ACM WiSeC 2022

Attack Impact and Misbehavior Detection in Vehicular Platoons

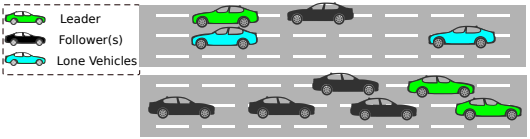
Konstantinos Kalogiannis, Mohammad Khodaei,
Weaam Mostafa Nemr Mohamed Bayaa and Panos Papadimitratos
Networked Systems Security (NSS) group, www.eecs.kth.se/nss

Overview

- The case of platooning
  - Benefits
  - Platoon properties
- Literature & Challenges
  - Misbehavior
  - Misbehavior Detection Scheme (MDS)
  - Maneuvering Protocols
- Our Investigation
  - Adversarial Model
  - Misbehavior Impact
  - Controller Comparison
  - Detection & Mitigation

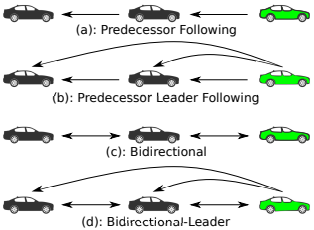
Platooning Application

- Benefits
  - Road Safety
  - Traffic Management
  - Fuel Efficiency
- Cooperative Awareness Message (CAM)
  - Periodic (e.g. every 100 ms)
  - Basic Information
  - Acts as neighborhood discovery



Platoon-Specific Properties

- Intra-Platoon Information Flow
  - Single hop
  - Most common: Predecessor Leader
  - Leader holds more power

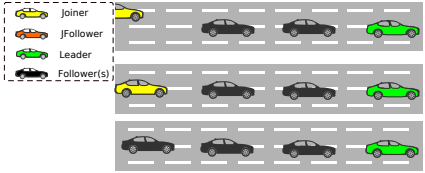


- Controllers
  - Constant Vehicle Spacing
  - Constant Time Headway

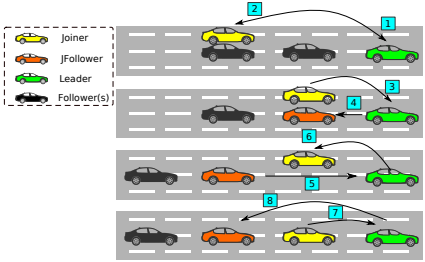
Controller	Policy	Predecessor			Leader			Topology
		D	S	A	P	S	A	
ACC	CTH	R	R	–	–	–	–	–
PATH	CVS	R	VR	V	–	V	V	PL Following
Consensus (CNSS)	BOTH	R	–	–	V	V	–	PL Following
Flatbed (FLBD)	CVS	R	VR	–	–	V	–	Leader Following
Ploeg (PLG)	CTH	R	R	V	–	–	–	Predecessor Following

Platoon Maneuvers

- Basic Maneuvers: Tail position
  - Join
  - Exit



- Extra configurations: all positions
  - Group vehicles based on destination
  - Group vehicles based on capabilities



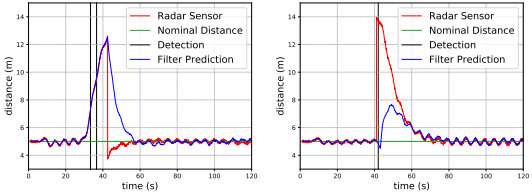
Related Work

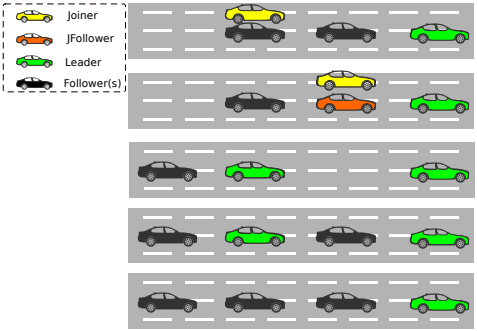
- Authentication & Privacy[a]
- Attacks[b]
  - Falsification
  - Jamming
- MDS[cd]
  - Plausibility checks
  - Kalman Filter
  - ML approaches

[a] KhodaeiJP2018J:SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems
[b] HeijdenLK2017C:Analyzing attacks on cooperative adaptive cruise control (CACC)
[c] IorioRSBR2019C:Detecting Injection Attacks on Cooperative Adaptive Cruise Control
[d] KamelAPKJU2020J:Simulation Framework for Misbehavior Detection in Vehicular Networks

Challenges

- Insiders
  - Inherent knowledge of the platoon
  - Can eavesdrop on all messages
  - Leader can provoke maneuvers
- Maneuvers
  - Can affect MDS
  - Vulnerable Protocols
- Pitfalls
  - Misbehavior & Controllers





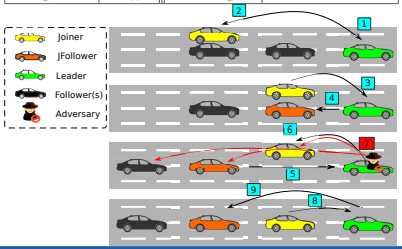
Adversary Model

- Internal Attacker
- External Jammers
- Collusion
  - Between internal & external
  - Multiple attackers
- Rational Attacker
  - Self-preservation
  - Physical presence

Misbehavior Configuration

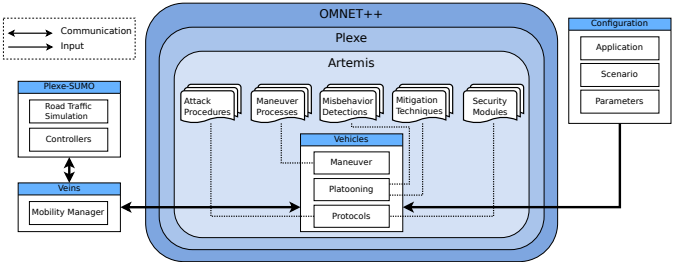
- Attack sophistication
  - Naive falsification & jamming
  - "Intelligent" falsification
  - Targeted jamming
- Scenarios
  - Attacks on static & maneuvering platoons
  - Collusion attacks on static platoons
  - Jamming attacks
- Basic Setup
  - Long highway
  - Sensor errors

Parameters	Value	Parameters	Value
Beacon interval	0.1s	Controller	PATH, Ploeg, Consensus, Flatbed
Carrier frequency	5.89 GHz	Spacing	5m, 0.5s, 0.8s, 5m
Physical layer bit-rate	6 Mbps	Leader speed	50, 80, 100, 150 kmph
Area size	5 KM × 50 M 4 lanes	Sensors	$\epsilon_p^{V2V} = 1m$, $\epsilon_s^{V2V} = 0.1m/s$, $\epsilon_a^{V2V} = 0.01m/s^2$, $\epsilon_p^{RAD} = 0.1m$, $\epsilon_s^{RAD} = 0.1m/s$
Number of vehicles	6 - 7 (Join)	Falsification steps	$Position_{step} = 2.5m$ $Speed_{step} = 0.5m/s$ $Acceleration_{step} = 0.05m/s^2$
Propagation delays	Randomized	Kalman Filter (KF)	$AverageWindow = 10$ values $Tolerance = 10$ detections $distance^{KF}_{threshold} = 0.33$ $distance^{RAD}_{threshold} = 0.25$ $acceleration_{factor} = 0.05$
Vehicle TX Range	600m	Leader speed pattern	Sinusoidal
Jammer TX Range	50m	Number of executions	10 times
TX power	100mW	Duration of simulation	120s
Thermal Noise	-95dBm	Warm-up period	30s
Sensitivity	-94dBm	Mitigation Headway	2s
Sliding window	1s-9(1)s	Vehicle length	4 m



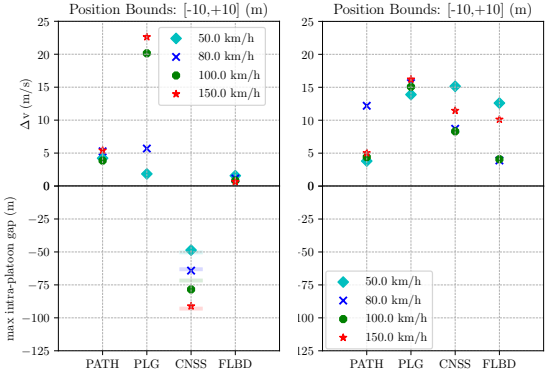
Simulation Framework

- Simulation
  - Expands widely used tools
  - Utilizes SUMO
- Modules
  - Attack scenarios (x11)
  - Maneuvers (x5)
  - Defensive mechanisms (x2)
  - Mitigation mechanisms (x2)
- Capabilities
  - Combination of modules
  - Sensor errors
  - Python/ML modules integration

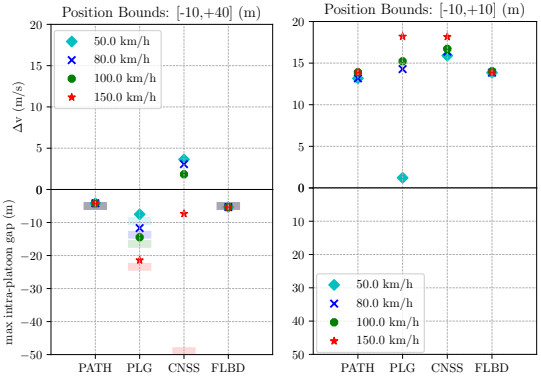


Misbehavior Impact

- Combined Position During Join
  - Follower vs Leader
  - Different collisions → different severity

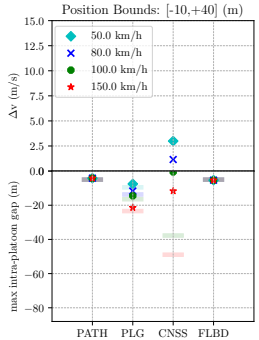


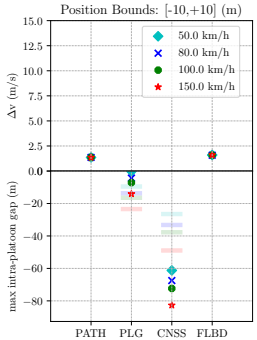
- Leader Position During No Maneuver
  - Gradual vs Combined
  - Combined attacks affect all controllers

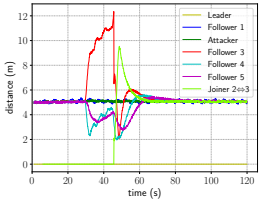


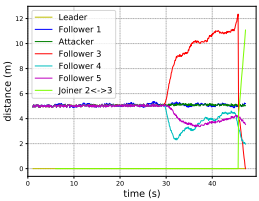
Misbehavior Impact

- Gradual Position & Target Jamming
  - Potentially less impactful
  - Depends on controller
- Extra: Join Pitfall
  - Different controllers: Joiner **vs** Platoon
  - Relatively negative values can lead to collisions









Rational Attacker

F: Follower; L: Leader; Red: Attacker Crashes; Green: Attacker is safe

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}	LF {3,5,7,9,11}	LF {3,5,7,9,11}	LF {3,5,7,9,11}	LF {3,5,7,9,11}	LF {3,5,7,9,11}	LF {3,5,7,9,11}	LF {3,5,7,9,11}	LF {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}	LF {-50,0}	LF {-50,0} F 50	LF {-50,0,50}	LF {-50,0,50,100}	LF {-50,0}	LF {-50,0} F 50	LF {-50,0,50}	LF {-50,0,50,100}
	Consensus	L {100,150}	L 150	L 150	-	L {100,150}	L 150	L {0, 50}	L -50	L {100,150}	L 150	L 150	-
	Flatbed	L {100,150}	L {100,150}	L 150	-	F {-50,0}	LF {-50,0} L 50	LF {-50,0} L 50	F {-50,0,50,100}	L {100,150}	L {100,150}	L 150	-
	Ploeg	-	-	-	-	-	-	-	-	-	-	-	-
Acceleration (m/s^2)	PATH	F {-30,-10}	F {-30,-10}	F {-30, -10}	F {-30, -10}	F {-30,-10}	LF -30, F -10	LF -30, F -10	LF -30, F -10	F {-30,-10}	F {-30,-10}	F {-30,-10}	F {-30,-10}
	Consensus	-	-	-	-	-	-	-	-	-	-	-	-
	Flatbed	-	-	-	-	LF -10, F -30	F {-30,-10}	L -10, F -30	F {-30,-10,10,30}	-	-	-	-
	Ploeg	LF {-10,-30}	LF -30	LF -30	LF -30	L, -10, LF -30	LF -30	LF -30	LF {10,30}	LF -30	LF -30	LF -30	L -30
Gradual Position (m)	PATH	-	-	-	-	-	-	-	-	-	-	-	-
	Consensus	LF -10/+40	LF -10/+40	-	-	LF -10/+40	LF -10/+40	L -10/+40	-	LF -10/+40	LF -10/+40	L -10/+40	-
	Flatbed	-	-	-	-	-	-	-	-	-	-	-	-
	Ploeg	-	-	-	-	-	-	-	-	-	-	-	-
Gradual Speed (m/s)	PATH	LF {-10/+17}	LF {-10/+17}	LF {-10/+17}	LF {-10/+17}	LF -10/+17	LF -10/+17	LF -10/+17	LF -10/+17	LF -10/+17	LF -10/+17	LF -10/+17	LF -10/+17
	Consensus	L -10/+17	L -10/+17	L -10/+17	L -10/+17	L -10/+17	L -10/+17	L -10/+17	L -10/+17	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	L -10/+17	L -10/+17	L -10/+17	L -10/+17	L -10/+17	L -10/+17	L -10/+17	L -10/+17
	Ploeg	-	-	-	-	-	-	-	-	-	-	-	-
Gradual Acceleration (m/s^2)	PATH	L -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10
	Consensus	-	-	-	-	-	-	-	-	-	-	-	-
	Flatbed	-	-	-	-	LF -10/+10	-	L -10/+10	F -10/+10	-	-	-	-
	Ploeg	LF -10/+10	LF -10/+10	LF -10/+10	LF -10/+10	L -10/+10	LF -10/+10	LF -10/+10	LF -10/+10	LF -10/+10	LF -10/+10	LF -10/+10	LF -10/+10
Combined Position (m)	PATH	L -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10
	Consensus	L -10/+10	L -10/+10	L -10/+10	L -10/+10	L -10/+10	L -10/+10	L -10/+10	L -10/+10	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	LF -10/+10	LF -10/+10	L -10/+10	LF -10/+10	LF -10/+10	LF -10/+10	LF -10/+10	LF -10/+10
	Ploeg	L -10/+10	LF -10/+10	LF -10/+10	LF -10/+10	F -10/+10	F -10/+10	LF -10/+10	LF -10/+10	LF -10/+10	LF -10/+10	LF -10/+10	LF -10/+10
Combined Speed (m/s)	PATH	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	LF -10/+10	LF -10/+10	LF -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10
	Consensus	L -10/+10	L -10/+10	-	-	L -10/+10	L -10/+10	L -10/+10	-	L -10/+10	L -10/+10	-	-
	Flatbed	L -10/+10	L -10/+10	L -10/+10	L -10/+10	LF -10/+10	L -10/+10	L -10/+10	L -10/+10	L -10/+10	L -10/+10	L -10/+10	L -10/+10
	Ploeg	LF -10/+10	LF -10/+10	L -10/+10	LF -10/+10	LF -10/+10	LF -10/+10	LF -10/+10	LF -10/+10	LF -10/+10	LF -10/+10	L -10/+10	LF -10/+10
Combined Acceleration (m/s^2)	PATH	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10
	Consensus	-	-	-	-	-	-	-	-	-	-	-	-
	Flatbed	L -10/+10	L -10/+10	L -10/+10	L -10/+10	L -10/+10	L -10/+10	L -10/+10	L -10/+10	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	L -10/+10	LF -10/+10	LF -10/+10	LF -10/+10	LF -10/+10	LF -10/+10	LF -10/+10	LF -10/+10

Rational Attacker

- Path
  - Follower attacks are more valuable
  - Relatively negative values are better

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)
Speed (km/h)	PATH	LF {-50,0}	LF {-50,0} F 50	LF {-50,0,50}	LF {-50,0,50,100}	LF {-50,0}	LF {-50,0} F 50	LF {-50,0,50}	LF {-50,0,50,100}	LF {-50,0}	LF {-50,0} F 50	LF {-50,0,50}	LF {-50,0,50,100}
Acceleration (m/s^2)	PATH	F {-30,-10}	F {-30,-10}	F {-30, -10}	F {-30, -10}	F {-30,-10}	LF -30, F -10	LF -30, F -10	LF -30, F -10	F {-30,-10}	F {-30,-10}	F {-30,-10}	F {-30,-10}
Gradual Speed (m/s)	PATH	LF {-10/+17}	LF {-10/+17}	LF {-10/+17}	LF {-10/+17}	LF -10/+17	LF -10/+17	LF -10/+17	LF -10/+17	LF -10/+17	LF -10/+17	LF -10/+17	LF -10/+17
Gradual Acceleration (m/s^2)	PATH	L -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10
Combined Position (m)	PATH	L -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10
Combined Speed (m/s)	PATH	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	LF -10/+10	LF -10/+10	LF -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10
Combined Acceleration (m/s^2)	PATH	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10	F -10/+10

- Consensus
  - Few good collisions
  - Good collisions only during Join

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)	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}	LF {3,5,7,9,11}	LF {3,5,7,9,11}	LF {3,5,7,9,11}	LF {3,5,7,9,11}	LF {3,5,7,9,11}	LF {3,5,7,9,11}	LF {3,5,7,9,11}	LF {3,5,7,9,11}
Speed (km/h)	Consensus	L {100,150}	L 150	L 150	-	L {100,150}	L 150	L {0, 50}	L -50	L {100,150}	L 150	L 150	-
Gradual Position (m)	Consensus	LF -10/+40	LF -10/+40	-	-	LF -10/+40	LF -10/+40	L -10/+40	-	LF -10/+40	LF -10/+40	L -10/+40	-
Gradual Speed (m/s)	Consensus	L -10/+17	L -10/+17	L -10/+17	L -10/+17	L -10/+17	L -10/+17	L -10/+17	L -10/+17	L -10/+17	L -10/+17	L -10/+17	L -10/+17
Combined Position (m)	Consensus	L -10/+10	L -10/+10	L -10/+10	L -10/+10	L -10/+10	L -10/+10	L -10/+10	L -10/+10	L -10/+10	L -10/+10	L -10/+10	L -10/+10
Combined Speed (m/s)	Consensus	L -10/+10	L -10/+10	-	-	L -10/+10	L -10/+10	L -10/+10	-	L -10/+10	L -10/+10	-	-

Controller Comparison

- Expected behavior
  - Simple attacks affect certain controllers
  - Attacker's position is important
- Combined Attacks
  - Potent Speed & Acceleration
  - Position is *almost* always catastrophic
- Consensus is overall the best

Controller Resilience (%)

Controller	Simple			Gradual			Combined		
	P	S	A	P	S	A	P	S	A
PATH	100	0	20	100	0	0	0	0	0
Ploeg	100	100	20	100	100	0	0	0	0
Consensus	0	50	100	0	33.3	100	0	45.8	62.5
Flatbed	91.7	14.7	51.7	87.5	0	33.3	0	29.1	29.1

Controller Instability (%)

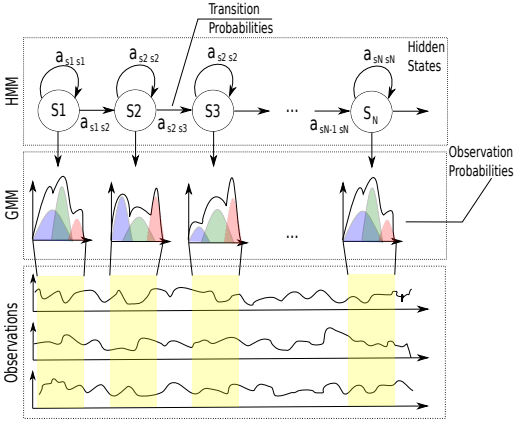
Controller	Simple			Gradual			Combined		
	P	S	A	P	S	A	P	S	A
PATH	0	2.9	17.5	0	0	0	0	0	0
Ploeg	0	0	20	0	0	0	0	0	0
Consensus	0	35.3	0	37.5	16.7	0	50	25	37.5
Flatbed	8.3	54.9	40	12.5	50	33.3	0	16.7	4.2

Controller Crash (%)

Controller	Simple			Gradual			Combined		
	P	S	A	P	S	A	P	S	A
PATH	0	97.1	62.5	0	100	100	100	100	100
Ploeg	0	0	60	0	0	100	100	100	100
Consensus	100	14.7	0	62.5	50	0	50	29.2	0
Flatbed	0	30.4	8.4	0	50	33.4	100	54.2	66.7

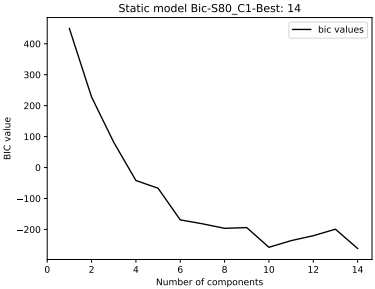
Hidden Markov Model

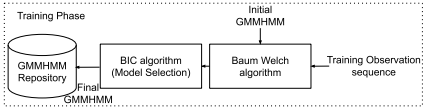
- Basic
  - States depend **only** on the previous state
  - Observations are based on each state
  - We cannot see the (hidden) states
- What do they solve?
  - P1: Estimate model parameters given some observations
  - P2: What is the likelihood of some observations being represented by a model?
  - P3: Given observations which (hidden) states produced it?



HMM - Training

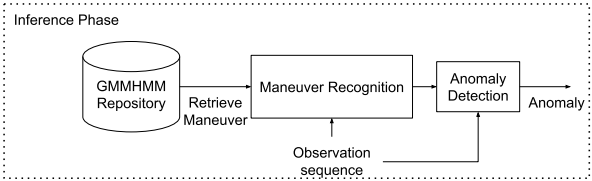
- Training Goal
  - Find initial parameters
  - Select the *best* model (underfit vs overfit)
- Find best model
  - $BIC = k \ln(n) - 2 \ln(\hat{L})$
  - $k = \#parameters$
  - $\hat{L} = \max likelihood$
  - $n = \#Observations$
- Training
  - Gather $O_t = (rd_{i,j}, rv_{i,j})$ for each maneuver
  - $rd_{i,j}, rv_{i,j}$ are controller outputs
  - Single Observation set per car's controller, speed and maneuver





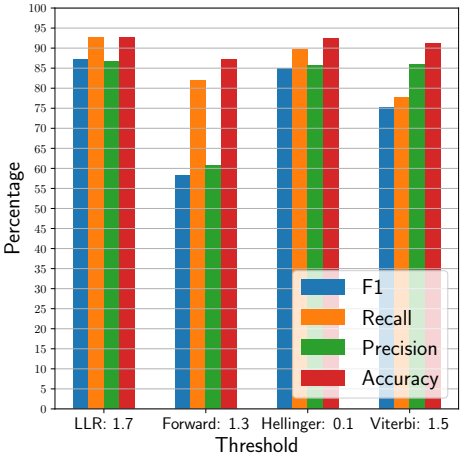
HMM - Detection

- Maneuver Recognition & Attack Detection
  - P2/Forward: $\max\left(L(\lambda_1|O_{trip}), L(\lambda_2|O_{trip}), L(\lambda_3|O_{trip})\right)$
  - P3/Viterbi: Biggest state chain similarity wins
  - Detect: $\mathrm{H}(L(\lambda_{chosen}|O_{trip}), L(\lambda_{chosen}|O_{benign}))$
- Attack Detection **Only**
  - Hellinger: $\min\left(L(\lambda_i|O_{trip}), L(\lambda_i|O_{benign})\right)$
  - Log Likelihood Ratio (LLR): $\min\left(\log L(\lambda_i|O_{trip}) - \log L(\lambda_i|O_{benign})\right)$



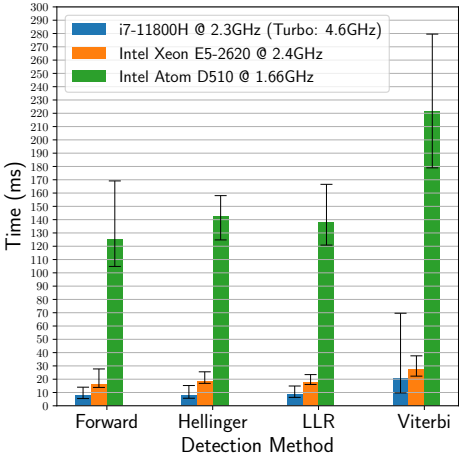
Misbehavior Detection Rates

- Metrics
  - Precision: $\frac{TP}{TP+FP}$
  - Recall: $\frac{TP}{TP+FN}$
  - Accuracy: $\frac{TP+TN}{P+N}$
  - F1: $\frac{2TP}{2TP+FP+FN}$
- Window
  - Forward & Viterbi: 9(1)s
  - Hellinger & LLR: 1s



Misbehavior Detection Overhead

- Timings
  - Worst Case: Viterbi
  - Best Case: Forward
  - On-Board Unit (OBU) slower
  - All $\leq$1s (window)
- Detection & Timings
  - Best Case: LLR
  - Worst time: $<$ 2 beacons



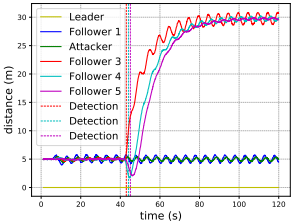
ACM WiSeC 2022

Attack Impact and Misbehavior Detection in Vehicular Platoons

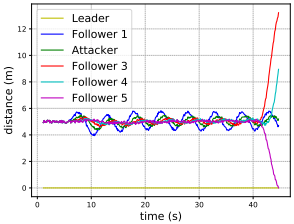
Konstantinos Kalogiannis, Mohammad Khodaei,
Weaam Mostafa Nemr Mohamed Bayaa and Panos Papadimitratos
Networked Systems Security (NSS) group, www.eecs.kth.se/nss

Appendix - Mitigation Techniques

- Current Techniques
  - Degrade to Adaptive Cruise Control (ACC)
  - Gracefully degrade to ACC
- Effectiveness
  - Collusion attacks still lead to crash
- Considerations
  - Speed of detection is important
  - Jamming response affects the outcome



Without jamming



With jamming/collusion