A Model-based Simulation to Evaluate the Attack's Severity in a Wirelessly Connected Mobile Vehicle Platoons

Ahmed Waleed Khalil Al-Nasir
Department of Artificial Intelligence
College of Computer Science and Information Technology,
University of Anbar
Ramadi, Anbar, IRAQ.
ahmedwaleedalnasir@uoanbar.edu.iq
Orcid.org/0000-0001-5808-4305

DOI: http://dx.doi.org/10.31642/JoKMC/2018/130110
Received Dec. 21, 2025. Accepted for publication Feb.11, 2026

Abstract— *In this paper, a model-based is presented for co-simulation framework to evaluate the severity of cyber-attacks on the wirelessly connected platoons of vehicles (Vehicular network). Two representative attack scenarios are implemented (Shift & Scale) and simulated in a simplified CACC-like model. Numerical results quantify spacing deviations, acceleration anomalies and recovery behavior, illustrating the framework's utility for assessing resilience and guiding mitigation strategies.*

Keywords— Cyber-physical systems, Model-based design, Cyber-attacks, Vehicle platoons, System resilience.

I. INTRODUCTION

Autonomous driving systems are complex cyber physical systems (CPS) integration computation, control and communication. Mobile wireless vehicle connected platooning systems uses cooperative strategies (CACC: Cooperative Adaptive Cruise Control) to improve the efficiency of traffic and safety, but connectivity introduces cybersecurity risks [1]. Simulations usually used to test the behavior of the system. Model-based and co-simulation approaches enable safety, repeatable evaluation of attacks on the dynamics of a platoon [2]. This work focuses on study and analyzes the platoon behavior under attack by employing the features of co-simulation framework. Despite the growing body of research on CACC and connected swarms, most assumptions significantly limit the realism of security evaluations under adversarial conditions. Moreover, current attack models often fail to capture the dynamic and distributed nature of real-world vehicular environment. This study aims to bridge this gap by evaluating reproducible attack scenarios while considering practical system limitations.

II. LITERATURE REVIEW

Recent researches have concentrated on the improvement of safety and robustness of CACC within heterogeneous vehicle platoons. De Haan et al. in 2024 put forth observer based de-centralized CACC system that tackles actuator delays to uphold string stability in mixed platoons. Wan et al. in 2024 proposed a multi objective CACC framework that enhances the fuel efficiency and reduces emissions in the context of event-triggered communications. Kang et al. in 2024 devised a disturbance observer-based approach of CACC that enhance resilience to dynamic uncertainty. In the same way, Redi and Lefber in 2024 tested a prediction-based controller using both theoretical modeling and real-vehicle tests, proving that it can handle time delay and cyber-attacks.

III. SIMULATION AND COMPONENTS

For the requirements of the work in this paper, a platoon is simulated with a centralized CACC-like controller and simplified longitudinal vehicle dynamics. The first vehicle (leader) follows a predefined acceleration profile and followers use a PD (Proportional-Derivative) controller to track a desired spacing for safety (each vehicle maintain the correct spacing and speed (mix of sensors) relative to the vehicle in front: d_safe= 12m) [3][4]. Communication delay effects are explicitly modeled in this simplified numerical study, but it can be incorporated in the INTO-CSP framework in a subsequent work. Communication delays are not explicitly modeled in the current simulations; however, actuator saturation and timing effects partially capture delay-like behavior.

-Simulation parameters: Duration= 200 s, dt= 0.05 s (simulation time step), Followers= 4, Initial spacing= 1 m (between adjacent vehicles at t=0), Safety distance= 12 m (with smooth velocity/ matches the leader to avoid any oscillations), Controller gains: Kp= 0.6 (Proportional gain), Kd= 0.8 (Derivative gain). Kp and Kd are moderate and balanced to maintain spacing and valid for a small platoon to keep the string stable [5]. Acceleration saturation: [-6,3] m/s2.

-Platoon: Leader + 4 follower vehicles in a single lane. Control: Centralized CACC.
-Saturation/ actuator limits: applied to commanded acceleration before integration into vehicle dynamics.
-Attack start-time (baseline DSE)= 60s.
-Attack duration (baseline= 10s.)

While current model captures core CACC dynamics and reproducible attack behaviors, it does not fully account for complex factors such as stochastic communication delays and sensor interference mechanisms. These aspects were partially abstracted to maintain experimental clarity and reproducibility. Incorporating adaptive delay modeling and interference-aware sensing mechanisms represents an important direction for future work.

IV. ATTACK SCENARIOS

Two attacks are evaluated: Shift and Scale.

Shift attack: additive offset Δ applied to the desired acceleration of a target follower.

$u_i'(t) = u_i(t) + \Delta(t).$ ....(1) , where: ui(t) represents the nominal acceleration command generated by the PD controller, and Δ(t) denotes the attack signal injected during the attack interval. The Δ(t) introduces a constant or time-varying bias to the actuator input, resulting in unintended acceleration or deacceleration.

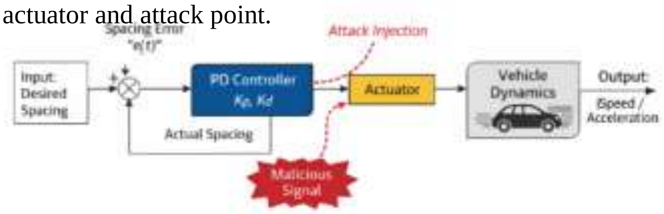
In the numerical calculations, Δ = +1.0 m/s2 applied to follower 2 during the time interval t=40s and t= 60s. The attack produces a sudden bias that creates a spacing error.

Scale attack: multiplicative factor a applied to desired acceleration of α target follower.

$u_i'(t) = \alpha(t)\, u_i(t).$ ....(2) , where: α(t) represents the scaling factor introduced by the attacker during the attack interval.

In the numerical calculations, α = 1.5 applied to follower 3 between t=40s and t= 60s. The attack amplifies for α <1 or attenuates for α >1 control actions, and can produce overreaction/underreaction dynamics.

Above equations (1,2) describes the longitude dynamics for the following vehicle in CACC platoon. Equation (1) represents the evolution of the inter-vehicle spacing, where the spacing error is defined as the difference between the actual distance and desired safe distance. Equation (2) models the vehicles acceleration dynamics, which are influenced by the control input generated by the CACC controller and the actuator behavior. Parameters denote the velocity, acceleration, and spacing of vehicles respectively. A block diagram (1) below is showing the CACC system including the actuator and attack point.



Block-Diagram1: CACC system and attack point

u(t)=Kpe(t)+Kde'(t) **.** ………………………........... (3) , where: K*p* and K*d* denote the proportional and derivative gains, and e(t) represents the spacing error.

The attack signal is injected at the actuator input after the PD controller output.

As illustrated in the diagram above, the attack signal is injected at the actuator input, after the PD controller output and before the vehicle dynamics block. The scale attack directly modifying the control signal before it's applied to the vehicle dynamics.

V. RESULTS AND ANALYSIS

In this section, baseline and attacks are presented with MATLAB / Simulink with Python Scripts. Figures show inter-vehicle spacing, velocities, and accelerations. Tables also summarize severity metrics of each attack scenario computed from simulation traces.

Baseline:

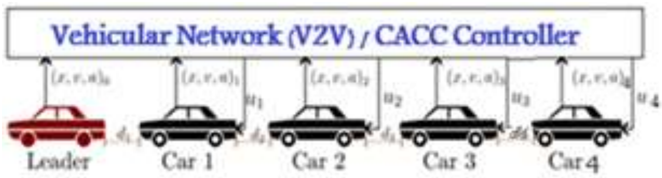


Fig. 1. Five Vehicles Platoon Setup

Baseline inter-vehicle spacing and vehicle dynamics:
Simulations for baseline (no attack) case:

- Leader trajectory: accelerates from 0 → 20 m/s over 30 s, then maintains 20 m/s.
- Followers (4 vehicles): respond through the CACC controller
- (Parameters: Kp=0.6, Kd=0.8, d_safe=12).
- Simulation time duration: 200 s, dt=0.05.

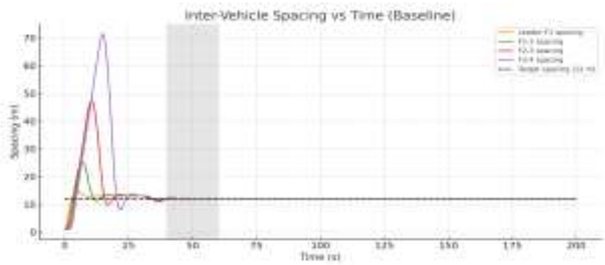


Fig. 2. Inter-vehicles spacing vs. time

* Shaded area represents attack window (40-60 s).

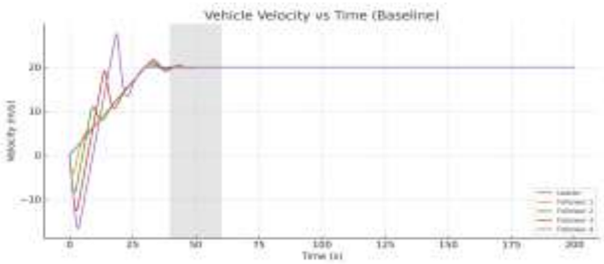


Fig. 3. Velocity vs. time (Velocities)

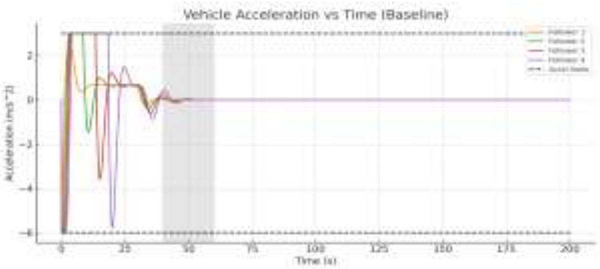


Fig. 4. Accelerations

VI. SHIFT ATTACKS

A shift attack was applied to the second follower in the specific interval:
(Δ= +1.0 m/s^2 between t=40 and 60s)

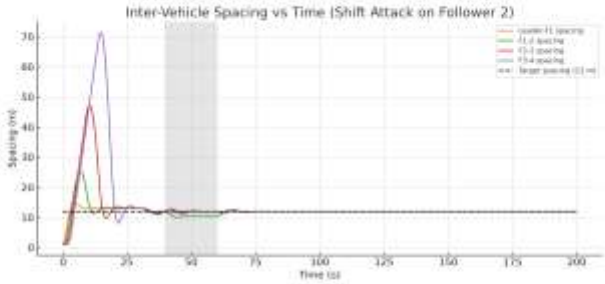


Fig. 5. Inter-vehicle spacing under Shift attack

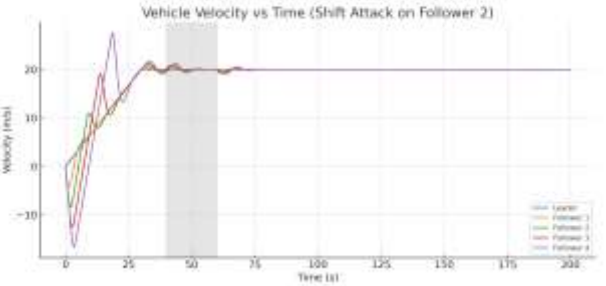


Fig. 6. Velocities under Shift attack

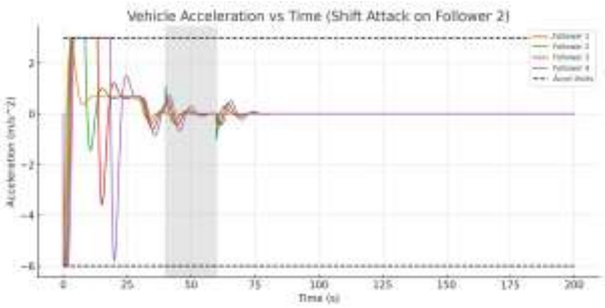


Fig. 7. Accelerations under Shift attack

Table 1. Shift attack severity metrics

Vehicle ID	**Max. Spacing Error (m)**	**Min. Spacing (m)**	**Peak Accel (m/s^2)**	**Recovery Time (s)**	**Severity Level**
1	11.0	1.0	6.00	0.00	High
2	43.0203	1.0	6.00	1.3	High
3	92.595	-4.770	6.00	5.8	High
4	144.089	-32.97	6.00	14.25	High

VII. SCALE ATTACKS

A scale attack was applied to the third follower in the specified interval:
(α= 1.5 between t=40s and t=60s)

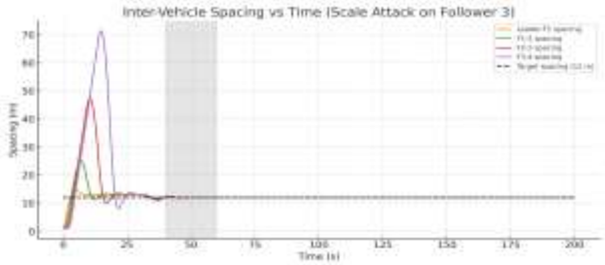


Fig. 8. Inter-vehicle spacing under Scale attack

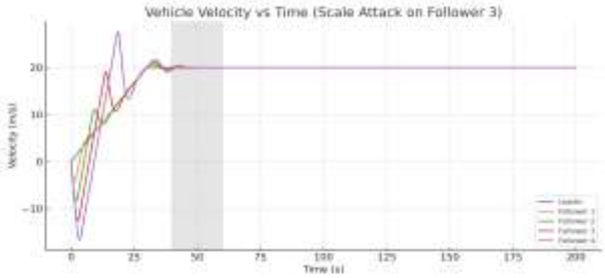


Fig. 9. Velocities under Scale attack

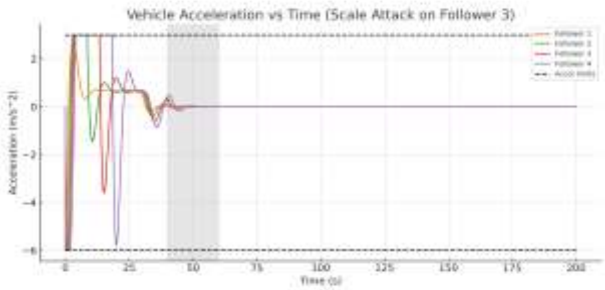


Fig. 10. Accelerations under Scale attack

Table 2. Scale attack severity metrics

Vehicle ID	**Max. Spacing Error (m)**	**Min. Spacing (m)**	**Peak Accel (m/s^2)**	**Recovery Time (s)**	**Severity Level**
1	11.0	1.0	5.40	0.00	High
2	43.108	1.0	5.40	2.10	High
3	92.595	-4.770	6.00	1.28	High
4	142.122	-31.88	6.00	0.00	High

In the above two tables we note many values in the Shift and Scale metrics are similar, this is due to the combination of simulation setup and platoon dynamics. For small numbers of followers, any disturbance injected into one vehicle quickly propagates down the platoon. Vehicles in the tail amplify spacing error, which makes their Max Spacing Error large regardless of which attack type was applied. On the other hand, short attack duration (attack window of 20s) is small relative to the total simulation time, and the system quickly stabilizes after the attack ends. So, recovery times and Min/Max spacing usually converge to similar numbers.

The observed increase in spacing error is primarily caused by malicious manipulation of the actuator command, which disrupts the feedback control loop of the CACC system. This behavior highlights the vulnerability to integrity attacks, particularly in dense vehicle swarms where error propagate rapidly. Compared to baseline conditions, the attack amplifies instability, potentially leading to unsafe braking events.

The curves presented in the above figures were obtained through time-domain simulations conducted using the proposed CACC model. Each simulation was executed over fixed duration, during which the system operated under normal conditions before the cyber-attacks. Shift and scale attacks were introduced at predefined time instants by manipulating input signals. Vehicle spacing, acceleration, and control signals were recorded continuously and averaged over multiple simulation runs to ensure consistency.

VIII. SEVERITY COMPARATIVE ANALYSIS

The below figure illustrates the average MSE under Shift and Scale attacks including communication delays and actuator dynamics.

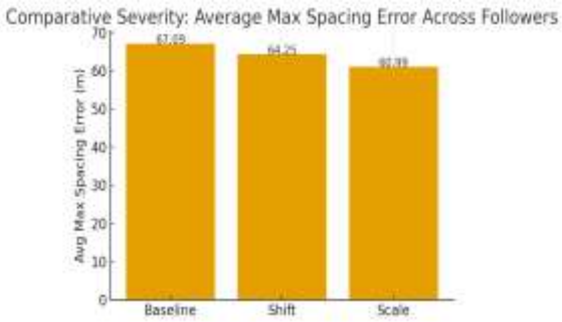


Fig. 11. Comparative **MSE**

* Baseline= 67.086, Shift= 64.235, Scale= 60.993.

IX. DSE HEATMAPS ENHANCED VISULAS

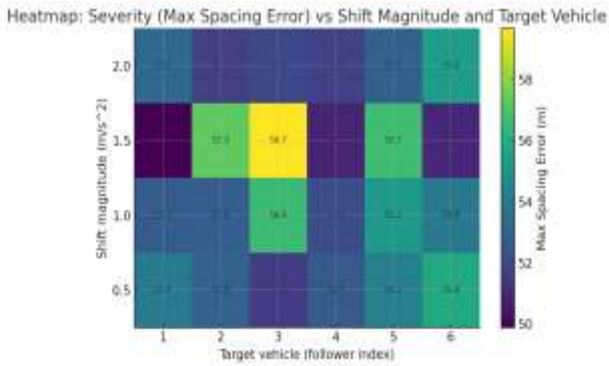


Fig. 12. Heatmap-Shift Severity

The heatmap for Shift attack severity (MSE) across shift magnitude and target vehicles.

Fig. 13. Heatmap-Scale Severity

The heatmap for Scale attack severity (MSE) across Scale factors and target vehicles.

X. CONCLUSIONS

A model-based framework of co-simulation was used for evaluation of the impact of actuator-focused cyber-attacks on a wirelessly connected platoon of vehicles. The shift and scale attacks induced measurable spacing deviations and acceleration anomalies in a targeted follower, severity depended on the attack magnitude and location of the target. The numerical outcomes illustrate the utility of systematic DSE-style experiments of the quantify resilience and guide mitigation strategies. Furthermore, understanding the temporal evolution of the anomalies enables the design of recovery mechanisms, such as adaptive controller reconfiguration or attack-aware filtering, to mitigate unsafe vehicle behavior. Further future work will integrate full INTO-CSP co-simulations with FMUs, incorporate communication delays, sensor attacks and evaluate mitigation approaches.

ACKNOWLEDGEMENT

The Department 0f AI, College 0f C.S & I.T, University of Anbar, Ramadi, Iraq, is ackn0wledged for supporting this paper.

REFERENCES

[1] E. Lefeber, et al., Cooperative adaptive cruise control of heterogeneous vehicles, Technical paper, 2020.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[2] De Haan, et al., Observer-based cooperative adaptive cruise control for heterogeneous vehicle platoons with actuator delay, IEEE Intelligent Transportation Systems Conference (ITSC), 2024.

[3] Wen, et al., Multi-objective cooperative adaptive cruise control platooning of intelligent connected commercial vehicles in event-triggered conditions, *Actuators* journal, 2024.

[4] Kang, et al., Disturbance observer-based robust cooperative adaptive cruise control for heterogeneous vehicles, *Energies* journal (MDPI), 2024.

[5] De Haan, et al., Platooning of heterogeneous vehicles with actuation delays: theoretical and experimental results, *arXiv* preprint, 2024.