CRITIX
RESEARCH GROUP

Confirmed-Location Group Membership for Intrusion-Resilient Cooperative Maneuvers

Júlio Mendonça, Azin Bayrami Asl, Federico Lucchetti, Marcus Völp
julio.mendonca@uni.lu, azin.bayramiasl@uni.lu, federico.lucchetti@unil.ch, marcus.voelp@uni.lu

12 September 2024

UNIVERSITY OF LUXEMBOURG
UNIL | Université de Lausanne

Motivation

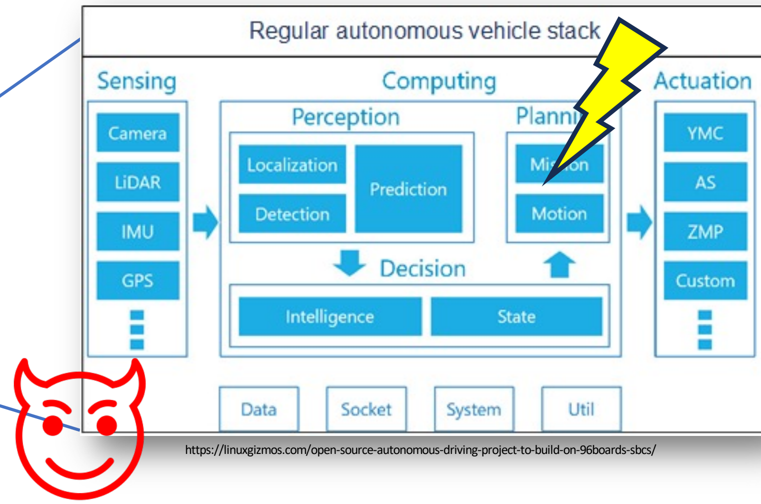
Connected Autonomous Vehicles

Autonomous Vehicles

https://www.techaheadcorp.com/blog/self-driving-cars-development/

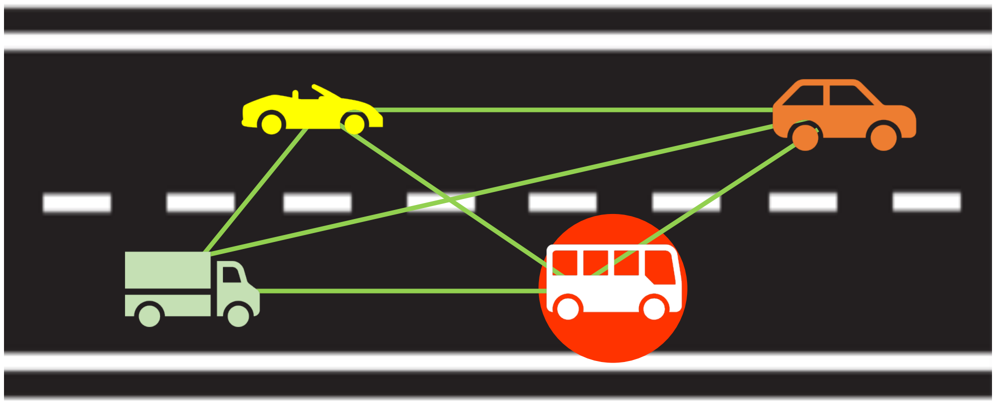
https://medium.com/@recogni/autonomous-vehicles-and-a-system-of-connected-cars-944f86275663

Faults and attacks can compromise vehicles



https://linuxgizmos.com/open-source-autonomous-driving-project-to-build-on-96boards-sbcs/

Challenges

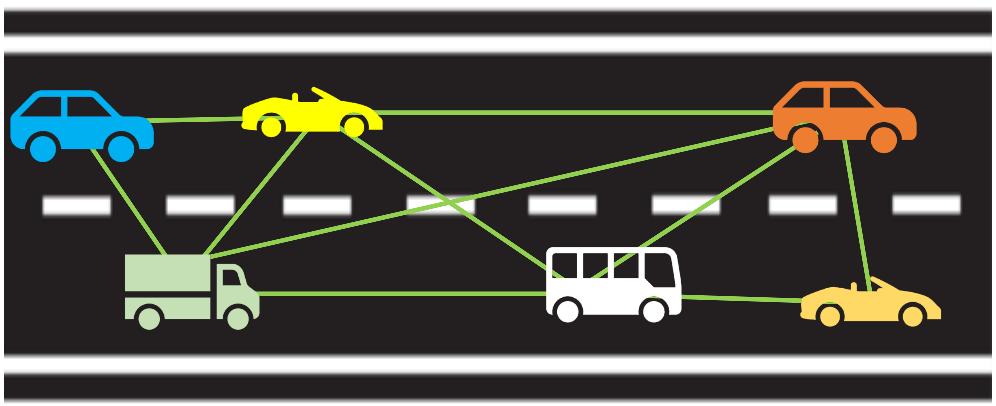


Current consensus algorithms (e.g., Damysus [9]) assume a fixed number of nodes *N*

Pre-defining how many faulty nodes ***f*** the system can tolerate, we can derive ***N*** (or vice-versa)

[9] J. Decouchant, D. Kozhaya, V. Rahli, and J. Yu, "DAMYSUS: streamlined BFT consensus leveraging trusted components," in Proceedings of the 17th European Conference on Computer Systems, 2022, pp. 1–16.

Challenges



Current consensus algorithms (e.g., Damysus [9]) assume a fixed number of nodes *N*

Pre-defining how many faulty nodes f the system can tolerate, we can derive ***N*** (or vice-versa)

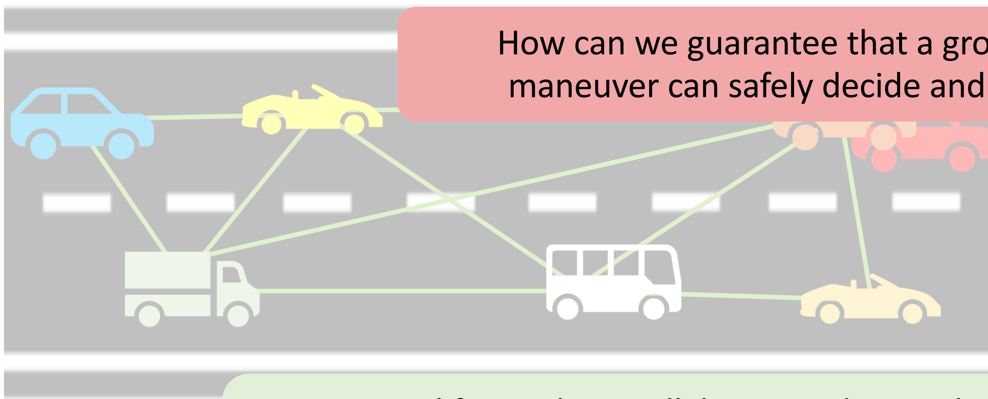
Driving scenarios are dynamic

How to define N and f, in these cases?

[9] J. Decouchant, D. Kozhaya, V. Rahli, and J. Yu, “DAMYSUS: streamlined BFT consensus leveraging trusted components,” in Proceedings of the 17th European Conference on Computer Systems, 2022, pp. 1–16.

Challenges

Current consensus algorithms (e.g., Damysus [9]) assume a fixed number of nodes N



How can we guarantee that a group of vehicles participating in a maneuver can safely decide and compute a correct maneuver?

...lty nodes f the system can tolerate, we can derive N (or vice-versa)

Driving scenarios are dynamic

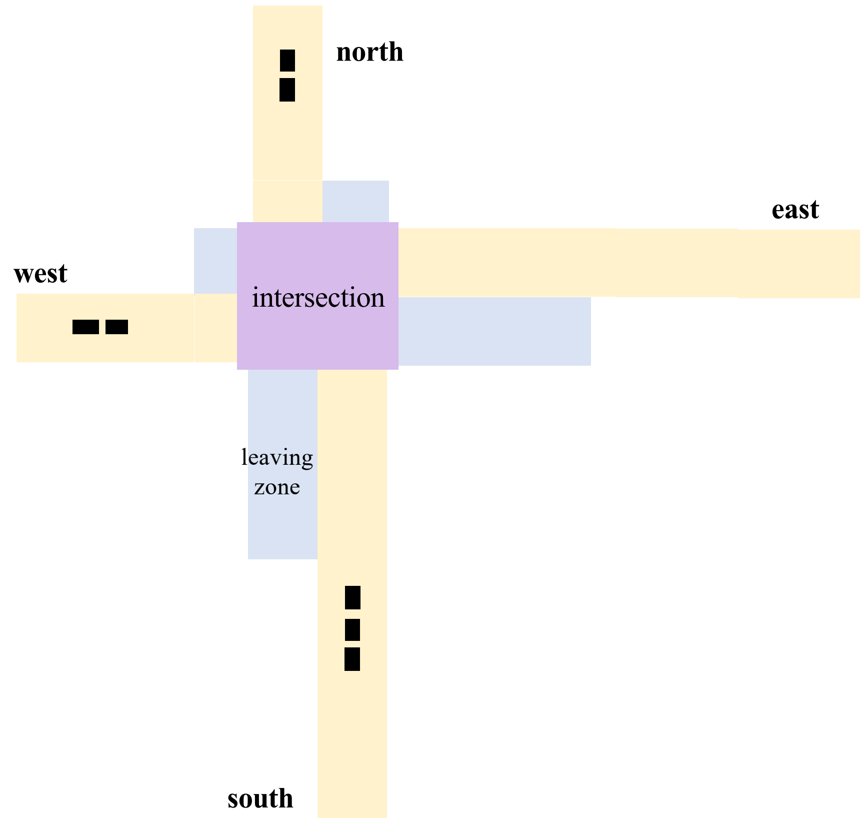
How to define N and f, in these cases?

A protocol for resilient collaborative driving that **leverages reliable location** information of vehicles **to define members of a group** capable of safely reaching an agreement on maneuvers using **consensus algorithms**.

Malicious entities can try to impersonate various vehicles (Sybil attacks)

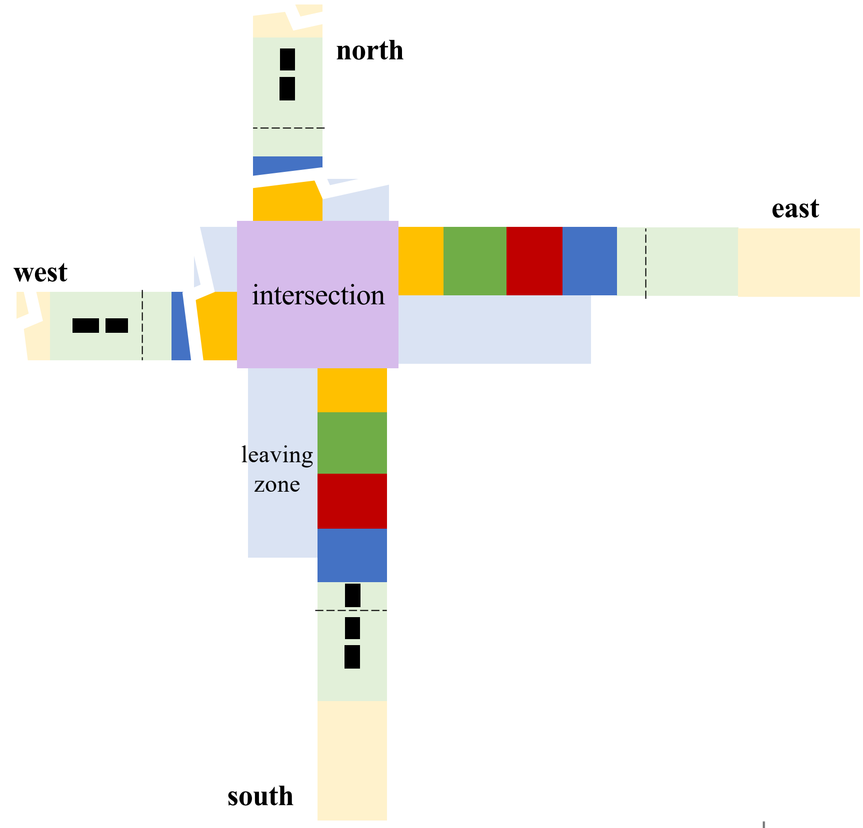
[9] J. Decouchant, D. Kozhaya, V. Rahli, and J. Yu, "DAMYSUS: streamlined BFT consensus leveraging trusted components," in Proceedings of the 17th European Conference on Computer Systems, 2022, pp. 1–16.

Protocol - Intersection crossing use case



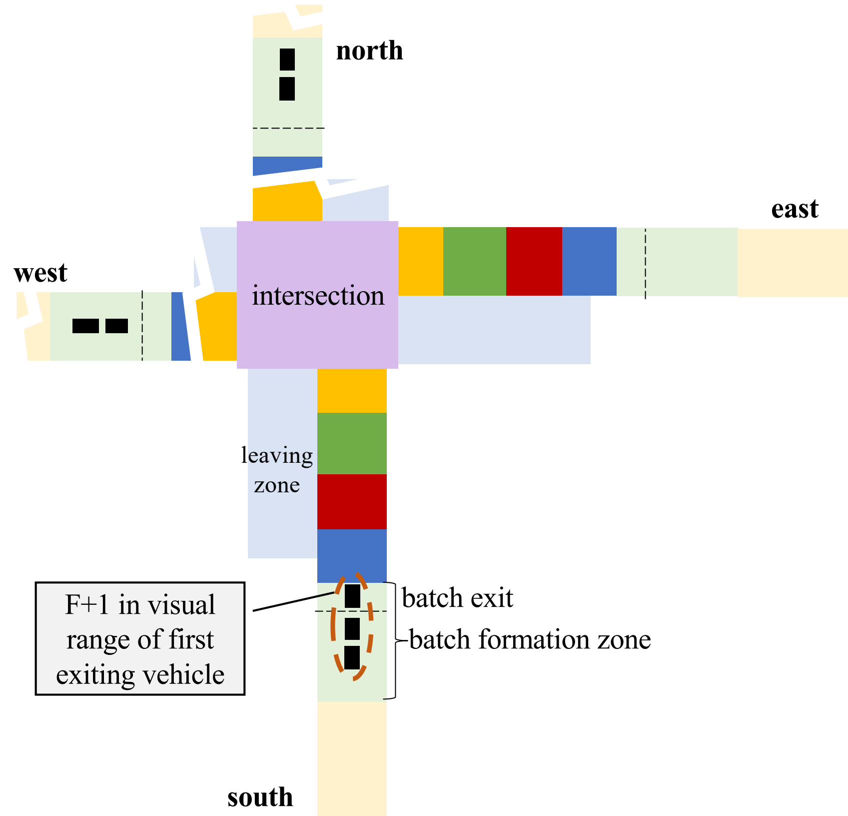
Protocol - Intersection crossing use case

Divide the protocol in phases



Protocol - Intersection crossing use case

- Divide the protocol in phases
- Location-based activation
- Batch formation define N *(i.e.,# vehicles)*



Protocol - Intersection crossing use case

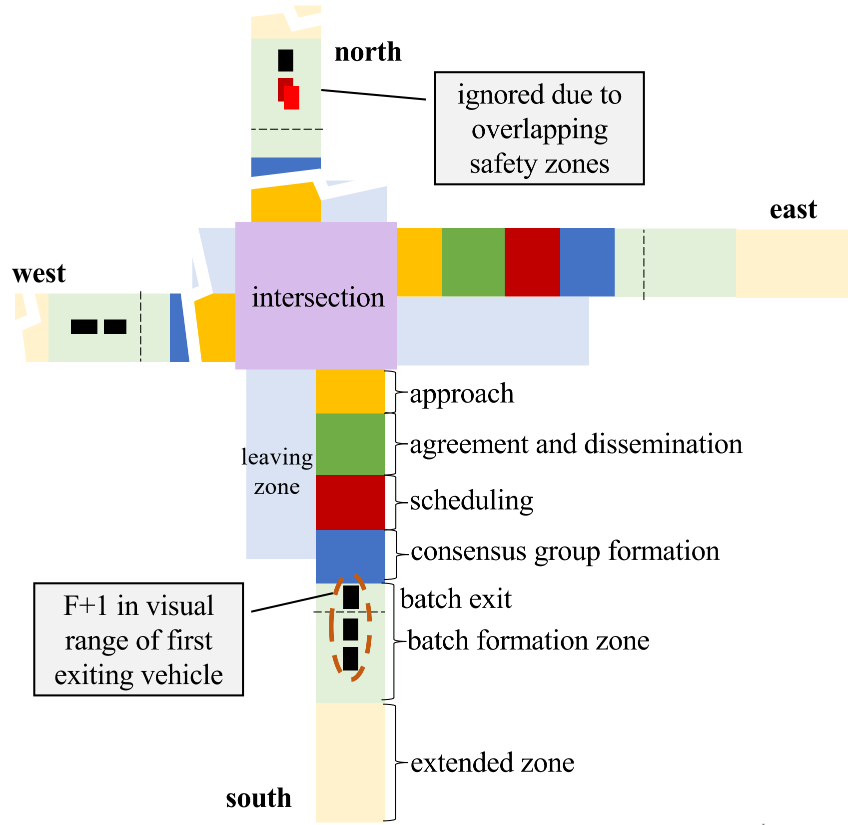
Divide the protocol in phases

Location-based activation

Batch formation define *N (i.e.,# vehicles)*

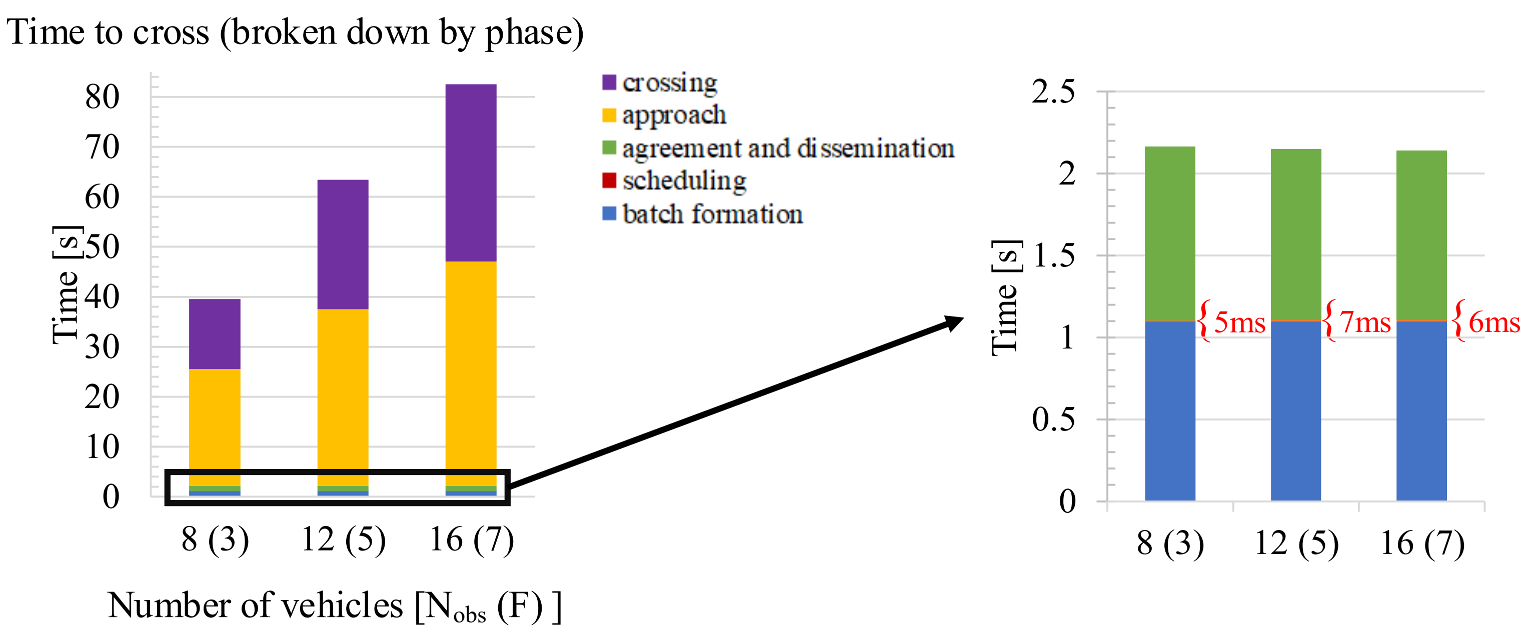
Derive the number of faulty tolerated vehicles f

Define consensus group |CG| = 2f+1



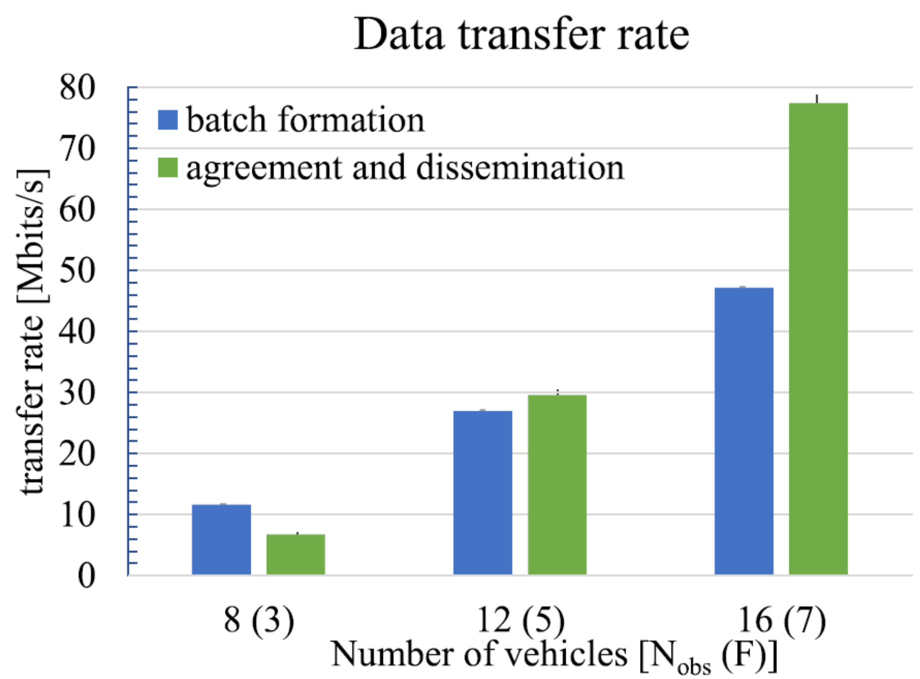
Results –Time to cross

Total time that **a group of vehicles** spends in each phase of the protocol



Results – Data transfer rate(1)

Data transfer rate that **an entire group of vehicles** consumes during phases of the protocol



Results – Data transfer rate(2)

Impact of the constant c *(security level adaptation)* on the data transfer rate of **an entire group of vehicles** during the agreement phase of the protocol

Overall data transfer rate (Mbits/s)

Configuration	Average	Min	Max
$N_{obs} = 16$, c=3 (F=7)	77.3644	75.32063	78.73396
$N_{obs} = 16$, c=4 (F=5)	29.51153	28.47576	30.20559
$N_{obs} = 16$, c=6 (F=3)	8.161355	7.587071	8.461247
$N_{obs} = 16$, c=9 (F=1)	0.569509	0.389318	0.676919

Conclusions

We introduced a novel approach that relies on trust anchors to reliably report a vehicle's location;

We proposed a protocol for constrained-location-based group membership;

We defined our protocol to work with a dynamic number of vehicles;

We used state-of-the-art simulators to evaluate our protocol regarding the time to execute a complex cooperative maneuver and the data transfer rate used.

CRITIX
RESEARCH GROUP

Confirmed-Location Group Membership for Intrusion-Resilient Cooperative Maneuvers

Paper link

Júlio Mendonça
julio.mendonca@uni.lu

UNIVERSITY OF LUXEMBOURG

UNIL | Université de Lausanne

System model

We assume trust anchors [2] can reliably report a vehicle's location, verify received information, and sign messages

We parametrize our solution by a constant c ≥ 4 (hybrid, c ≥ 3) and F < N/c, which also means N > cF

We assume that faulty vehicles may not engage in the protocol:

The number of vehicles engaging N_{obs} should be in [N - F, N]

$N = N_{obs} + F$

Consequently, $F < \frac{N_{obs}}{c} + \frac{F}{c}$ and $F < \frac{N_{obs}}{c-1}$

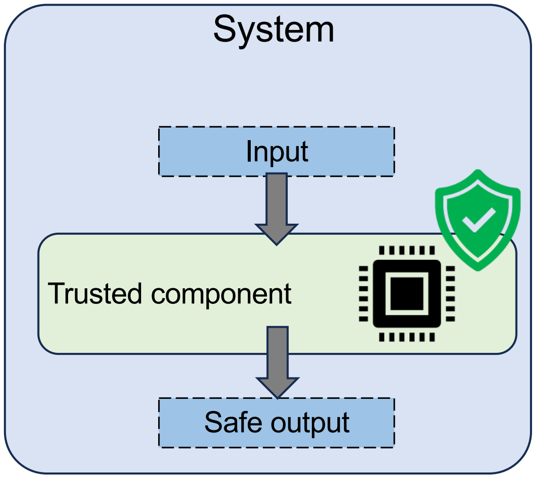
[2] A. Shoker, V. Rahli, J. Decouchant, and P. Esteves-Verissimo, "Intrusion resilience systems for modern vehicles," in 2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring), 2023, pp. 1–7.

Trust Anchors

A security-dedicated independent controller in the vehicle [1, 2];

We focus on defining functionalities, not a new design;

We define functions to enforce drive, certify location, localize, and sign messages.



[1] J. Han and A. Cho, "Practical in-vehicle security architecture based on trust anchors," in 2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring), 2023, pp. 1–3
[2] A. Shoker, V. Rahli, J. Decouchant, and P. Esteves-Verissimo, "Intrusion resilience systems for modern vehicles," in 2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring), 2023, pp. 1–7.