CommPact:

Evaluating the Feasibility of Autonomous Vehicle Contracts

University of Michigan, Ann Arbor

Jeremy Erickson, Shibo Chen, Melisa Savich, Shengtuo Hu
Advisor: Z. Morley Mao

Platooning

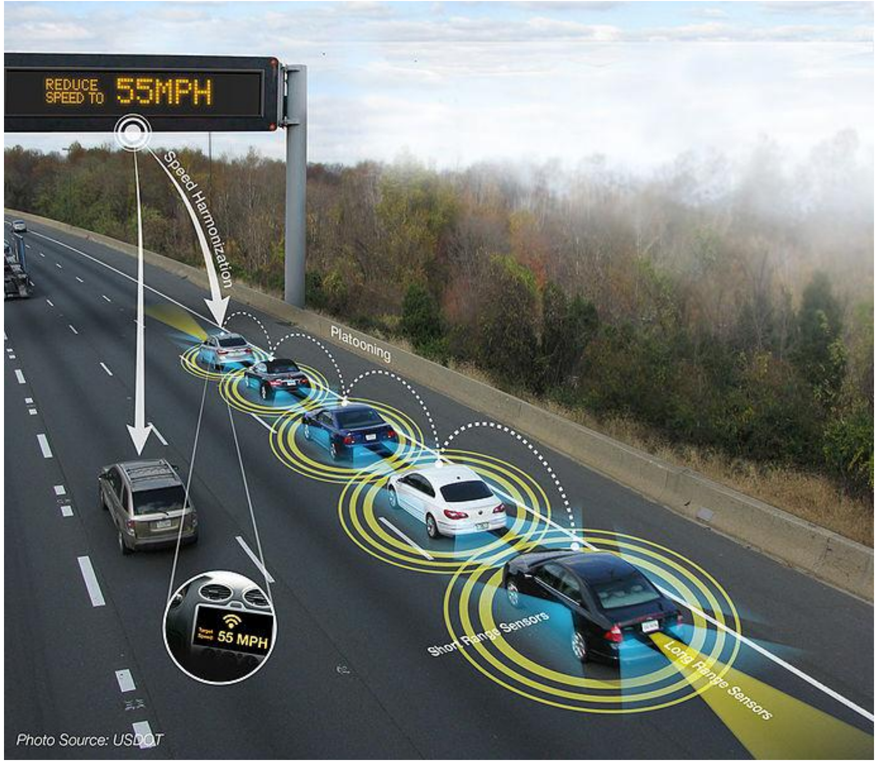
Goal: reduce following distance between vehicles

Advantages:

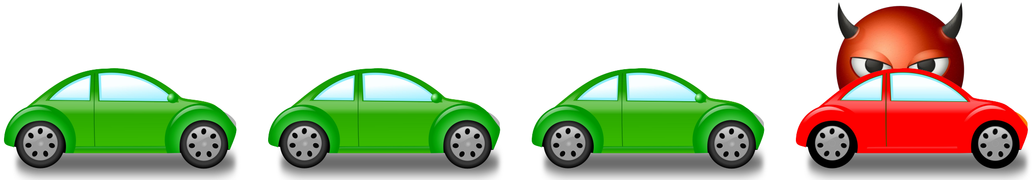
- Decrease drag (improve fuel economy)
- Increase traffic density

Disadvantages:

- Safety concerns



Safety concerns



One malicious vehicle could suddenly brake and cause a massive accident

Recent Example:
"Police say a car going east on the QEW in Mississauga suddenly moved into the left lane in front of a line of cars and hit the brakes — causing five vehicles to slam into one another."
http://toronto.citynews.ca/2018/02/08/qew-fatal-crash-arrest/

By reducing its own following distance, an autonomous vehicle is violating a safety parameter

Before doing so, we would like some assurance that the vehicle is still safe!

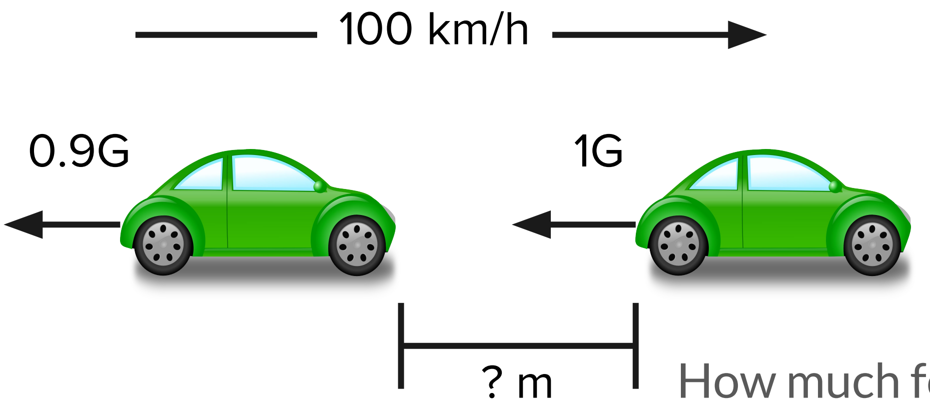
Braking rates vary significantly

Model	Category	Weight (lbs | kg)	Deceleration (m/s^2)
2017 Koenigsegg Agera RS	Super	3000 | 1360	11.62 to 12.85
2015 Ford Mustang GT	Sport	3805 | 1726	10.93
2016 Mazda MX-5 (Miata) Club	Sport	2332 | 1058	10.44
2016 Honda Civic Sedan (Touring)	Compact	2923 | 1326	10.09
2016 Honda Civic Sedan (EX)	Compact	2790 | 1266	9.29
2015 Ford F-150	Truck	5160 | 2341	9.15
2017 Toyota Sienna Limited	Minivan	4560 | 2068	8.87
2016 Ford F-150	Truck	4629 | 2100	7.93

Reactive approach to sudden braking

Leader emergency brakes.

Let's assume the follower reacts instantly.

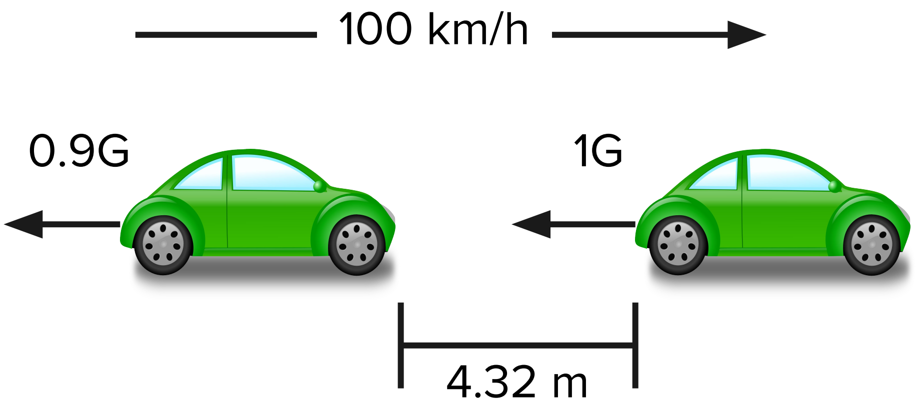


10% braking variance

How much following distance do we need?

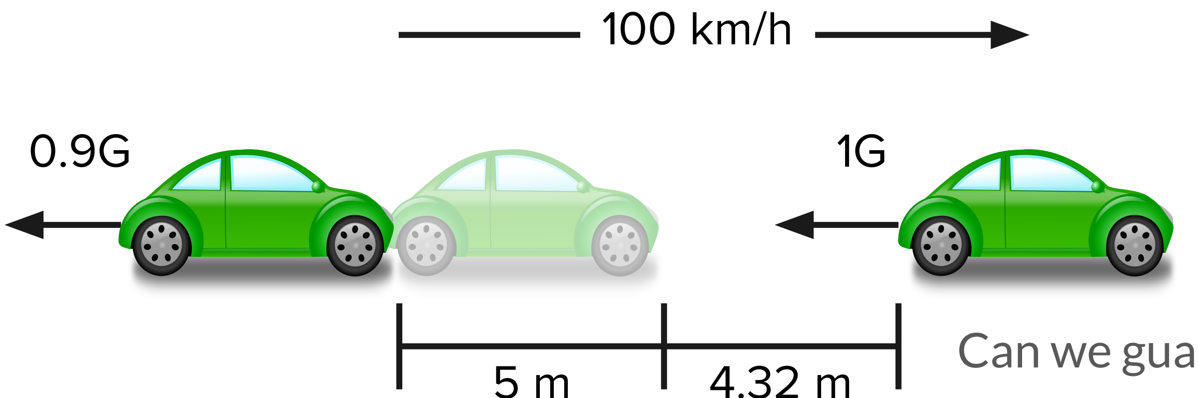
Reactive approach to sudden braking

In this circumstance, we need 4.32 meters of following distance for safety



Reactive approach to sudden braking

Every 172ms of follower delay = 5 meters of additional following distance



Can we guarantee safety and still platoon at suitable following distances?

Autonomous Vehicle Contracts

What if platooning vehicles agreed not to crash into one another?

Threat Model

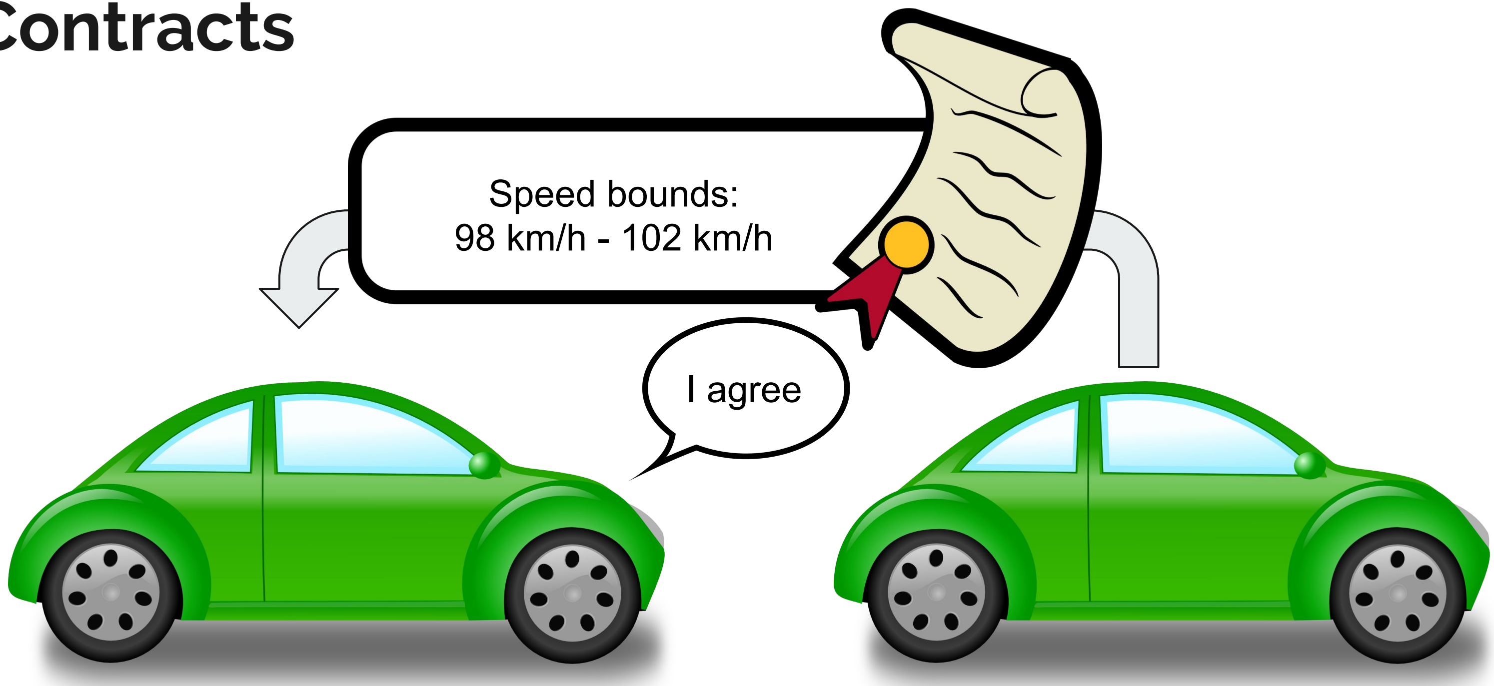
We assume the perspective of a human passenger in an autonomous vehicle.

You must trust your own vehicle

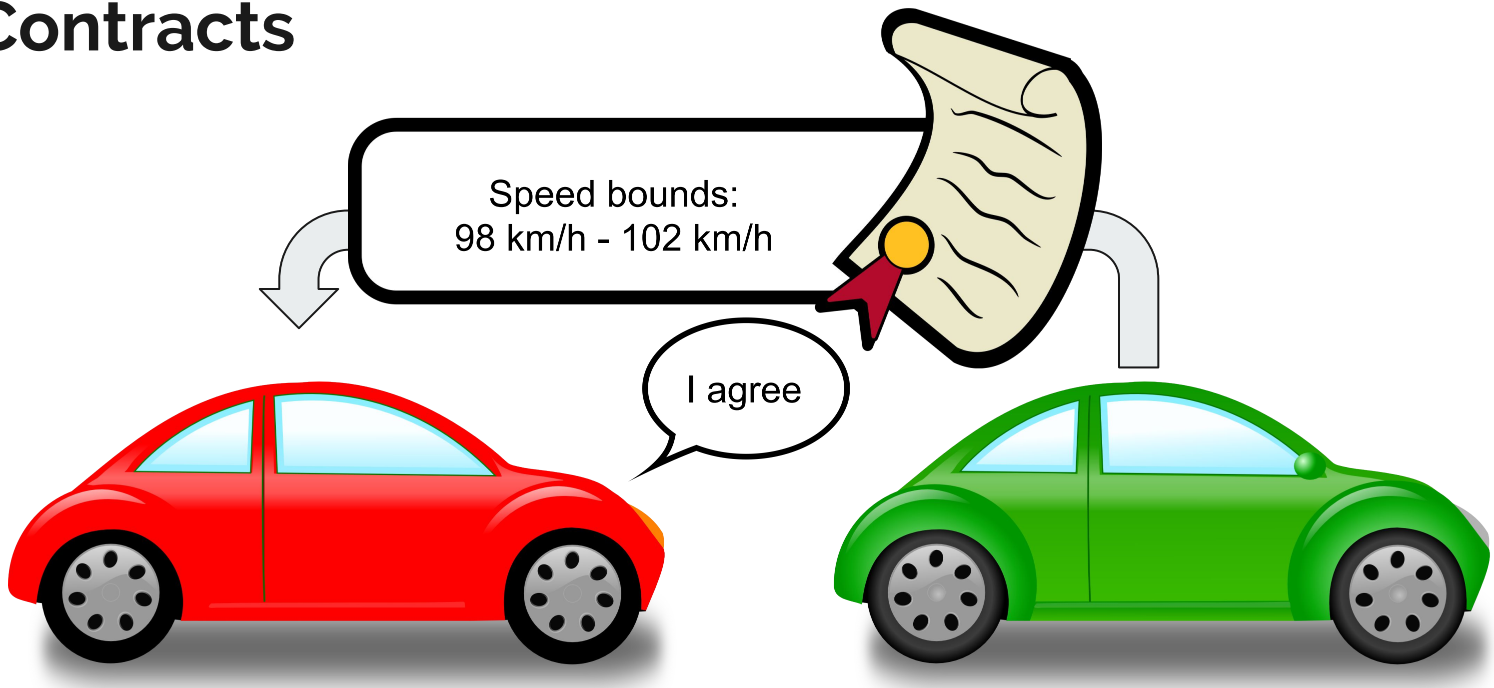
Any other vehicle in the platoon may be malicious

Malicious vehicles can accelerate and brake, send arbitrary network traffic, jam communications

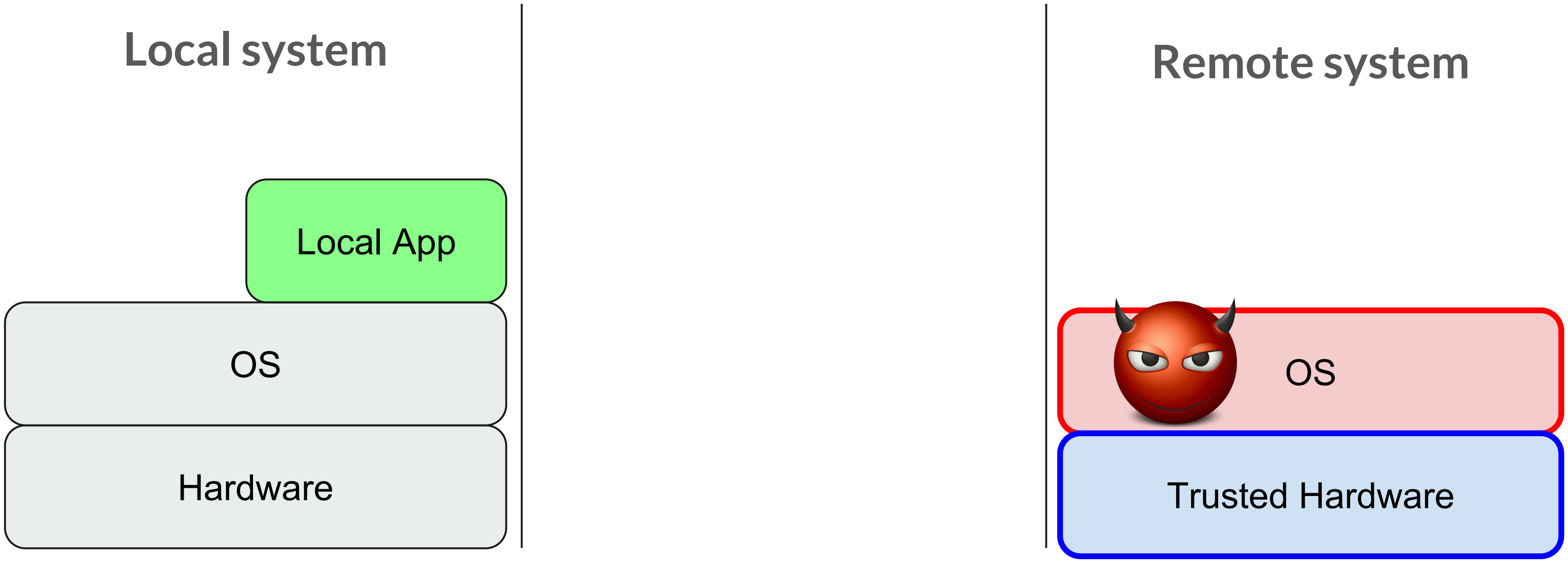
Contracts



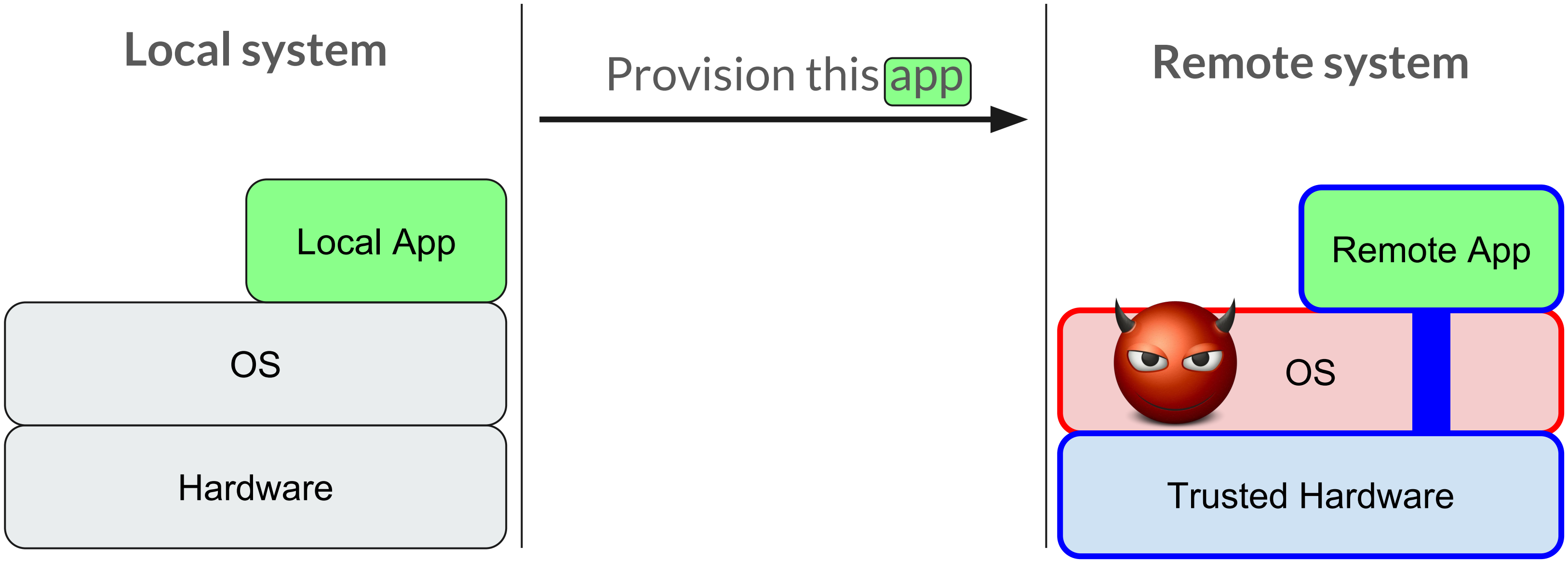
Contracts



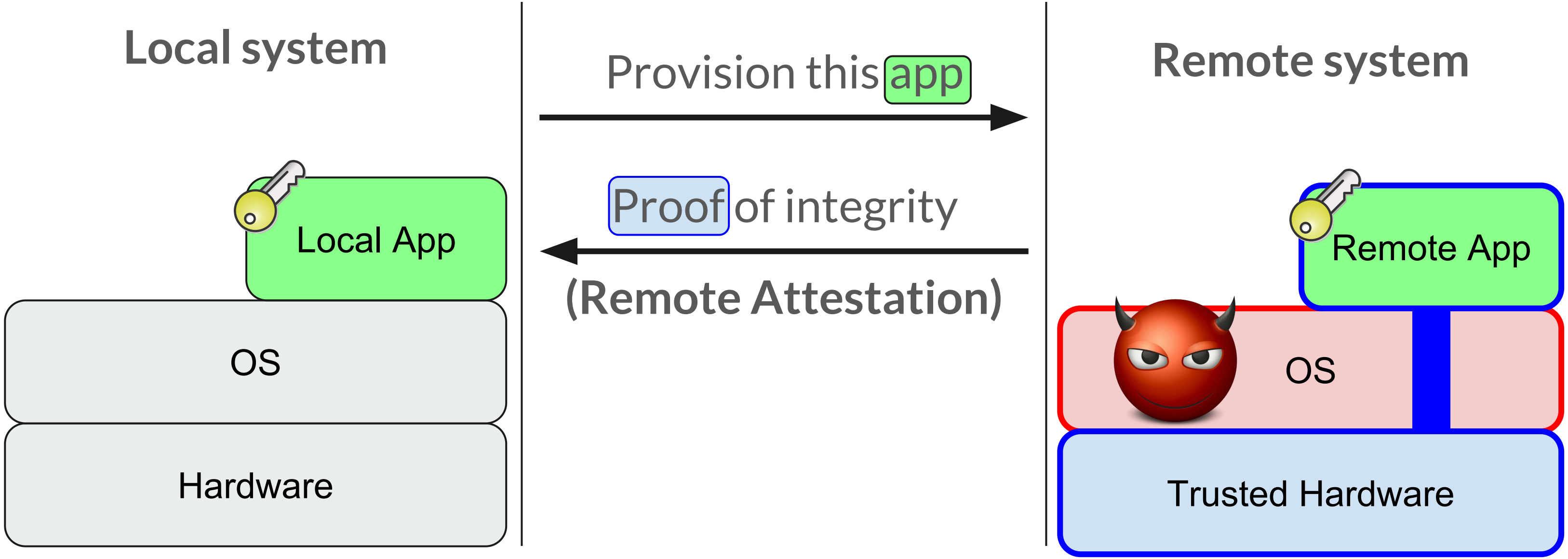
Background: Trusted execution with enclaves



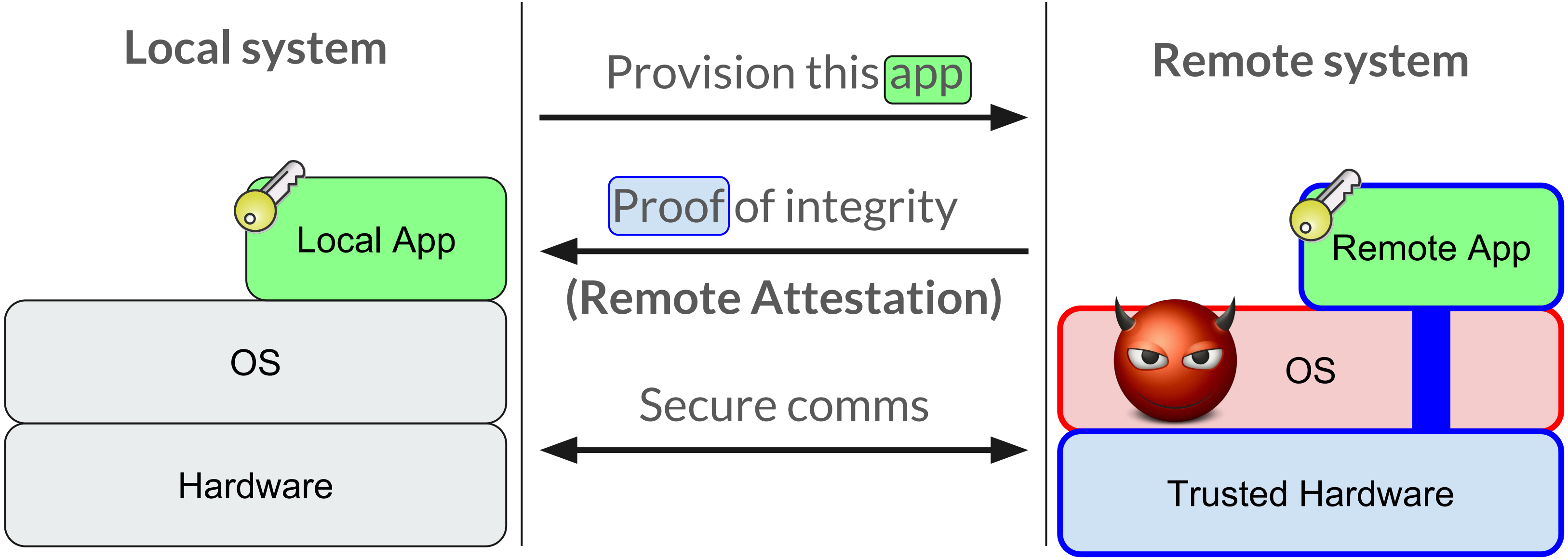
Background: Trusted execution with enclaves



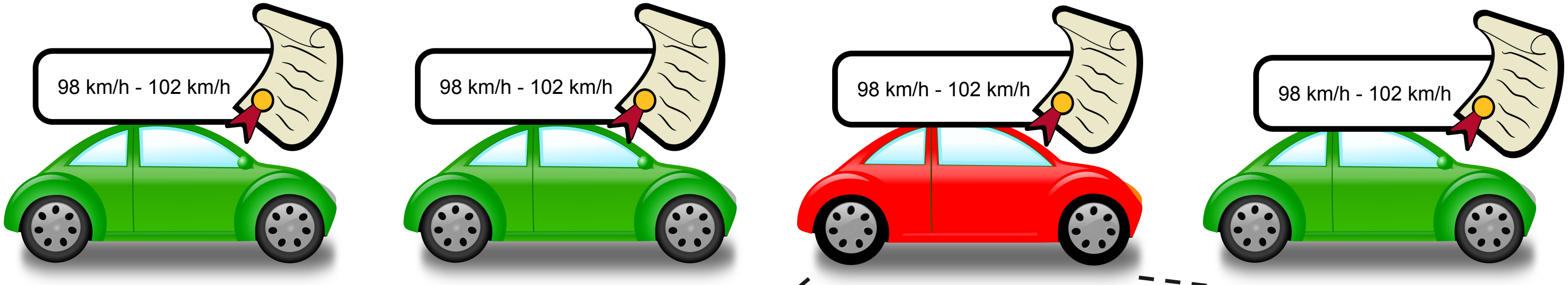
Background: Trusted execution with enclaves



Background: Trusted execution with enclaves

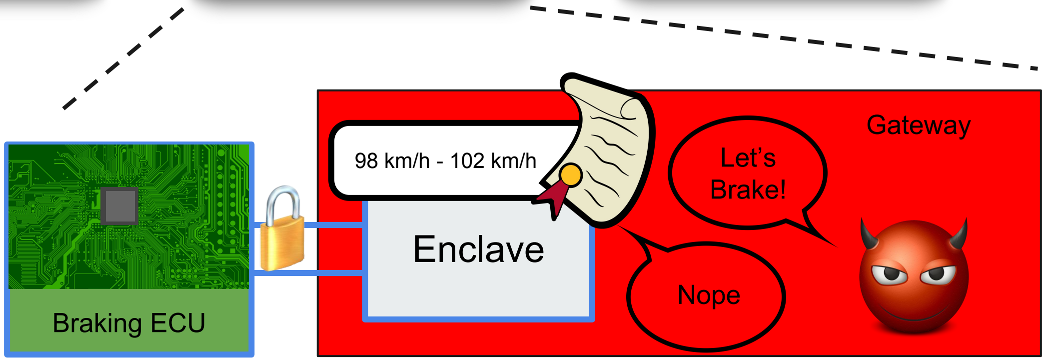


Use enclaves to *enforce* contract parameters

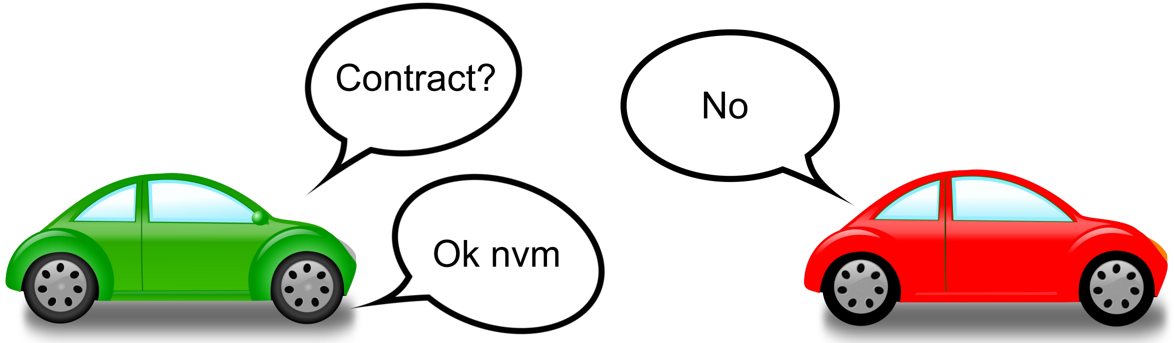


Enclave filters commands sent to the Powertrain/Braking ECUs

ECUs will ignore all commands not signed by the enclave



We can't force others to sign contracts

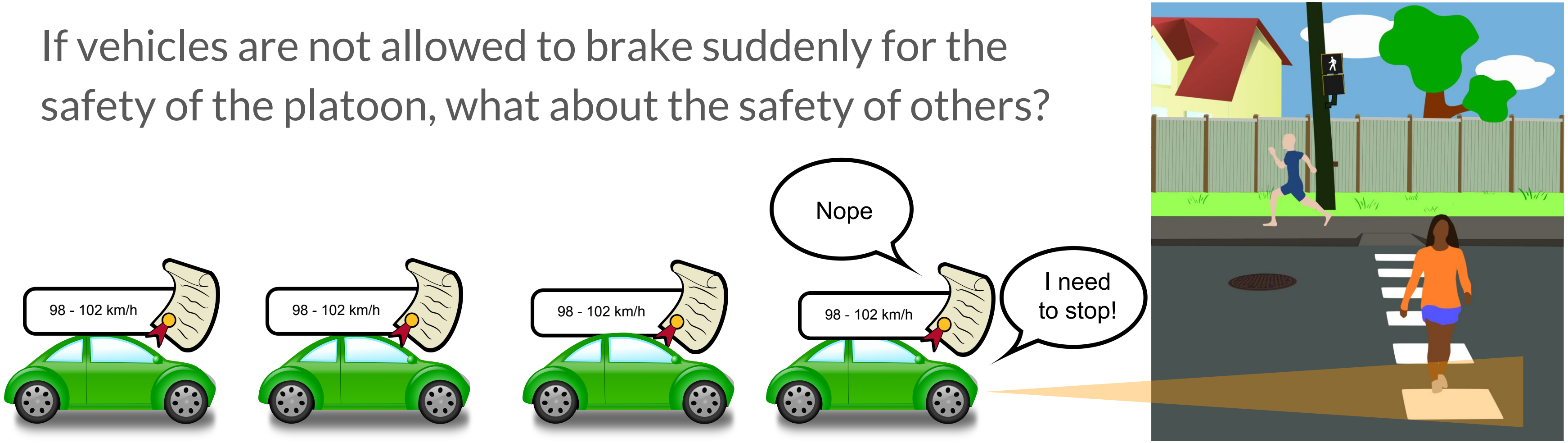


But we can refuse to form a platoon without a contract, retaining our safe separation distance

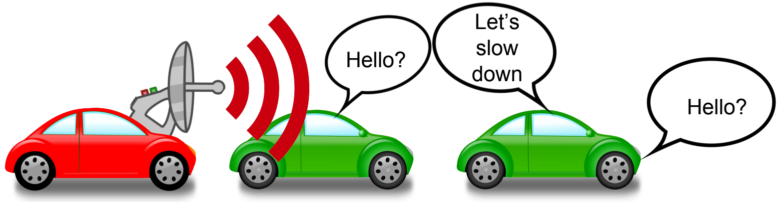
Once we do negotiate a contract, we can bound vehicle speed and acceleration

What happens if we *need* to brake?

If vehicles are not allowed to brake suddenly for the safety of the platoon, what about the safety of others?



In case of emergency…



Emergency Responsiveness

Attackers can jam communications, so vehicles cannot necessarily coordinate a response while still under contract

Therefore

We must allow vehicles to regain individual autonomy as soon as possible

Platoon Safety

A malicious vehicle could fabricate an "emergency" to void a contract while the platoon is still formed

Therefore

We can't release vehicles from contract until they have reached safe separation

On the feasibility of contracts

Can we terminate a contract quickly enough?

Goal: Separate and return autonomy in 1500 ms

How long does it take for current vehicles to react to an emergency?

Human Perception Response Time (PRT): ~1500 ms

If we can achieve vehicle separation and autonomy in a similar time frame, it may be considered sufficient emergency responsiveness

Goal: Separate and return autonomy in 1500 ms

How long does it take for current vehicles to react to an emergency?

Human Perception Response Time (PRT): ~1500 ms

If we can achieve vehicle separation and autonomy in a similar time frame, it may be considered sufficient emergency responsiveness

Phases of terminating a contract

1. Recovery Phase

Detect emergency or communications failure

Even if one vehicle detects an emergency, it may not be able to communicate this failure to the platoon

If communications fail, an a timeout must elapse before the platoon begins to separate

2. Separation Phase

Each vehicle must achieve a safe following distance before the contract can terminate

Without guaranteed communications, each vehicle must separate independently

Vehicle separation must remain coordinated to ensure safety

Separation Phase

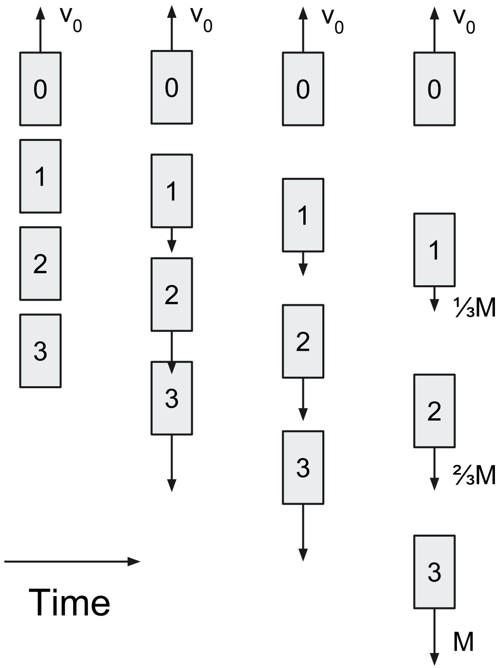
Goal: 1000 ms

Emergency Termination Procedure (ETP)

When the ETP is invoked, we wish to separate the platoon vehicles *as quickly as possible*

Communications may not be possible

We can **pre-program** a synchronized separation procedure into each vehicle in the event of communications failure



Separation Equation:

$$A_n = \frac{n}{N}M$$

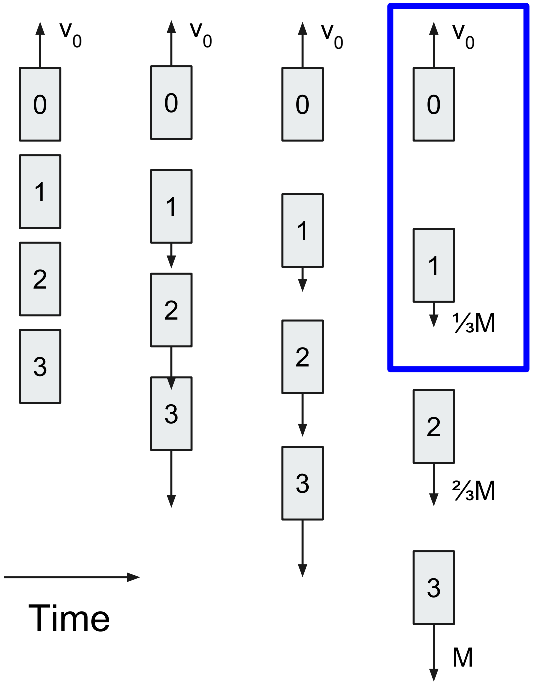
M: Maximum Deceleration
N: Highest Vehicle Index
n: Vehicle Index
A_n: Deceleration for specific vehicle

Emergency Termination Procedure (ETP)

When the ETP is invoked, we wish to separate the platoon vehicles *as quickly as possible*

Communications may not be possible

We can **pre-program** a synchronized separation procedure into each vehicle in the event of communications failure

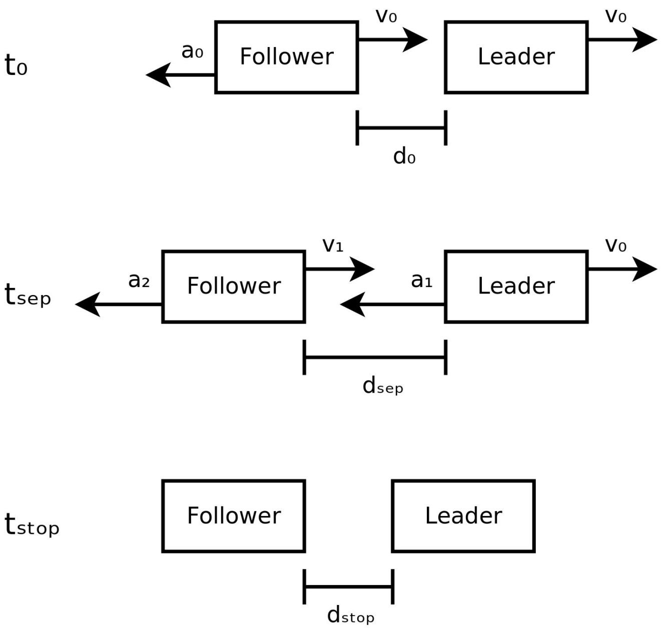


Separation Equation:

$$A_n = \frac{n}{N} M$$

M: Maximum Deceleration
N: Highest Vehicle Index
n: Vehicle Index
A_n: Deceleration for specific vehicle

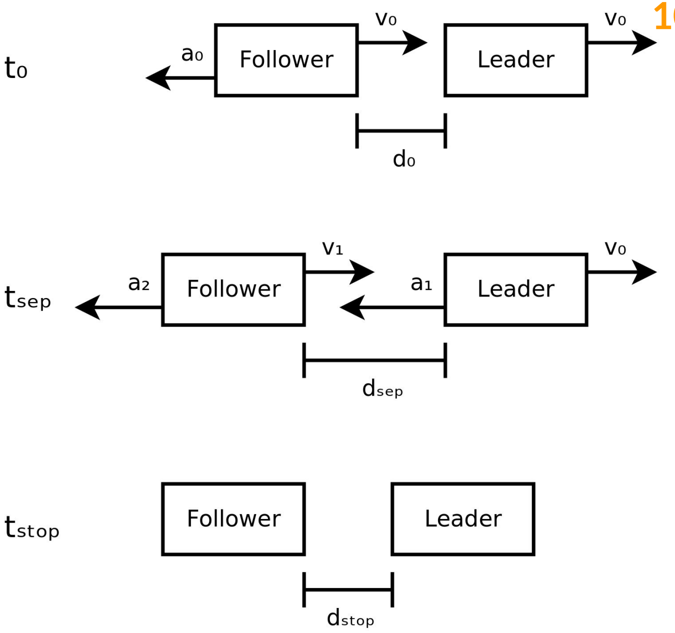
How long does separation take?



$$(a_0^2 a_1 - a_0 a_1 a_2)t_{sep}^2 + (2a_0 a_1 v_0)t_{sep} + v_0^2(a_1 - a_2) + 2a_1 a_2(d_0 - d_{stop}) = 0$$

Platoon Size	v_0 m/s	a_0 m/s^2	a_1 m/s^2	a_2 m/s^2	d_0 m	d_{stop} m	t_{sep} ms
2	27.77	-8.82	-9.81	-8.82	1.0	1.0	158
3	27.77	-4.41	-9.81	-8.82	1.0	1.0	307
4	27.77	-2.94	-9.81	-8.82	1.0	1.0	451
5	27.77	-2.20	-9.81	-8.82	1.0	1.0	594
6	27.77	-1.76	-9.81	-8.82	1.0	1.0	728
7	27.77	-1.47	-9.81	-8.82	1.0	1.0	867
8	27.77	-1.26	-9.81	-8.82	1.0	1.0	982

How long does separation take?

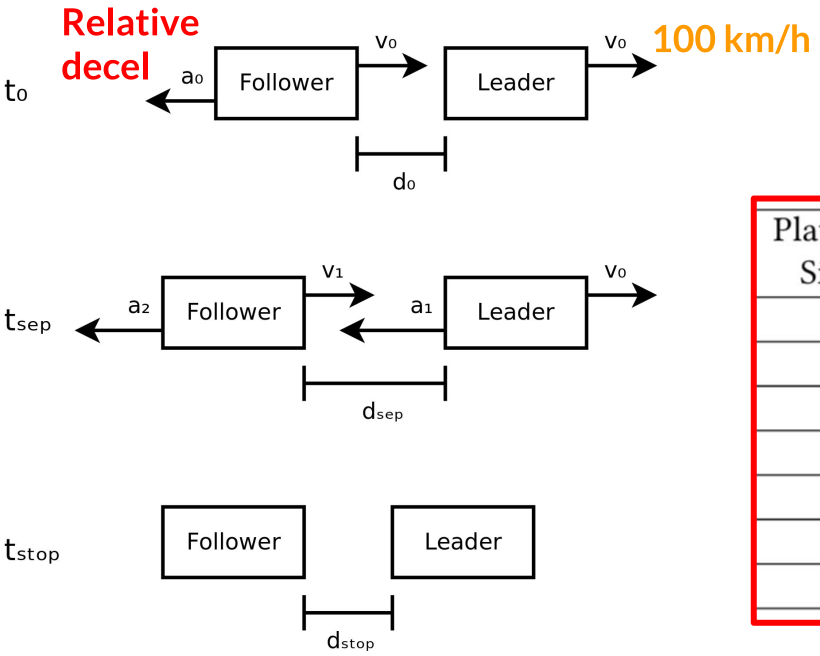


100 km/h

$$(a_0^2 a_1 - a_0 a_1 a_2) t_{sep}^2 + (2 a_0 a_1 v_0) t_{sep} +$$
$$v_0^2 (a_1 - a_2) + 2 a_1 a_2 (d_0 - d_{stop}) = 0$$

Platoon Size	v_0 m/s	a_0 m/s^2	a_1 m/s^2	a_2 m/s^2	d_0 m	d_{stop} m	t_{sep} ms
2	27.77	-8.82	-9.81	-8.82	1.0	1.0	158
3	27.77	-4.41	-9.81	-8.82	1.0	1.0	307
4	27.77	-2.94	-9.81	-8.82	1.0	1.0	451
5	27.77	-2.20	-9.81	-8.82	1.0	1.0	594
6	27.77	-1.76	-9.81	-8.82	1.0	1.0	728
7	27.77	-1.47	-9.81	-8.82	1.0	1.0	867
8	27.77	-1.26	-9.81	-8.82	1.0	1.0	982

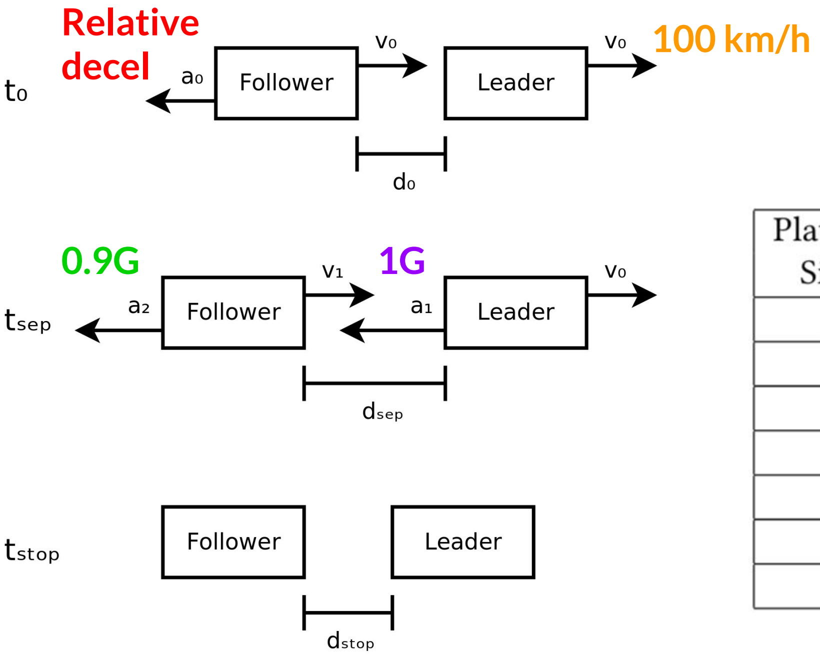
How long does separation take?



$$(a_0^2 a_1 - a_0 a_1 a_2) t_{sep}^2 + (2 a_0 a_1 v_0) t_{sep} + v_0^2 (a_1 - a_2) + 2 a_1 a_2 (d_0 - d_{stop}) = 0$$

Platoon Size	v_0 m/s	a_0 m/s^2	a_1 m/s^2	a_2 m/s^2	d_0 m	d_{stop} m	t_{sep} ms
2	27.77	-8.82	-9.81	-8.82	1.0	1.0	158
3	27.77	-4.41	-9.81	-8.82	1.0	1.0	307
4	27.77	-2.94	-9.81	-8.82	1.0	1.0	451
5	27.77	-2.20	-9.81	-8.82	1.0	1.0	594
6	27.77	-1.76	-9.81	-8.82	1.0	1.0	728
7	27.77	-1.47	-9.81	-8.82	1.0	1.0	867
8	27.77	-1.26	-9.81	-8.82	1.0	1.0	982

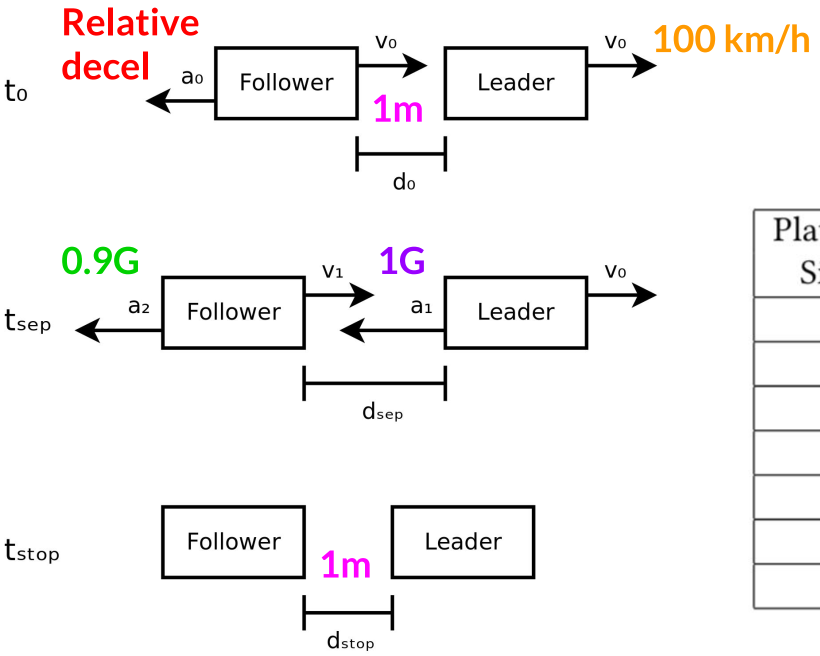
How long does separation take?



$$(a_0^2 a_1 - a_0 a_1 a_2) t_{sep}^2 + (2 a_0 a_1 v_0) t_{sep} + v_0^2 (a_1 - a_2) + 2 a_1 a_2 (d_0 - d_{stop}) = 0$$

Platoon Size	v_0 m/s	a_0 m/s^2	a_1 m/s^2	a_2 m/s^2	d_0 m	d_{stop} m	t_{sep} ms
2	27.77	-8.82	-9.81	-8.82	1.0	1.0	158
3	27.77	-4.41	-9.81	-8.82	1.0	1.0	307
4	27.77	-2.94	-9.81	-8.82	1.0	1.0	451
5	27.77	-2.20	-9.81	-8.82	1.0	1.0	594
6	27.77	-1.76	-9.81	-8.82	1.0	1.0	728
7	27.77	-1.47	-9.81	-8.82	1.0	1.0	867
8	27.77	-1.26	-9.81	-8.82	1.0	1.0	982

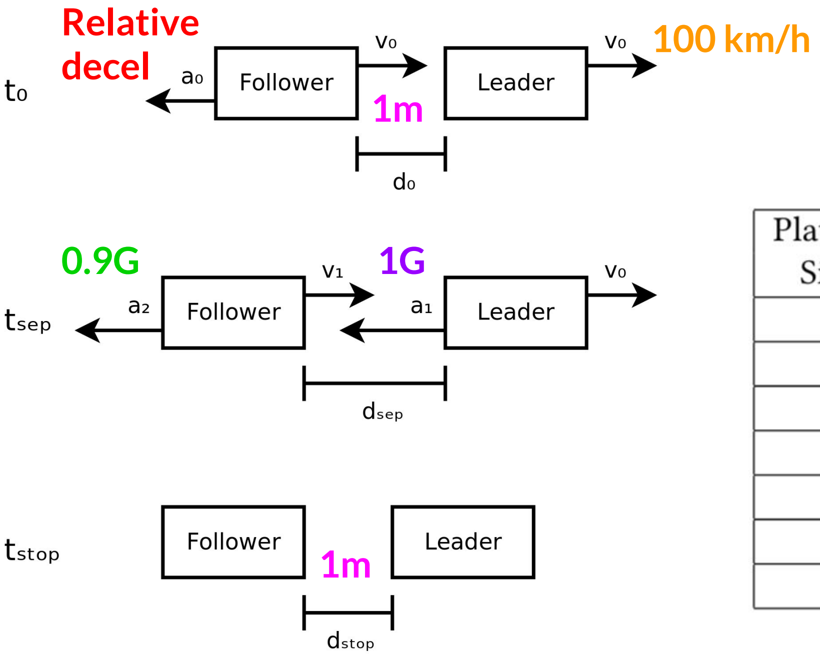
How long does separation take?



$$(a_0^2 a_1 - a_0 a_1 a_2) t_{sep}^2 + (2 a_0 a_1 v_0) t_{sep} + \\ v_0^2 (a_1 - a_2) + 2 a_1 a_2 (d_0 - d_{stop}) = 0$$

Platoon Size	v_0 m/s	a_0 m/s^2	a_1 m/s^2	a_2 m/s^2	d_0 m	d_{stop} m	t_{sep} ms
2	27.77	-8.82	-9.81	-8.82	1.0	1.0	158
3	27.77	-4.41	-9.81	-8.82	1.0	1.0	307
4	27.77	-2.94	-9.81	-8.82	1.0	1.0	451
5	27.77	-2.20	-9.81	-8.82	1.0	1.0	594
6	27.77	-1.76	-9.81	-8.82	1.0	1.0	728
7	27.77	-1.47	-9.81	-8.82	1.0	1.0	867
8	27.77	-1.26	-9.81	-8.82	1.0	1.0	982

How long does separation take?



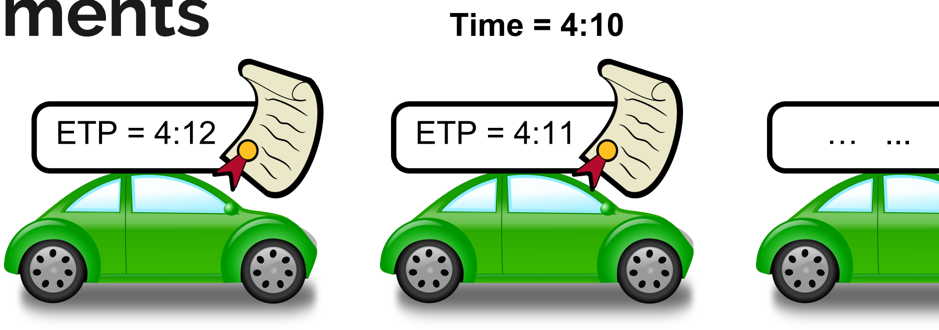
$$\boxed{\begin{aligned}(a_0^2 a_1 - a_0 a_1 a_2)t_{sep}^2 + (2a_0 a_1 v_0)t_{sep} + \\ v_0^2(a_1 - a_2) + 2a_1 a_2(d_0 - d_{stop}) = 0\end{aligned}}$$

Platoon Size	v_0 m/s	a_0 m/s^2	a_1 m/s^2	a_2 m/s^2	d_0 m	d_{stop} m	t_{sep} ms
2	27.77	-8.82	-9.81	-8.82	1.0	1.0	158
3	27.77	-4.41	-9.81	-8.82	1.0	1.0	307
4	27.77	-2.94	-9.81	-8.82	1.0	1.0	451
5	27.77	-2.20	-9.81	-8.82	1.0	1.0	594
6	27.77	-1.76	-9.81	-8.82	1.0	1.0	728
7	27.77	-1.47	-9.81	-8.82	1.0	1.0	867
8	27.77	-1.26	-9.81	-8.82	1.0	1.0	982

Recovery Phase

Goal: 500 ms

Synchronization Requirements

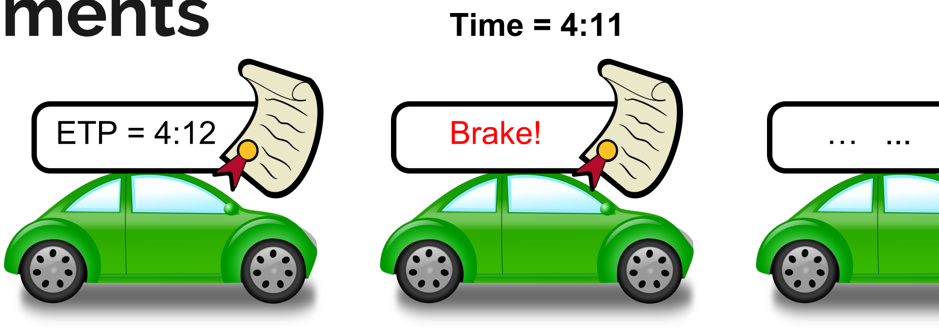


The ETP assumes vehicles are synchronized

If the ETP starts at different times for different vehicles, it could be catastrophic

Full synchronization across an untrustworthy communication channel cannot be guaranteed

Synchronization Requirements

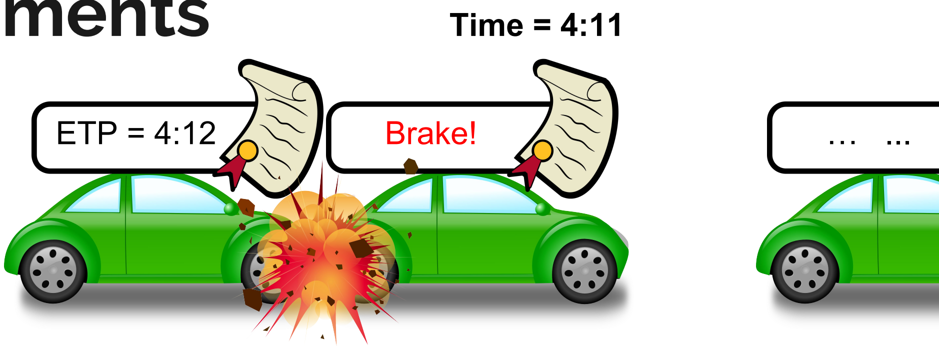


The ETP assumes vehicles are synchronized

If the ETP starts at different times for different vehicles, it could be catastrophic

Full synchronization across an untrustworthy communication channel cannot be guaranteed

Synchronization Requirements

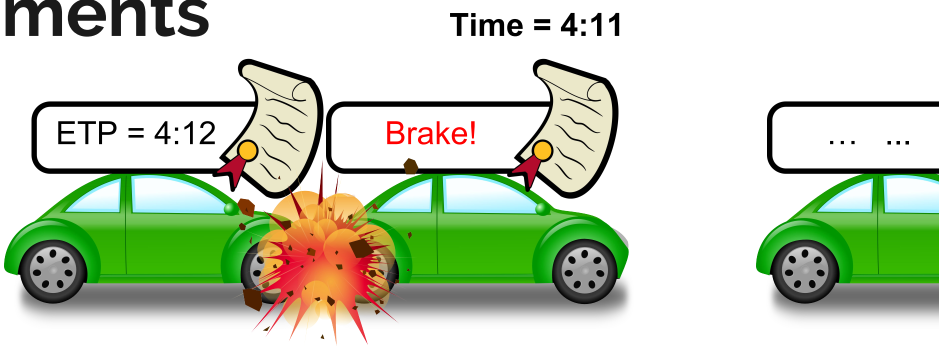


The ETP assumes vehicles are synchronized

If the ETP starts at different times for different vehicles, it could be catastrophic

Full synchronization across an untrustworthy communication channel cannot be guaranteed

Synchronization Requirements



The ETP assumes vehicles are synchronized

If the ETP starts at different times for different vehicles, it could be catastrophic

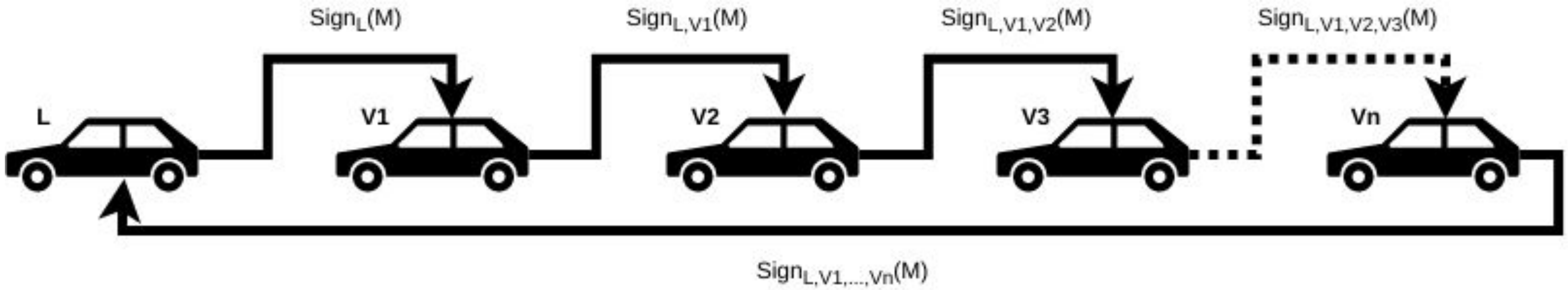
Full synchronization across an untrustworthy communication channel cannot be guaranteed

Key insight: A vehicle must start the ETP **no later than** any preceding vehicle

Contract Chain

During the Recovery Phase, the leader will periodically extend the contract's recovery phase timeout with a contract chain

The enclave will ensure that each vehicle's ECU updates the timeout *before* the enclave will sign the contract chain, and these signatures are passed *in order* to each vehicle in the platoon



Setting the ETP timeout

Goal #1: minimize the ETP timeout

Goal #2: support intermittent packet loss without invoking the ETP

Due to packet loss and intermittent connectivity issues, some contract chains may fail

Platoon size affects the latency (number of hops) for a contract chain to complete

The chance for a false positive can be calculated probabilistically

Packet loss rate vs. ETP timeout

Packet Loss Rate	Platoon Size	Chance of Termination per 1,000,000 Recovery Chains							
		3 Failed Recoveries		5 Failed Recoveries		8 Failed Recoveries		16 Failed Recoveries	
0.01%	2	7.9972e-6	✓	3.1985e-13	✓	2.5584e-24	✓	6.5470e-54	✓
0.01%	4	6.3943e-5	✗	1.0228e-11	✓	6.5431e-22	✓	4.2829e-49	✓
0.01%	6	2.1568e-4	✗	7.7616e-11	✓	1.6752e-20	✓	2.8081e-46	✓
0.01%	8	5.1092e-4	✗	3.2684e-10	✓	1.6717e-19	✓	2.7968e-44	✓
0.1%	2	0.0079403	✗	3.1856e-8	✓	2.5447e-16	✓	6.4883e-38	✓
0.1%	4	0.061487	✗	1.0123e-6	✓	6.4495e-14	✓	4.1763-33	✓
0.1%	6	0.19193	✗	7.6334e-6	✓	1.6365e-12	✓	2.6942e-30	✓
0.1%	8	0.39505	✗	3.1942e-5	✗	1.6184e-11	✓	2.6402e-28	✓
1%	2	0.99956	✗	0.0030540	✗	2.4104e-8	✓	5.9281e-22	✓
1%	4	1	✗	0.087212	✗	5.5829e-6	✓	3.2447e-17	✓
1%	6	1	✗	0.47594	✗	1.2948e-4	✗	1.7810e-14	✓
1%	8	1	✗	0.92108	✗	0.0011702	✗	1.4857e-12	✓
5%	2	1	✗	0.9965	✗	0.0073431	✗	6.0189e-11	✓
5%	4	1	✗	1	✗	0.68071	✗	1.6001e-6	✓
5%	6	1	✗	1	✗	1	✗	4.3228e-4	✗
5%	8	1	✗	1	✗	1	✗	0.017835	✗

Packet loss rate vs. ETP timeout

Increasing # contract chains →

Increasing packet loss rate and platoon size ↓

Packet Loss Rate	Platoon Size	3 Failed Re[illegible]		[illegible]		[illegible]		[illegible]ecoveries	
0.01%	2	7.99[illegible]2e-6	✓	3.1985e-13	✓	2.5584e-24	✓	6.5470e-54	✓
0.01%	4	6.3943e-[illegible]	✗	1.0228e-11	✓	6.5431e-22	✓	4.2829e-49	✓
0.01%	6	2.1568e-4	✗	7.7616e-11	✓	[illegible]	[illegible]	[illegible]46	✓
0.01%	8	5.1092e-4	✗	3.2684e-10	[illegible]	[illegible]	[illegible]	[illegible]44	✓
0.1%	2	0.0079403	✗	3.18[illegible]e-8	[illegible]	[illegible]	✓	6.4883e-38	✓
[illegible]	[illegible]	[illegible]7	✗	1.0123e-6	✓	6.4495e-14	✓	4.1763-33	✓
[illegible]	[illegible]	[illegible]	✗	7.6334e-6	✓	1.6365e-12	✓	2.6942e-30	✓
[illegible]	[illegible]	[illegible]	✗	3.1942e-5	✗	1.6184e-11	✓	2.6402e-28	✓
[illegible]	[illegible]	[illegible]	✗	0.0030540	✗	2.41[illegible]e-8	✓	5.9281e-22	✓
[illegible]	[illegible]	[illegible]	✗	0.087212	✗	5.5829e-6	✓	3.2447e-17	✓
1%	6	1	✗	0.47594	✗	1.2948e-4	✗	1.7810e-14	✓
1%	8	1	✗	[illegible]	[illegible]	[illegible]0011702	✗	1.4857e-12	✓
5%	2	1	[illegible]	[illegible]	[illegible]	[illegible]0073431	✗	6.01[illegible]e-11	✓
5%	4	1	[illegible]	1	✗	0.68071	✗	1.6001e-6	✓
5%	6	1	✗	1	✗	1	✗	4.3228e-4	✗
5%	8	1	✗	1	✗	1	✗	0.017835	✗

Low false positive

High false positive

How long do contract chains take?

Can we complete enough chains within 500 ms to avoid false positives?

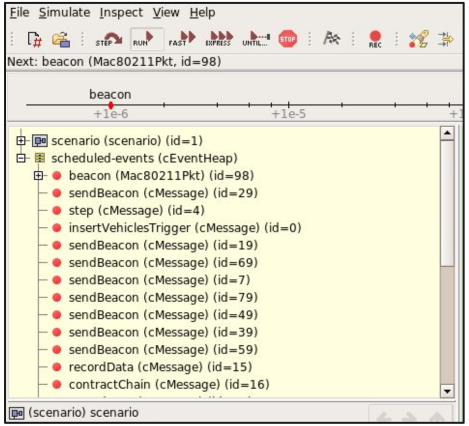
Platooning simulation

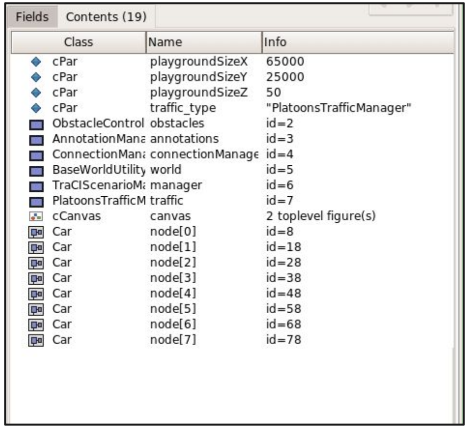
Our main evaluation platform is PLEXE,
a platooning extension for the Veins simulator,
running on an SGX-enabled supermicro server
http://plexe.car2x.org/

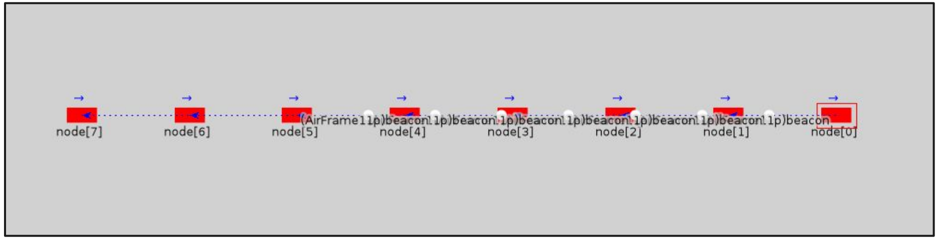
We have extended PLEXE to add an SGX enclave to each simulated vehicle

Any attempt to change vehicle speeds is governed by the CommPact enclave

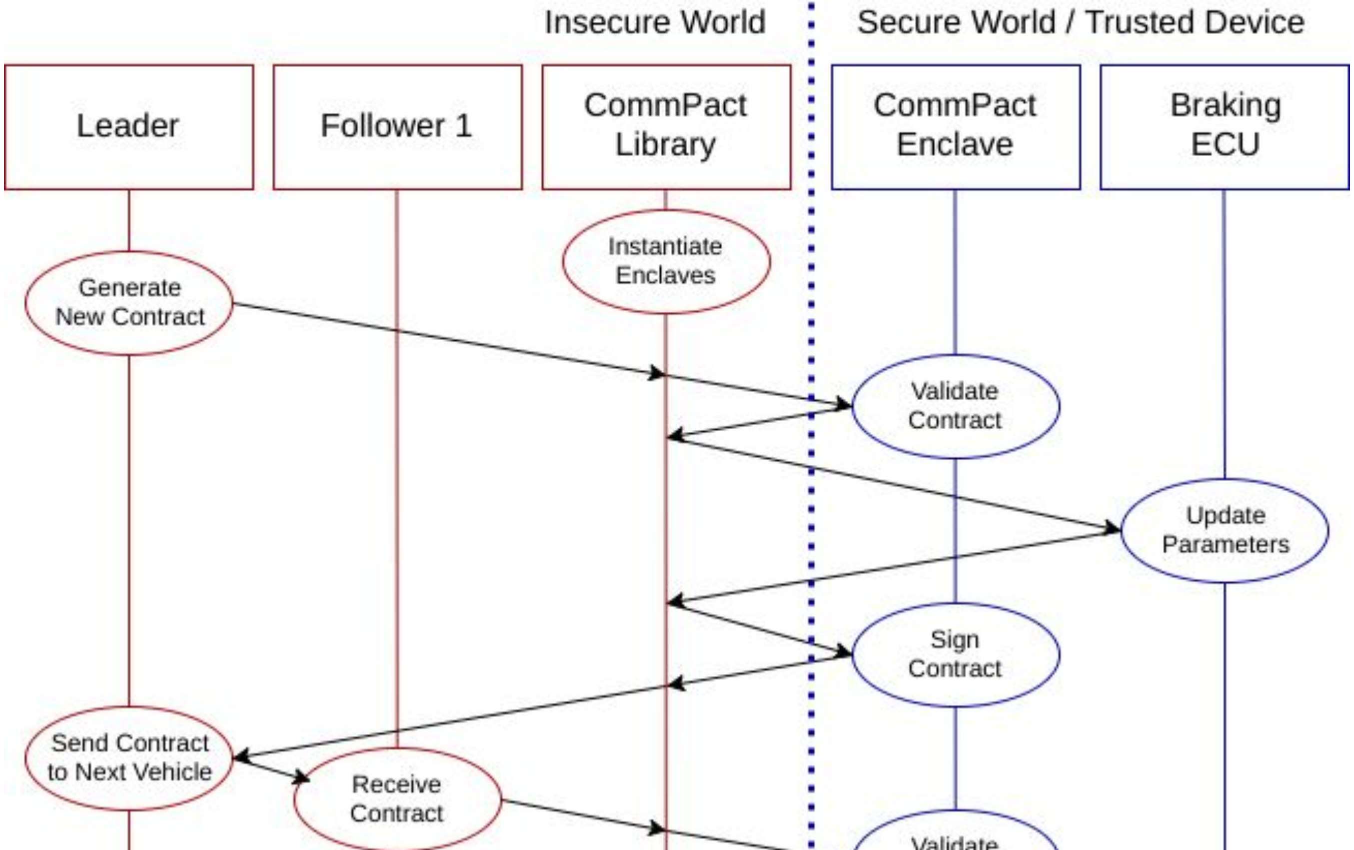
We can use this to approximate the latency of the overall contract chain, including enclave overhead



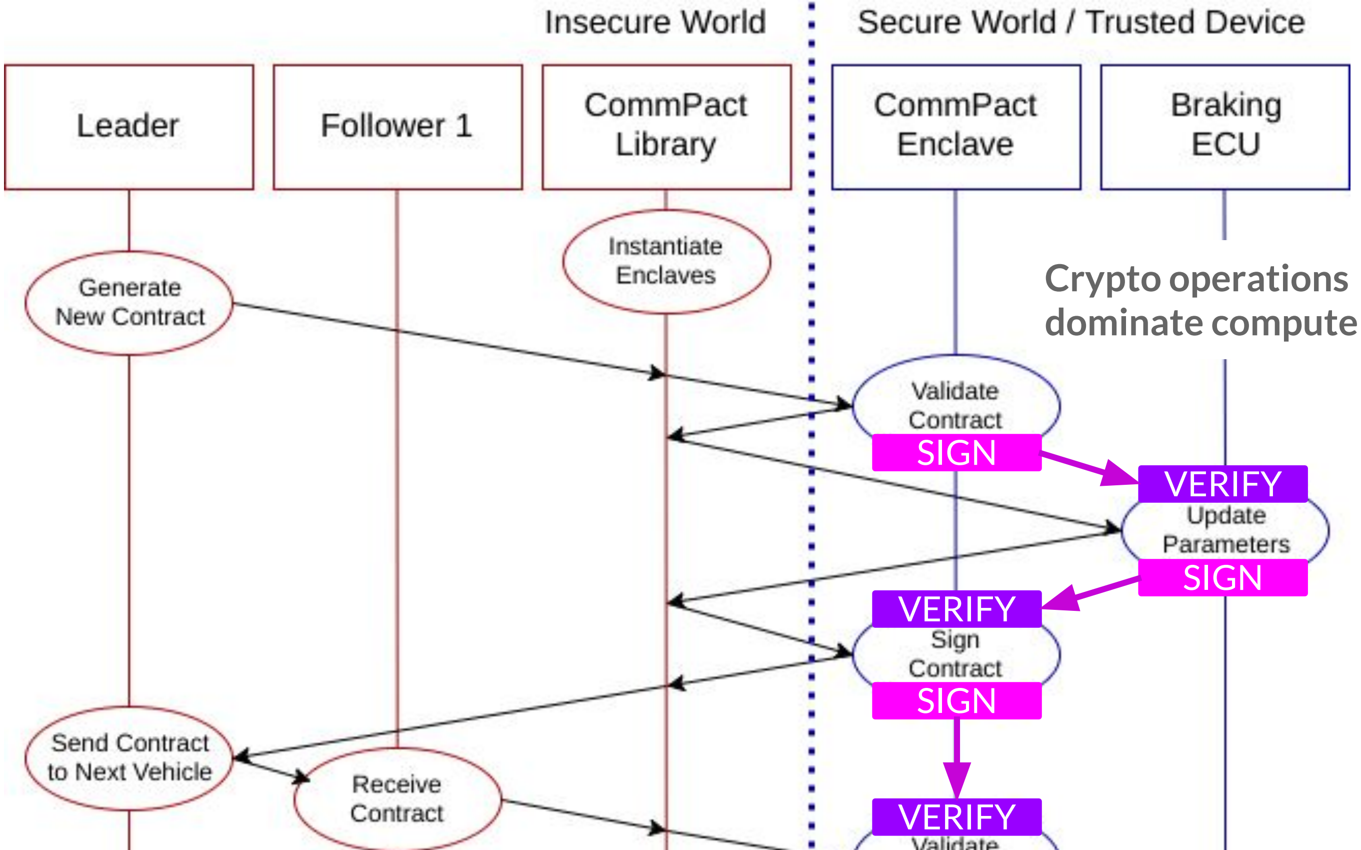




Critical Path

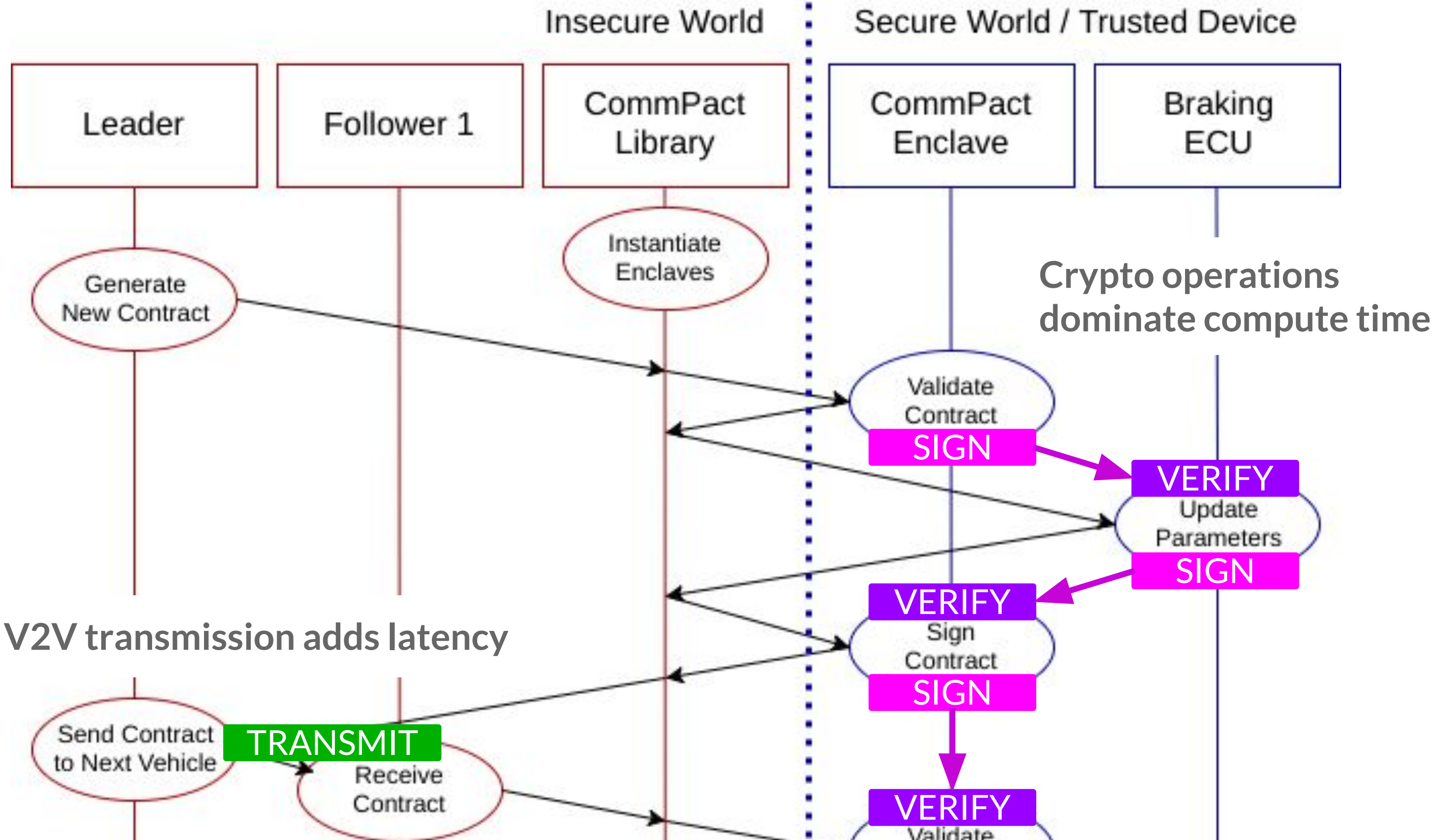


Critical Path



Crypto operations dominate compute time

Critical Path



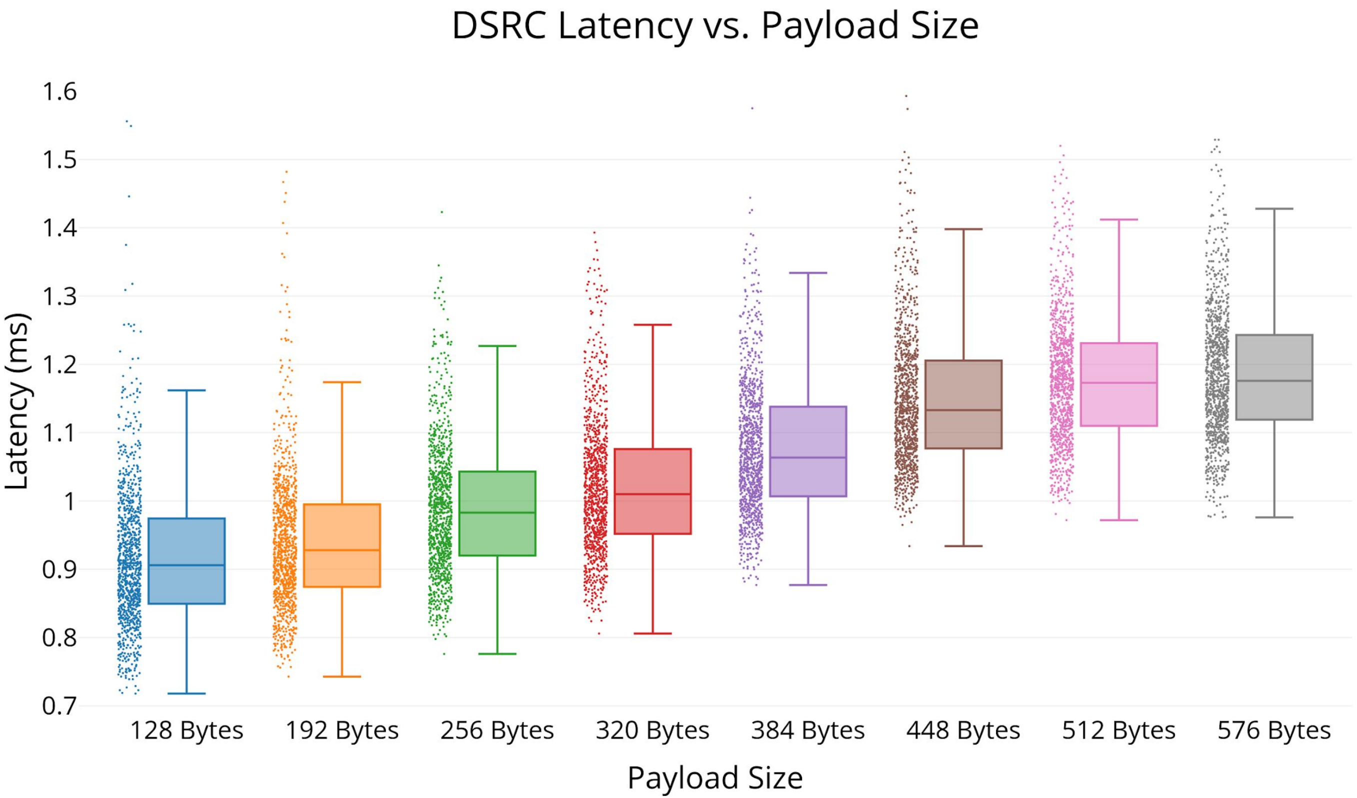
V2V latency measurements

We use Direct Short Range Communications (DSRC) in our prototype.

We performed latency measurements using two Cohda MK5 On-Board Units (OBUs).

Measured latency for 1000 round trips with packet sizes ranging from 128 to 576 bytes at distances between 1 meter and ~7 car-lengths.

DSRC latency measurements



Distance had a small and inconclusive impact on latency

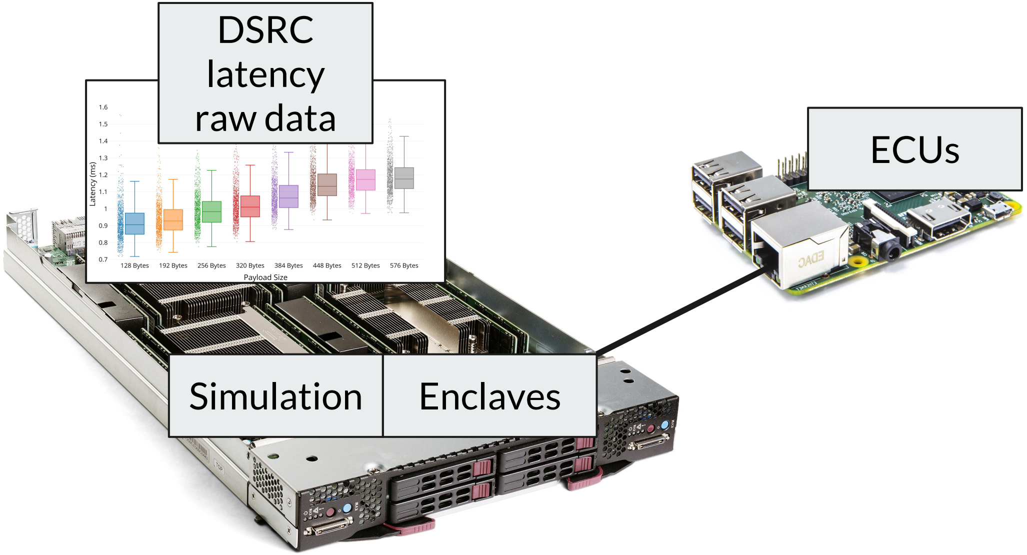
Simulation setup

Supermicro X11SSZ-QF motherboard w/ Intel Core I7-6700K 4.0 GHz

ECUs emulated with Raspberry Pi 3B+ connected over Fast Ethernet

Actual compute time for contract chain critical path is measured and recorded

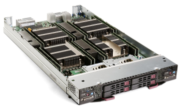
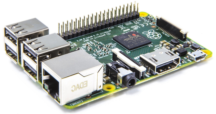
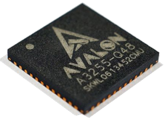
Measured DSRC latency data is fed into the simulation as well



Evaluation hardware vs. state of the art

Crypto operations in software dominate our overall compute time

ECDSA Sign and Verify operations over the NIST P-256 (secp256r1) curve

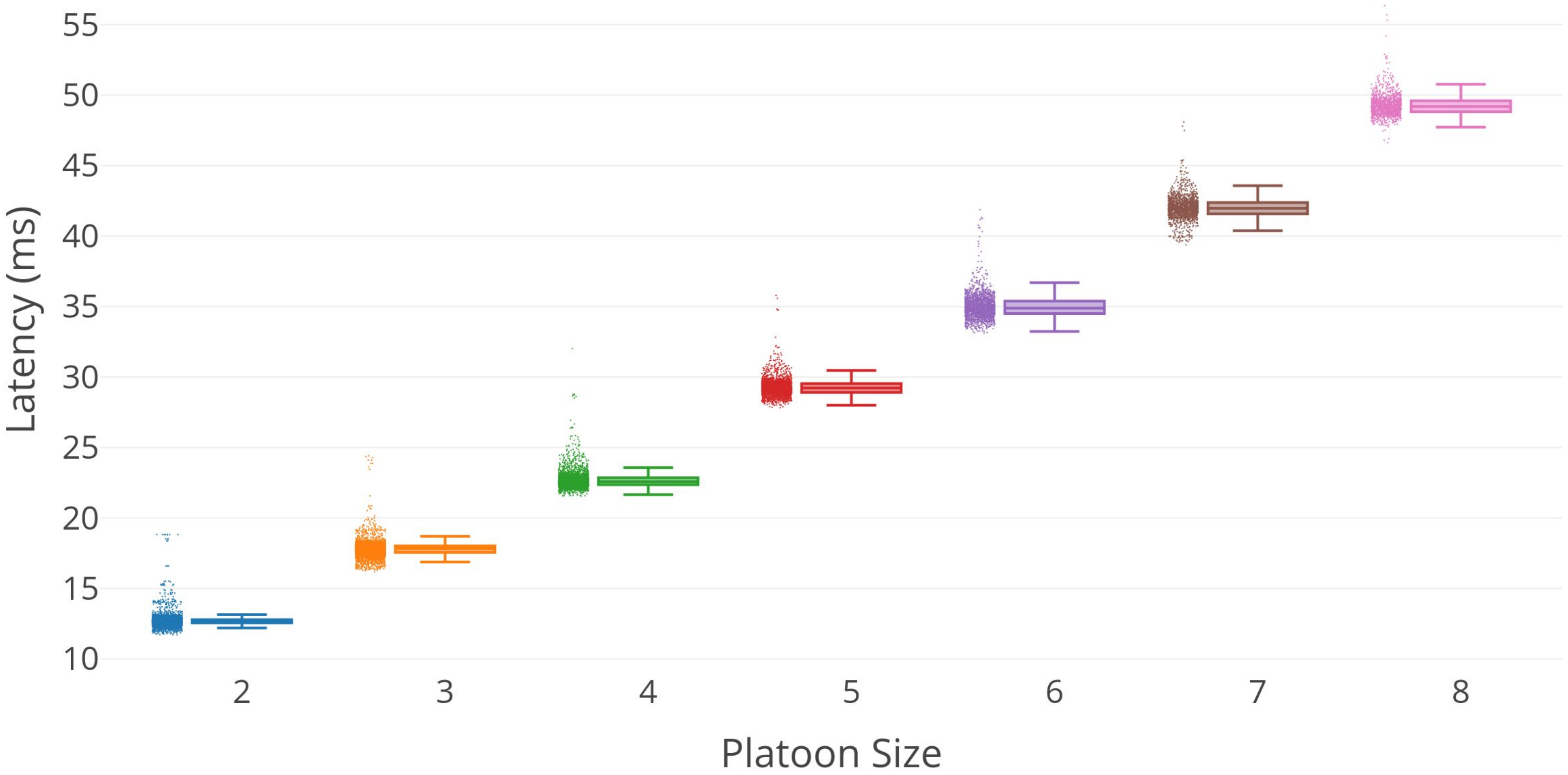




Operation	i7-6700K	RPI 3B+	ASIC
Sign	0.192 ms	0.709 ms	0.325 ms [1]
Verify	0.321 ms	1.321 ms	0.212 ms [2]

[1] M. Tamura and M. Ikeda, "1.68μJ/signature-generation 256-bit ECDSA over GF(p) signature generator for IoT devices," 2016 IEEE Asian Solid-State Circuits Conference (A-SSCC), 2016

[2] M. Knežević, V. Nikov and P. Rombouts, "Low-Latency ECDSA Signature Verification—A Road Toward Safer Traffic," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2016

Simulated Contract Chain Latency



Final results

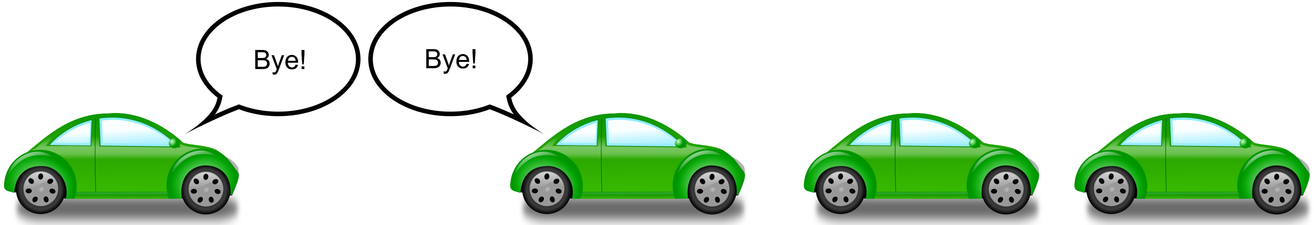
Platoon Size	# Chains	FP Rate per 10 hours	Recovery Phase	Separation Phase	Total Delay
2	7	0.00034%	89 ms	158 ms	247 ms
3	8	0.00012%	142 ms	307 ms	449 ms
4	8	0.00089%	181 ms	451 ms	632 ms
5	9	0.00019%	263 ms	594 ms	857 ms
6	9	0.00078%	315 ms	728 ms	1043 ms
7	10	0.00017%	420 ms	867 ms	1287 ms
8	10	0.00051%	493 ms	982 ms	1475 ms

What if the delay is too long?

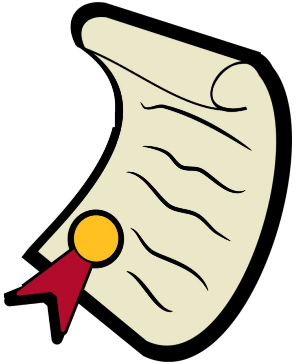
We can split the platoon!

The contract chain RTT and separation time are approximately linear to the # of vehicles in the platoon

We can keep the overall delay within acceptable bounds, whatever they may be, during changing conditions by adjusting the platoon length



Conclusion



New proposal: autonomous vehicle contracts

Can prevent malicious vehicles from causing platooning collisions

Requires careful balance of risk factors, but these factors can be mitigated

Ultimately, more work is needed to further investigate and develop AV Contracts

Questions?

Thank You

Other details

All images used in this presentation were original content, public domain, licensed under the CC0 non-attribution license, or are credited here.

https://upload.wikimedia.org/wikipedia/commons/3/3d/Raspberry_PI.jpeg

https://upload.wikimedia.org/wikipedia/commons/d/d0/Supermicro_SBI-7228R-T2X_blade_server.jpg

https://upload.wikimedia.org/wikipedia/commons/f/f0/Avalon_ASIC_A3255.png