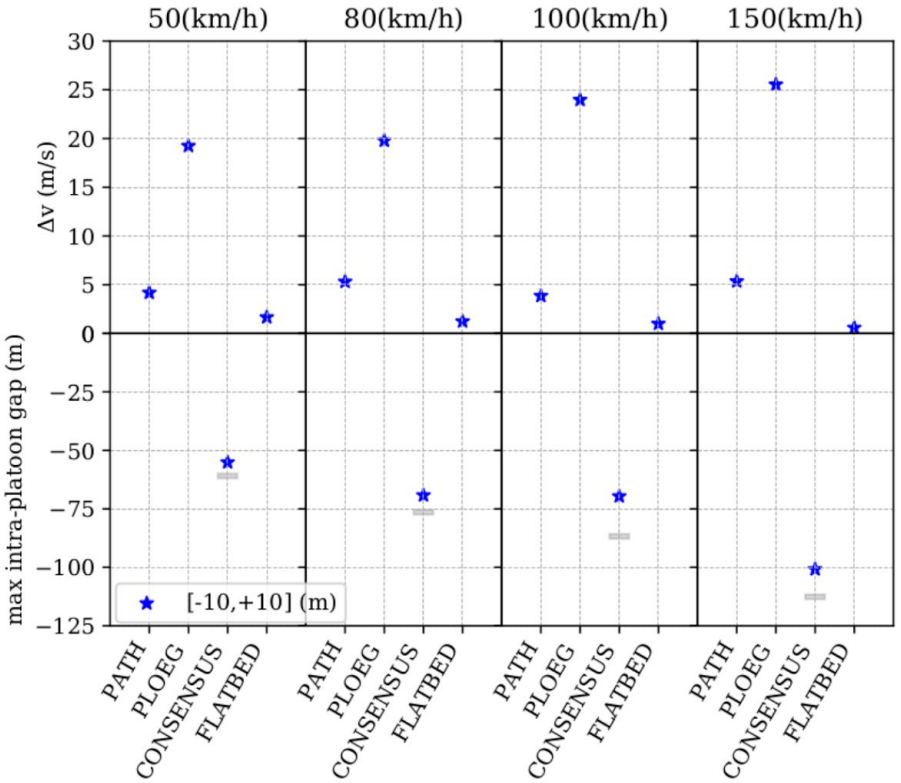
Smart Speed: Static vs Join



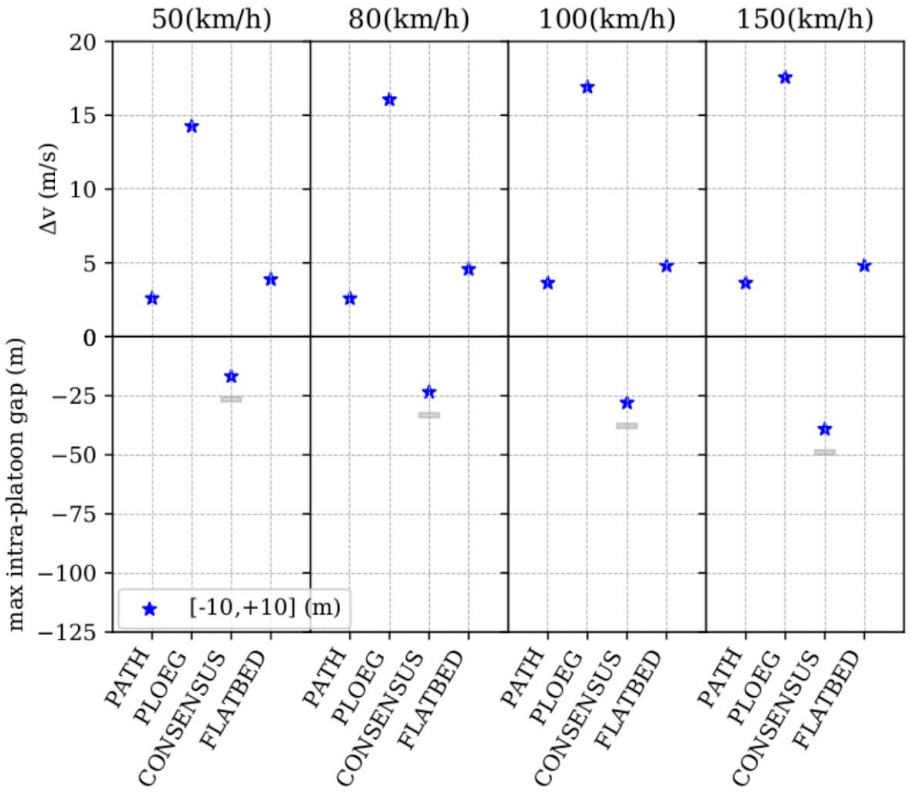


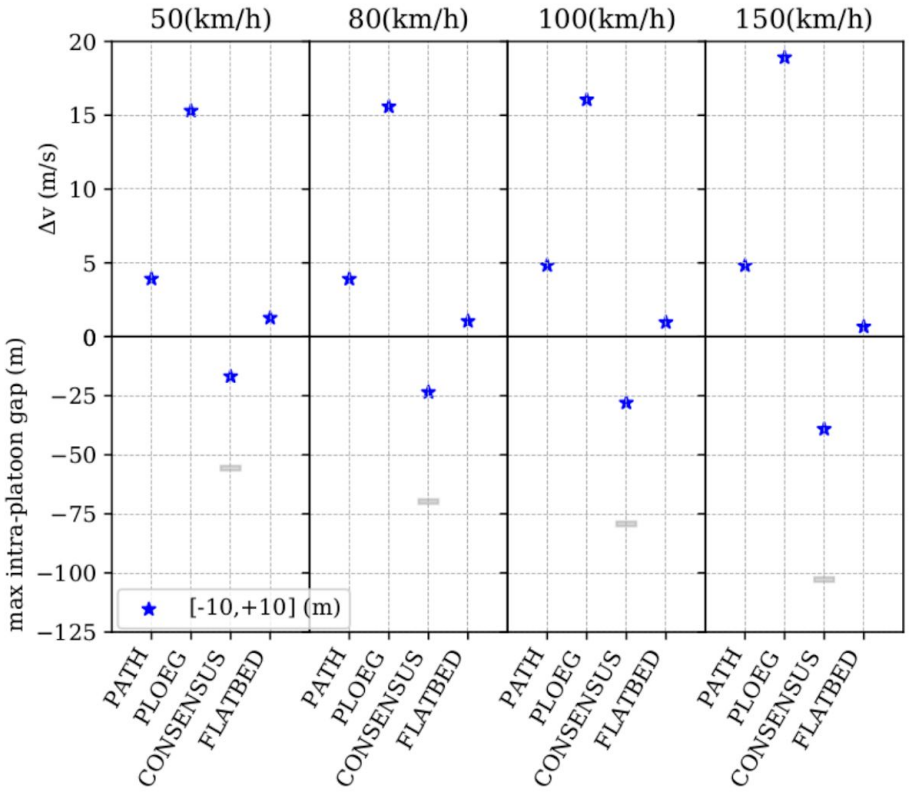
Smart Position: Static vs Join



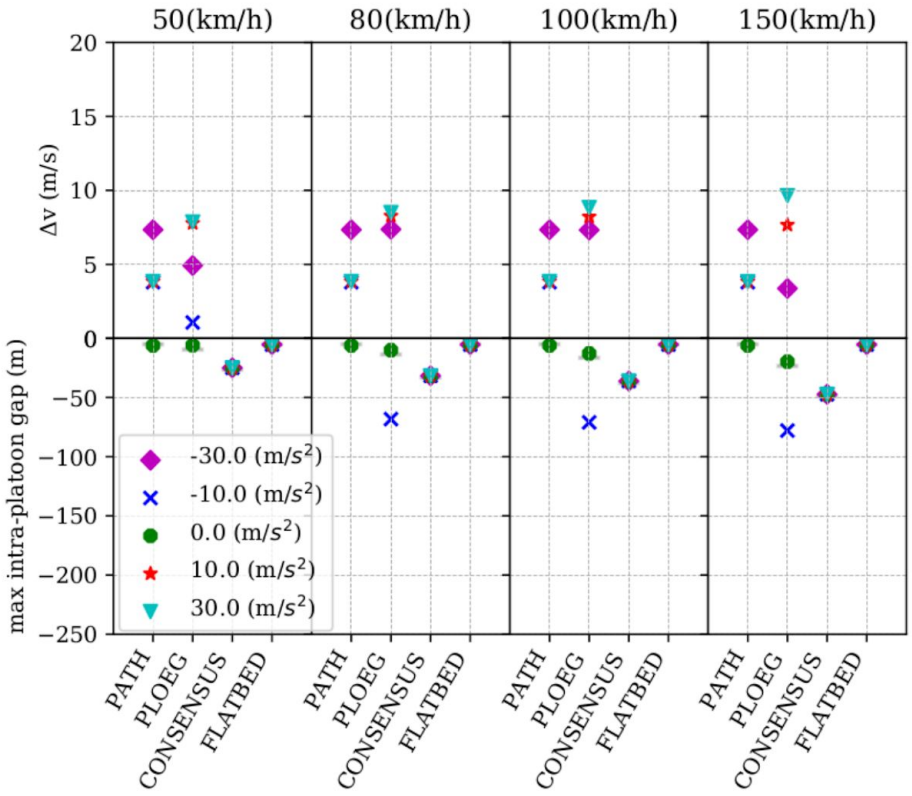


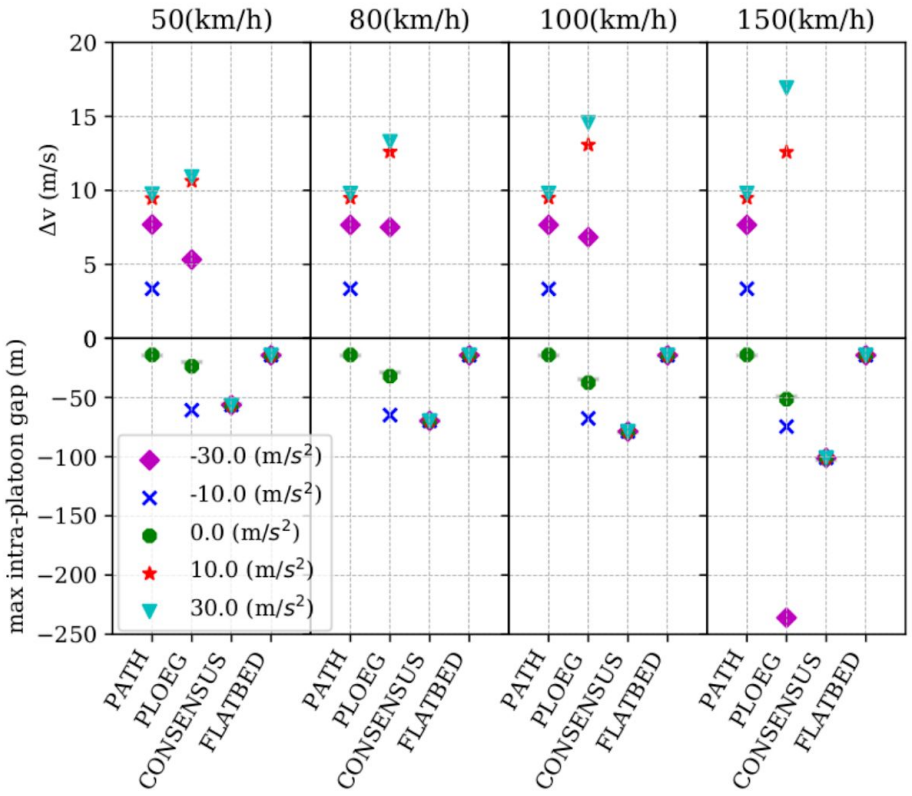
Smart Position: Static vs Exit



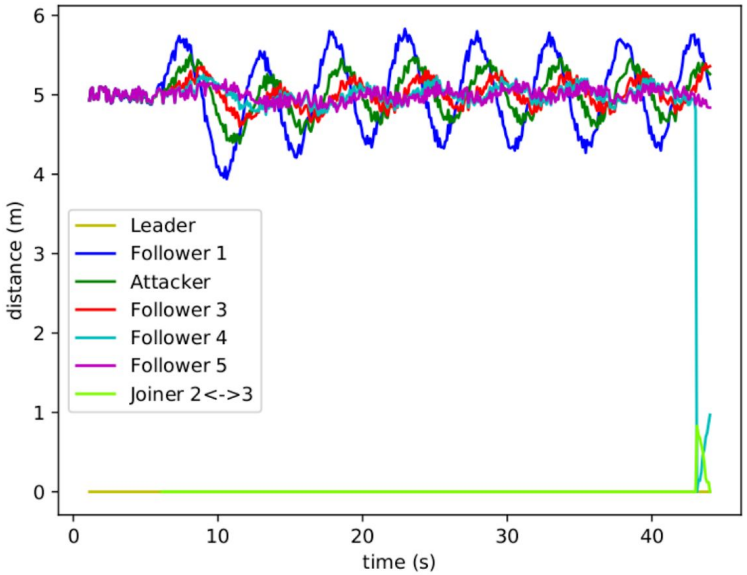


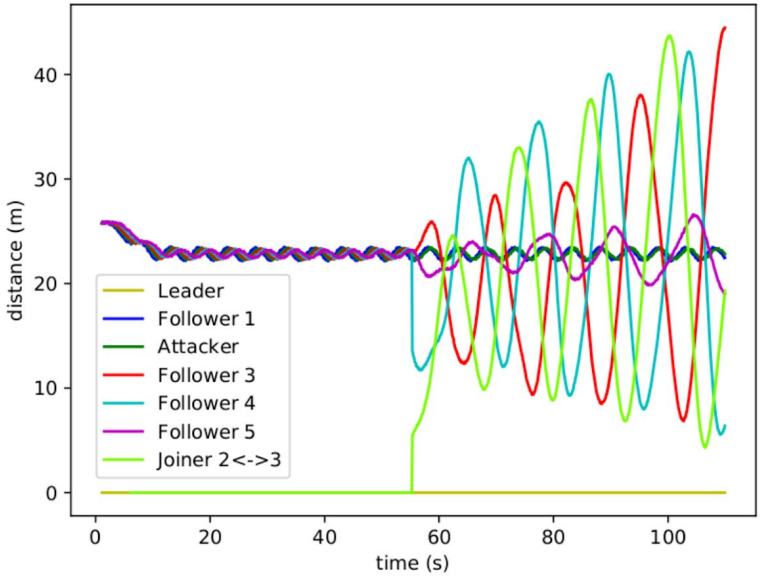
Acceleration: Static vs Exit



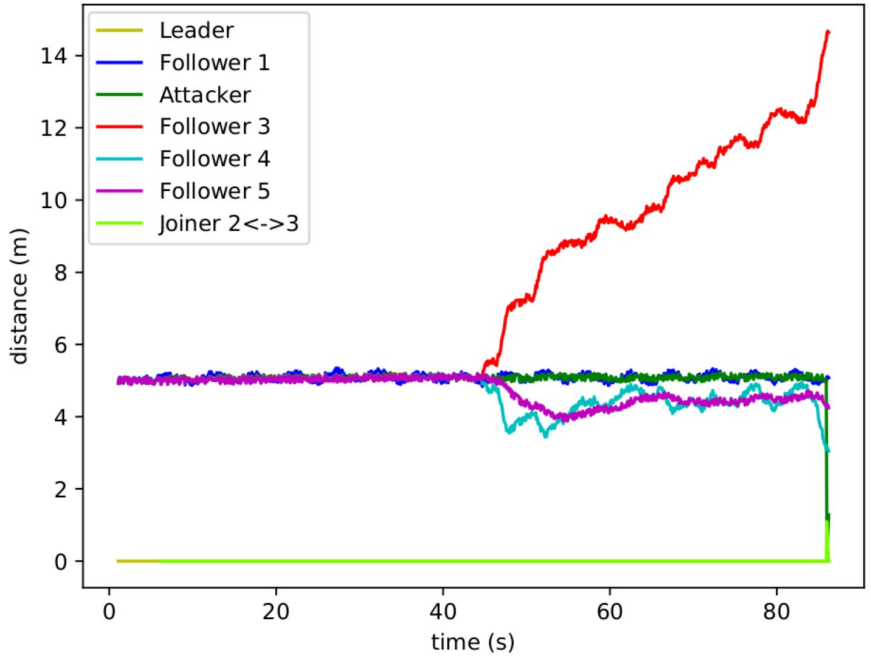


Join at Later Position: PATH vs Ploeg

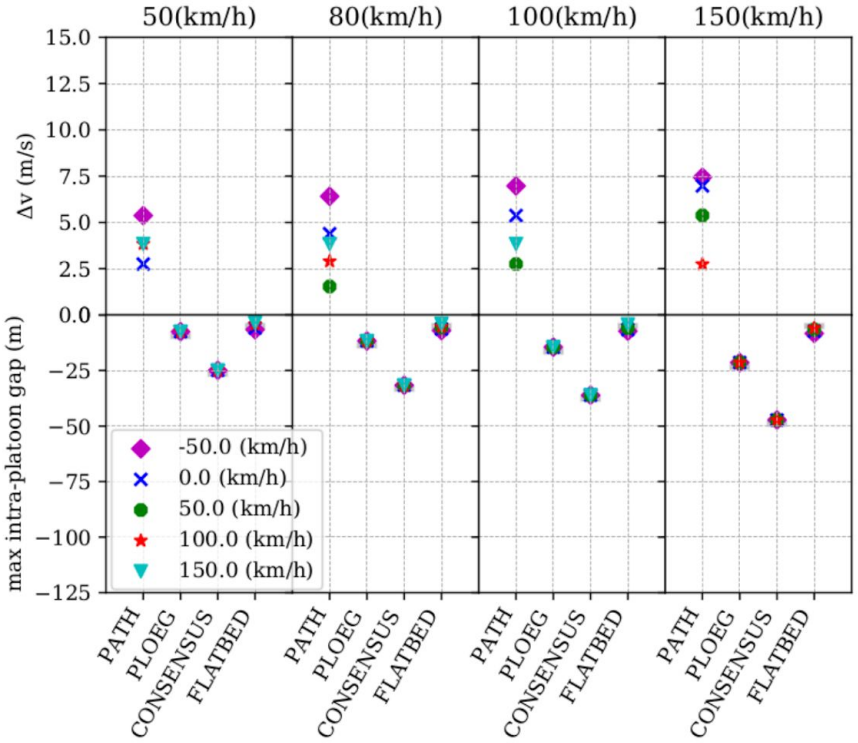


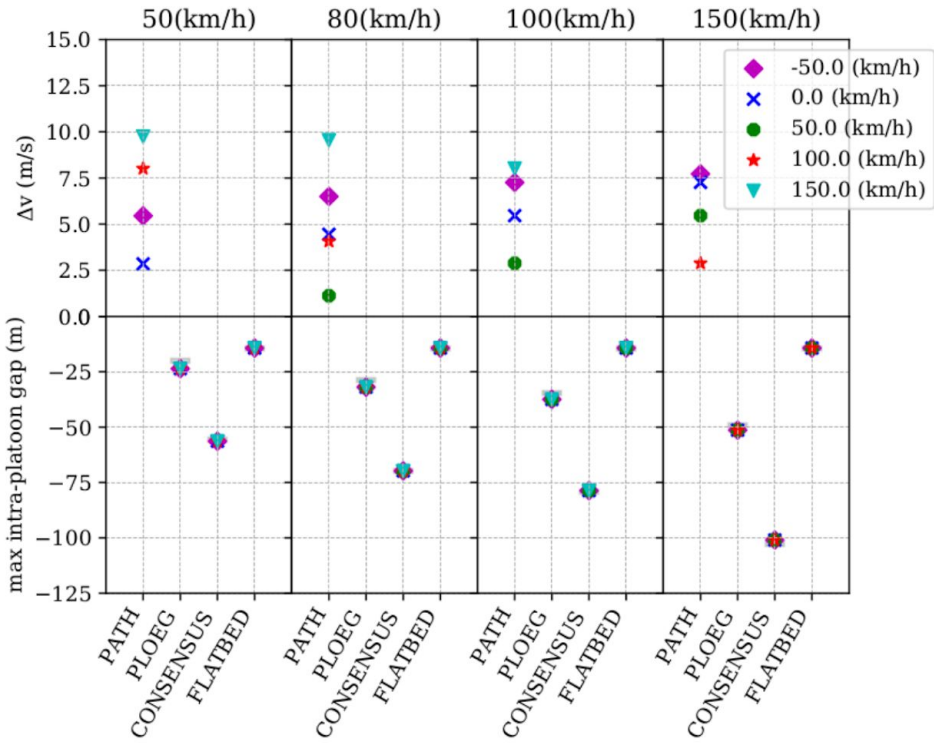


Join at Earlier Position: Flatbed



Speed Exit


50(km/h)
80(km/h)
100(km/h)
150(km/h)
Δv (m/s)
max intra-platoon gap (m)
15.0
12.5
10.0
7.5
5.0
2.5
0.0
−25
−50
−75
−100
−125
PATH
PLOEG
CONSENSUS
FLATBED
-50.0 (km/h)
0.0 (km/h)
50.0 (km/h)
100.0 (km/h)
150.0 (km/h)


50(km/h)
80(km/h)
100(km/h)
150(km/h)
Δv (m/s)
max intra-platoon gap (m)
15.0
12.5
10.0
7.5
5.0
2.5
0.0
−25
−50
−75
−100
−125
PATH
PLOEG
CONSENSUS
FLATBED
-50.0 (km/h)
0.0 (km/h)
50.0 (km/h)
100.0 (km/h)
150.0 (km/h)