Evaluations of Cyberattacks on Cooperative Control of Connected and Automated Vehicles at Bottleneck Points

Presentation Title

H. M. Sabbir Ahmad[1], Ehsan Sabouni[1], Wei Xiao[2], Christos G. Cassandras[1], Wenchao Li[1]

1. Boston University
2. Massachusetts Institute of Technology

Dependable Computing Lab, CODES Lab

BOSTON UNIVERSITY

GAME-CHANGING OPPORTUNITY: CONNECTED AUTOMATED VEHICLES (CAVs)

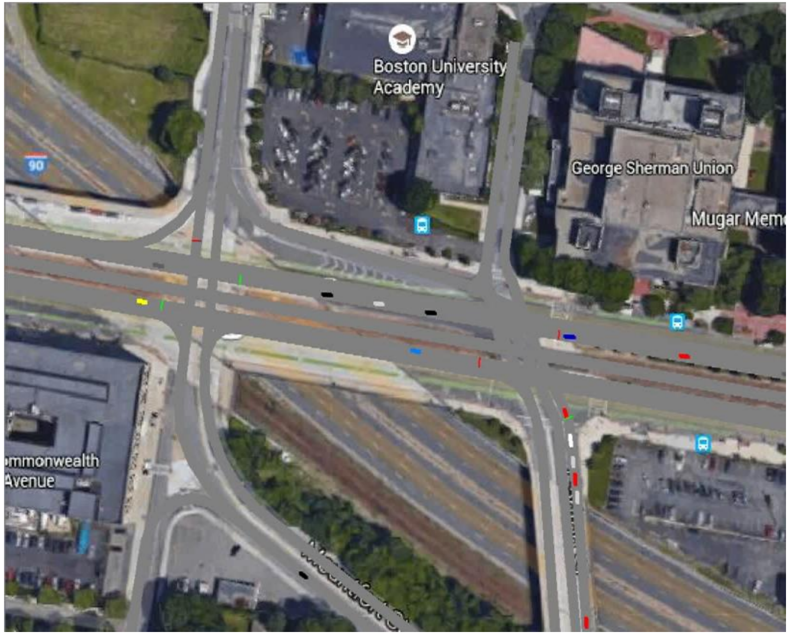
NO TRAFFIC LIGHTS, NEVER STOP…

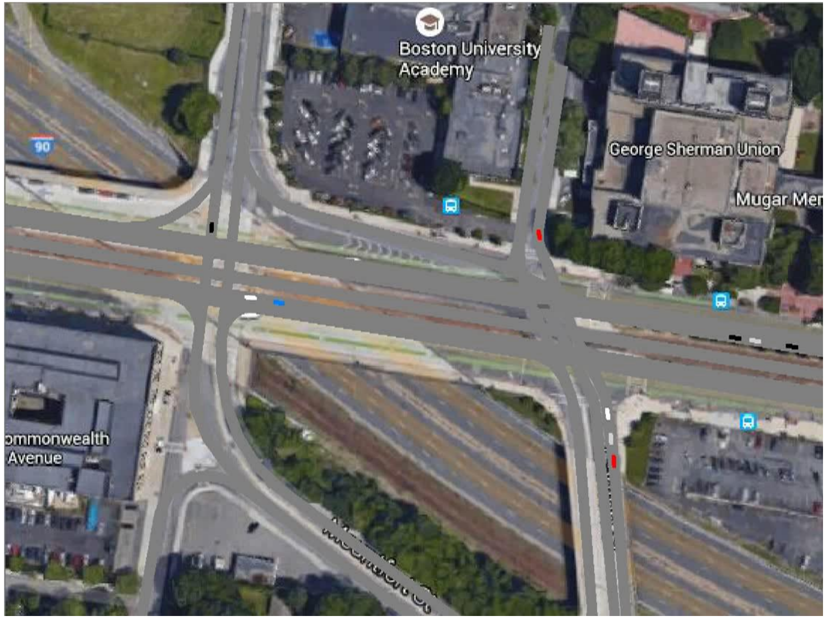
FROM (SELFISH) “DRIVER OPTIMAL” TO (SOCIAL) “SYSTEM OPTIMAL” TRAFFIC CONTROL

Motivation

With *traffic lights*

With *decentralized control* of CAVs





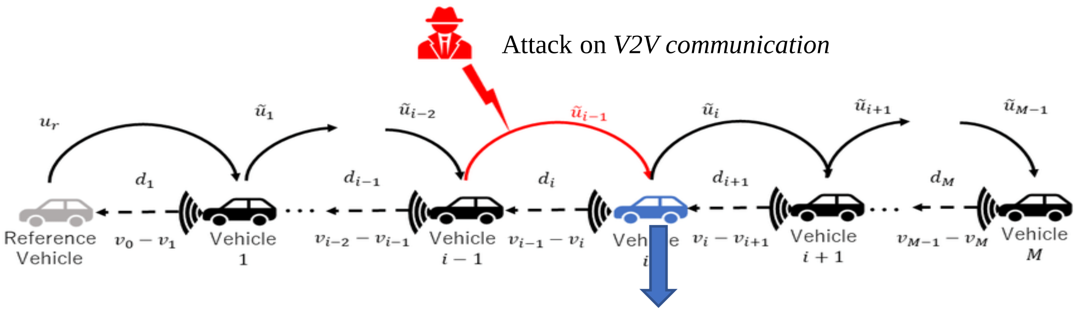
(BU Bridge – Commonwealth Ave, Boston)

Dependable Computing Lab, CODES Lab

BOSTON UNIVERSITY

Cybersecurity Challenge

Cyber attack can thwart CACC.



In-Vehicle Network Attacks:

I. Remote sensor attacks
II. GPS spoofing attacks
III. CAN bus vulnerabilities
IV. ECU software flashing attacks
V. ML attacks …

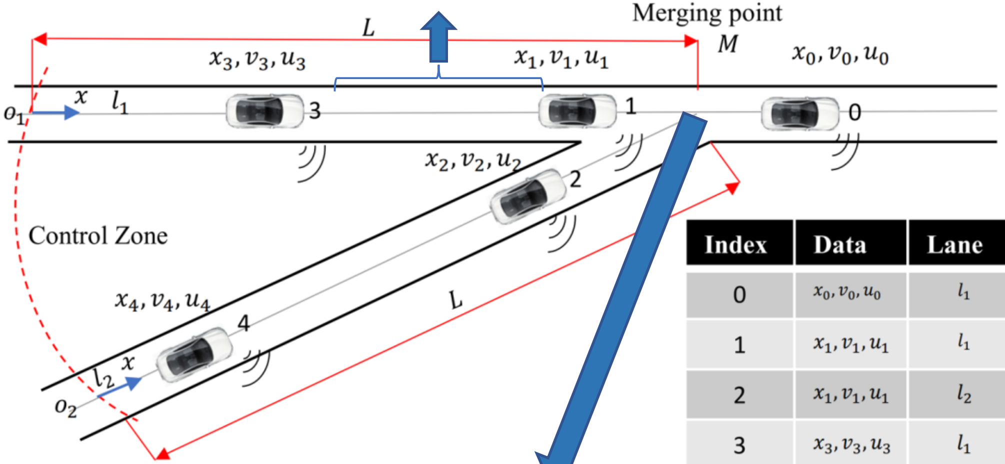
Our paper: first study on *security* of *SOTA* *coordination and control algorithms* for CAVs through *numerous traffic bottleneck points.*

[1]. Yamamoto, Yudai & Kuze, Naomi & Ushio, Toshimitsu. (2021). Attack Detection and Defense System Using an Unknown Input Observer for Cooperative Adaptive Cruise Control Systems. IEEE Access. PP. 1-1. 10.1109/ACCESS.2021.3124547.

CAV Coordination Problem at Bottleneck Points

Merging roadways

Rear-end safety constraint: $z_{i,i_p}(t) \geq \varphi v_i(t) + l$



Index	Data	Lane
0	x_0, v_0, u_0	l_1
1	x_1, v_1, u_1	l_1
2	x_1, v_1, u_1	l_2
3	x_3, v_3, u_3	l_1
4	x_4, v_4, u_4	l_2

FIFO Queue

RSU Coordinator

Safe merging constraint: $z_{i,i_m}(t_i^m) \geq \varphi v_i(t_i^m) + l$

- Provides coordination by maintaining a passing sequence (like Shortest Distance First (SDF), FIFO etc…). We used FIFO policy.
- The coordination is achieved using V2X communication between the CAVs and the coordinator.

Decentralized Constrained Optimal Control Problem formulation

Rear-end safety constraint

Safe merging constraints

Vehicle limitations:

$v_{i,\min} \leq v_i(t) \leq v_{i,\max}, \forall t \in [t_i^0, t_i^f]$

$u_{i,\min} \leq u_i(t) \leq u_{i,\max}, \forall t \in [t_i^0, t_i^f]$

Decentralized Controller:

Minimize travel time | Minimize energy consumption | Maximize centrifugal comfort

Objective: $\min_{u_i(t), t_i^f} \beta_1 \left(t_i^f - t_i^0\right) + \int_{t_i^0}^{t_i^f} \beta_2 C_i(u_i(t))dt + \int_{t_i^0}^{t_i^f} \beta_3 \kappa(x_i(t)) v_i^2(t)dt$

I. *CBF constraints* for rear-end, merging, and state constraints:

$$L_f b_1(\boldsymbol{x}) + L_g b_1(\boldsymbol{x})u + \alpha_1(b_1(\boldsymbol{x}))$$

II. CLF constraints for velocity tracking:

$$L_f V(\boldsymbol{x}) + L_g V(\boldsymbol{x})u + \epsilon V(\boldsymbol{x}) \leq e_i(t)$$

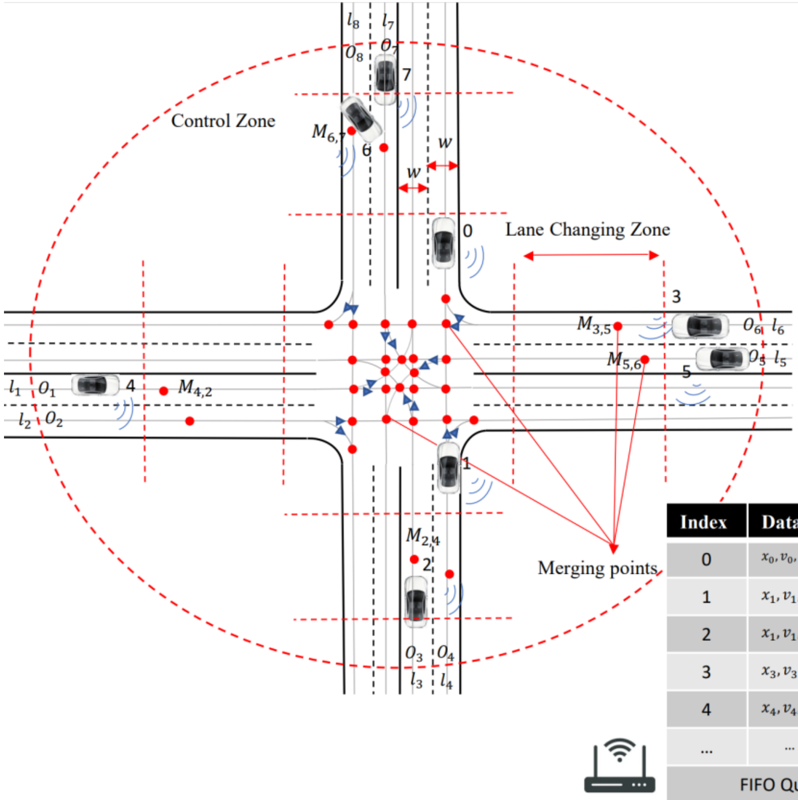
Control $u_i^*(t)$

Advantages of *CBF* based Controller:

i. The CBF OCP problem can be *solved in real time*.

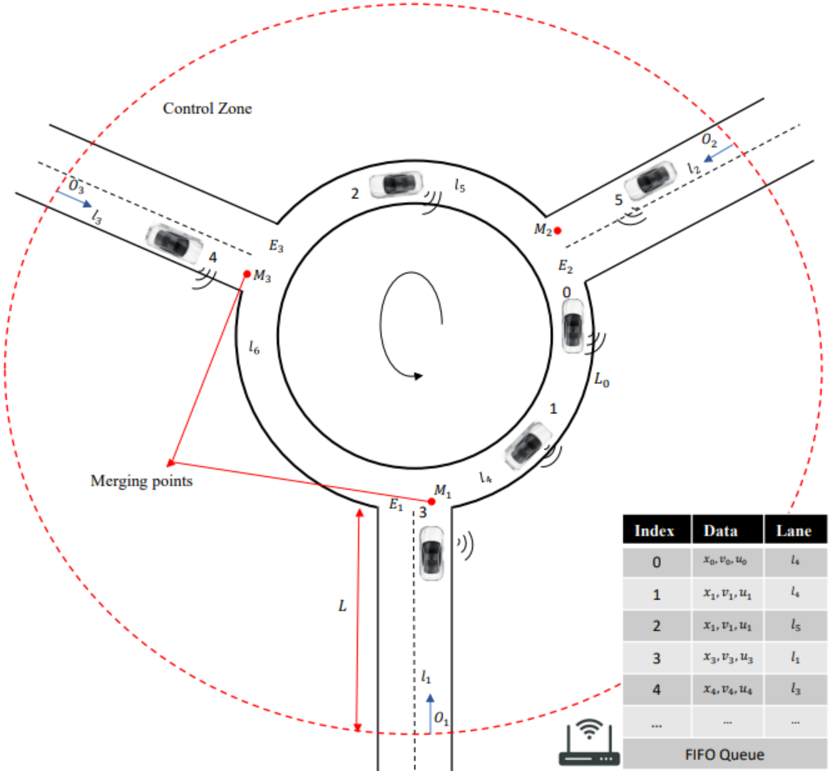
ii. *Safety guarantee* through *forward invariance property of CBFs*.

Signal-Free Intersection and Roundabout



Index	Data	Lane
0	x_0, v_0, u_0	l_4
1	x_1, v_1, u_1	l_4
2	x_1, v_1, u_1	l_3
3	x_3, v_3, u_3	l_6
4	x_4, v_4, u_4	l_1
...	...	...

FIFO Queue



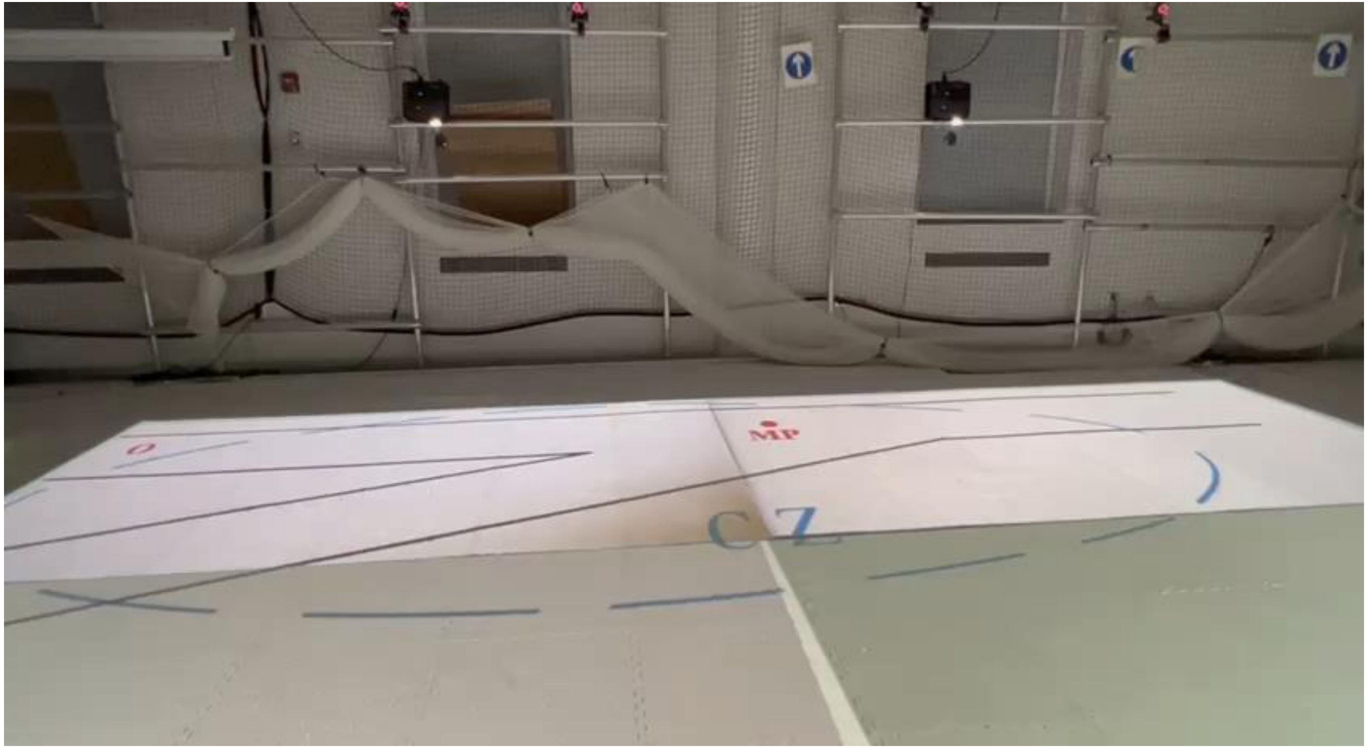
Index	Data	Lane
0	x_0, v_0, u_0	l_4
1	x_1, v_1, u_1	l_4
2	x_1, v_1, u_1	l_5
3	x_3, v_3, u_3	l_1
4	x_4, v_4, u_4	l_3
...	...	...

FIFO Queue

Dependable Computing Lab, CODES Lab

BOSTON UNIVERSITY

Merging roadway testbed using Decentralized CBF-OCP control scheme



Dependable Computing Lab, CODES Lab

BOSTON UNIVERSITY

Attack taxonomy - 1

- Systems assets: i. RSU Coordinator, and

  ii. The CAVs in the CZ.

- Information assets:

  I. RSU Queue table data of all CAVs in CZ.

  II. V2X communication data.

  III. CAV hardware (internal network, onboard sensors and actuators)

- We consider the *RSU as a trusted entity*; and primarily *focus on V2X communication network security*.

Attack taxonomy - 1

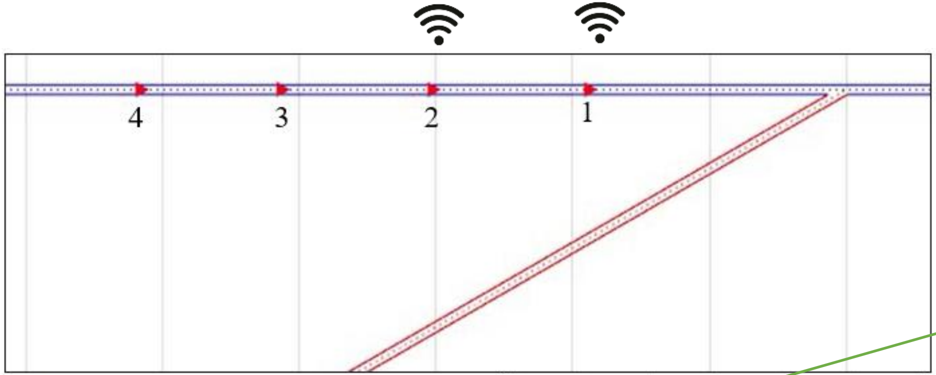
Attack category	Attack type	Network security requirements			
		Confidentiality	Integrity	Availability	Authenticity
Main-in-the-Middle attacks	Replay attack		×		
	False data injection attack		×		
	Slight Attack		×		
Communication hijacking attacks	DoS attack			×	
	Timing attack			×	
	Flooding attack			×	
	Black hole attack			×	
	Grey hole attack			×	
	Wormhole attack			×	
Spoofing attacks	Sybil attack				×
	Impersonation attack				×
Eavesdropping attack		×			
	Interception attack	×			

Simulated attacks

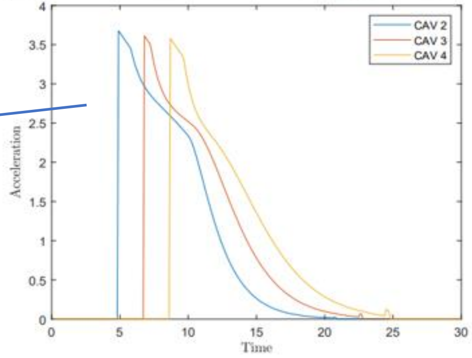
Attack modelling, simulation and results

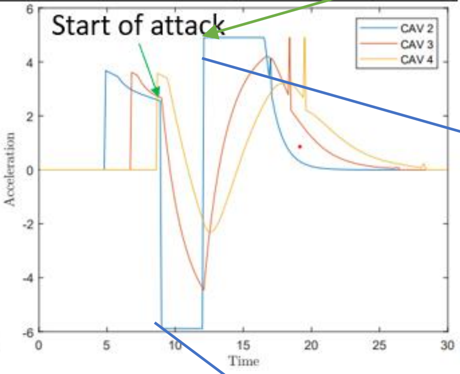
Timing Attack - Result

RSU CAV 1 data is delayed



End of attack



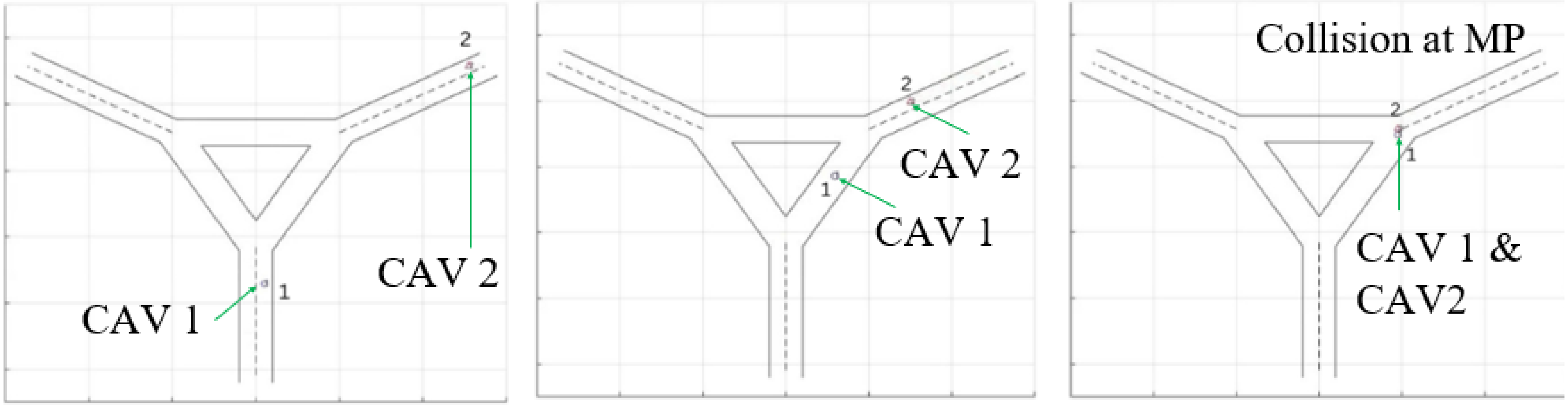


Acceleration profile, no attack

CAV 2 accelerates rapidly and CAVs behind follow suit.

CAV 2 decelerates rapidly and CAVs behind brakes as a result.

FDI Attack - results



RSU (CAV 1 data)

$\tilde{x}_1 = \boldsymbol{x_1} + \boldsymbol{v}$;
$\boldsymbol{v} \in \mathbb{R}^2$;
$\|v\|_\infty \leq c; c \in \mathbb{R}$

Injected bias

CAV 2 Controller

Sybil attack - Attacker capabilities

Three types of attacker models:

i) **Non-informed attacker:** Attacker with no knowledge of the infrastructure

$$\begin{bmatrix} \tilde{x}_{i,k} \\ \tilde{u}_{i,k} \end{bmatrix} = \begin{bmatrix} r_1 \\ r_2 \\ r_3 \end{bmatrix} \; r_i \in \mathbb{R}$$

ii) **Infrastructure aware adversary:** Has knowledge about the data packet structures, coordination requirements (constraints) and CAV physical model.

$$\begin{bmatrix} \tilde{\boldsymbol{x}}_{i,k} \\ \tilde{u}_{i,k} \end{bmatrix} = \begin{bmatrix} \left(f\left(\tilde{\boldsymbol{x}}_{i,k-1}\right) + g\left(\tilde{\boldsymbol{x}}_{i,k-1}\right)\tilde{u}_{i,k}\right)dt \\ \tilde{u}_i^k \end{bmatrix}$$

u_t s.t. rear and merging constraints, and vehicle constraints are satisfied.

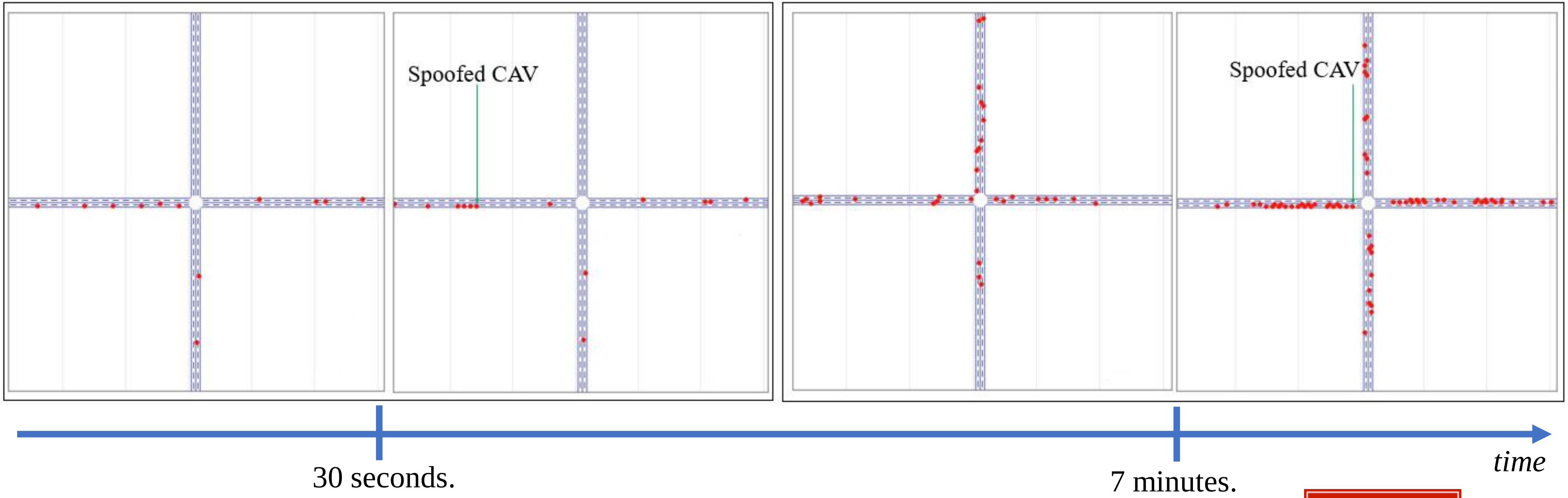
(ii) **Strategic adversary:** Adversary's aim adversary's aim is to cause havoc in the traffic network in the shortest time possible before getting detected. Hence, the data is generated using the same model as following:

$$\begin{bmatrix} \tilde{\boldsymbol{x}}_{i,k} \\ \tilde{u}_{i,k} \end{bmatrix} = \begin{bmatrix} \left(f\left(\tilde{\boldsymbol{x}}_{i,k-1}\right) + g\left(\tilde{\boldsymbol{x}}_{i,k-1}\right)\tilde{u}_{i,k}\right)dt \\ \tilde{u}_i^k \end{bmatrix}$$

$u^t \in \mathbb{R}$; $u_{\min} < u < u_{\max}$ and other constraints are not guaranteed to be satisfied.

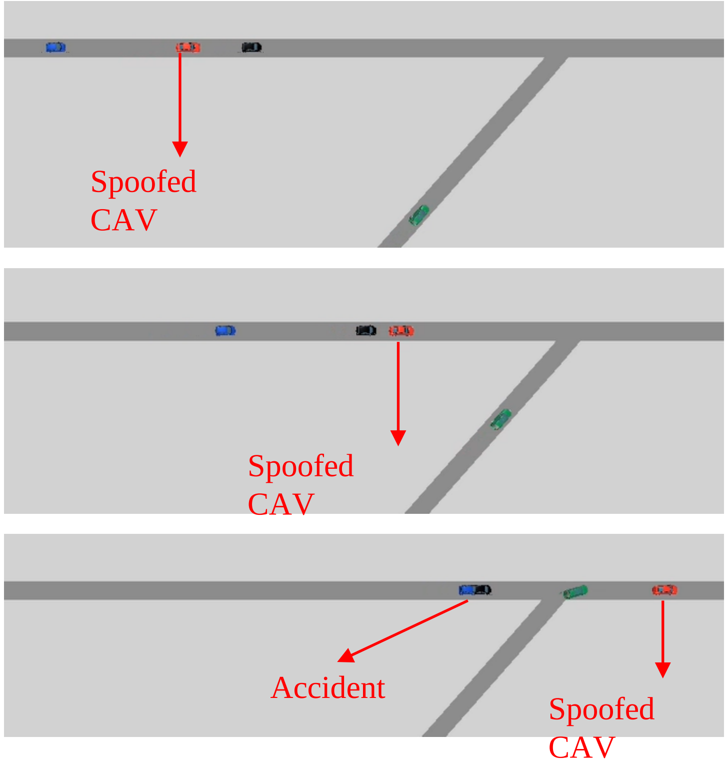
Sybil Attack - Infrastructure aware adversary

- Single spoofed CAV.
- FIFO policy whereby a single sybil CAV in one road causes congestion in other roads in the intersection.



Sybil Attack – Strategic adversary (VISSIM Simulation)

- Adversary spoofs a fake CAV.
- The rear end constraint was modified by adding a large bias as the following:
- Velocity reference for spoofed CAV was set to maximum value.
- *Spoofed CAV* eventually *overtakes* normal CAV ahead; result: *collision* between *physical CAV following it* and *physical CAV originally ahead of it.*



Conclusion and future works

- Our future plans: i. Relax the assumption of *perfect communication.*

  ii. Incorporate *attack resilience* in these SOTA coordination and control algorithms.

  iii. Design *attack detection and mitigation techniques* against V2X communication attacks.

The End

Please share any questions you have.