Resiliency of Vehicle Platoon Network Topologies under Physical Attack

Constance Hendrix, Gedare Bloom
University of Colorado Colorado Springs, Colorado Springs, CO, USA
{chendr12, gbloom}@uccs.edu

***Abstract*—Vehicle platooning inspires the future of transportation and yet introduces the possibility for physical attacks to disrupt autonomy operations. In this paper, we evaluate platoon resiliency in the presence of such attacks. Our evaluation includes 60 unique combinations of controller, control policy, and topology with an equal weight control schema while attacking specific platoon members. The experimental results show that the targeted vehicle, network topology, control policy, and controller all influence platoon resiliency with some configurations leading to platoon instability.**

I. Introduction

Driving automation and connectivity in vehicle platoons can improve road efficiencies in terms of fuel, capacity, safety, and emissions [1]. A vehicle platoon consists of a lead and following vehicles traveling cooperatively in a spatially compressed formation. The leader is assumed to be manually operated while the followers are controlled by a distributed controller providing cooperative adaptive cruise control (CACC) and lane centering control [2]. Given that a platoon is a collective unit, information from other vehicles sent over a network topology to be used by the distributed controller introduces new attack seams [3]. In addition to attacks by electronic means [4], physical attacks should be considered due to their low cost and ease of execution [5].

Selection of a controller, control policy, or a detection-response method may help mitigate the impact of an attack, but the impact as it relates to a targeted platoon member's controller and control policy remains under-investigated. Platoon impact is often related in terms of resiliency and robustness. We define resiliency as the platoon's ability to recover from a disabling attack by continuing to operate as a unit. Robustness indicates the platoon is less affected by perturbations. In this paper, we examine potential impact differences with changes in control configuration while targeting different platoon members and evaluating platoon resiliency to attack. We implemented two distributed control configurations for comparison to prior work [5] that examined platoon vulnerability based on a taxonomy of platoon network topologies.

This paper contributes a comprehensive evaluation of a vehicle platoon's performance based on platoon topology, physically attacked platoon member, and configuration of controller and control policy. Specific findings include: (i) platoon members with higher connectivity are less responsive to attack, which results in a less resilient platoon response; (ii) controller responsiveness significantly impacts resiliency; (iii) addition of a leader channel when a vehicle has low connectivity causes the vehicle to be less responsive to perturbations; and (iv) the constant time gap control policy causes platoon instability in nearest neighbor topologies when the connections to the front or rear exceeds four.

This work is supported in part by NSF CNS-2046705 and Colorado SB18-086.

II. Related Work

Hendrix and Bloom [5] introduced the platoon topology taxonomy that we adopt, which studied the impact of a spoofing and physical attack on specific vehicles in a platoon based on the platoon topology; however, they only examined the linear quadratic regulator (LQR) with constant distance (CD) control configuration. Performance was also measured using L_2 Gain from spoofing attack. Xiao et al. [6] demonstrated that the impact of communication delays while scaling platoons can be mitigated by using sliding mode control (SMC) and constant time gap (CTG) as opposed to a proportional-derivative or CD control policies. Wen et al. [7] introduced an effective layered control framework assuming mixed traffic in an urban setting using SMC. Van Nunen et al. [8] designed a model predictive controller using feed-forward control and a combination of CD and CTG to avoid string instability in a heterogeneous platoon suffering from packet losses. Thus, we are motivated to study the SMC controller and the CTG policy in the adversarial setting.

Pirani et al. [9] evaluate impact of platoon topology on robustness and resilience, but does not investigate platoon impact of a specific targeted vehicle. They found k-nearest neighbor ($k > 2$) and leader-to-all topologies were the most robust to attack due to their high connectivity and that a trade-off exists between robustness and resiliency. Zheng et al. [10] investigated the influence of topology on closed-loop stability and identified linear controller gain thresholds for stability. Wang et al. [11] noted that switching topologies or the use of time varying topologies can be used to mitigate communication loss. Dadras et al. [12] showed that a single vehicle attack can destabilize a vehicle platoon. Attacks were executed at different positions using local sensing. However, this prior work does not address platoon impact given a specific targeted follower using only intra-platoon communication across multiple controller-policy-topology configurations.

III. Platoon Physical Attack

A hard brake is assumed to occur due to a physical attack such as an object being thrown in front of a targeted vehicle. We use this attack with the following model to evaluate platoon response across topologies, varying controllers and control policies. The ramp disturbance, $w(t)$, is added to the targeted member's acceleration to model the effect of braking in response to a physical attack as

$$w(t) = \begin{cases} -c_0(t - t_1) & t_1 < t < t_2 | t = \{0 : T_s\} \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

where t_1 is braking start time, t_2 is brake release, T_s is the total simulation time, and c_0 is a constant defining the amplitude of deceleration. We assume brakes are applied upon attack overriding CACC until they are released.

IV. Vehicle Dynamic Model and Control

We assume a homogeneous platoon system where each vehicle uses CACC to maintain adherence to a control policy. We adopt a commonly used dynamic model of longitudinal control [13], [14] defined by state equations: $\dot{p}(t) = v(t)$, $\dot{v}(t) = a(t)$, and $\dot{a}(t) = \frac{1}{\tau}[-a(t) + u(t)]$. The state space model is translated as:

$$\dot{x}_i(t) = A_i x_i(t) + B_i u_i(t) + W_i w(t) \quad (2)$$

$$y_i(t) = C_i x_i(t) + D_i u_i(t) \quad (3)$$

$$A_i = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -1/\tau_i \end{bmatrix} \quad B_i = \begin{bmatrix} 0 \\ 0 \\ 1/\tau_i \end{bmatrix} \quad C_i = I \quad D_i = \vec{0} \quad (4)$$

where $x = \{p,\ v\ , a\}$—position, velocity, and acceleration—t is time, u is the control input, i is the vehicle number, τ is the engine time constant, and I is an identity matrix. We use two distributed full-state feedback controllers based on this model: an LQR and an SMC.

The LQR is determined given the zero-error state of Equation 2, the state-cost weight Q and input-cost weight R are initially selected heuristically using Bryson's rule in the infinite-horizon cost function, J, then adjusting Q to reduce the maximum acceptable value of position error.

$$J(u) = \int_0^\infty (x^T Q x + u^T R u) dt \quad (5)$$

The input gain for each vehicle, β in $u_i(t) = \beta x_i(t)$, is determined first by solving its algebraic Riccati equation, then its gain.

SMC uses the sign of the error to drive a dynamic system to a reference state with the control signal:

$$u_i(t) = \beta\ \text{sgn}(\sigma(t)) \qquad \sigma(t) = \dot{e(t)} + c_1 e(t)$$

where σ is the sliding manifold, and c_1 is a positive constant design parameter which weighs the error ($e(t)$) against its direction of change. The controller's goal is to drive the parameter σ towards zero. Due to the inherent discontinuity at zero, the following saturation function replaces the sign (sgn) function [15]:

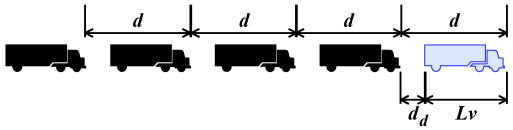


Fig. 1: Intra-Platoon Spacing Policy.

$$sat(y/\epsilon) = \begin{cases} y/\epsilon & \text{if } |y/\epsilon| \leq 1 \\ \text{sgn}(y/\epsilon) & \text{if } |y/\epsilon| > 1 \end{cases} \quad (6)$$

where ϵ is a small positive constant. This function significantly reduces chattering effects for smoother control [16].

V. Platoon Dynamic Model and Control

The platoon topology is a simple graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$. Vehicles are nodes ($\in \mathcal{V}$) and communication links are edges ($\in \mathcal{E}$) [9], [17]. The Laplacian matrix is $\mathcal{L} = \mathcal{D} - \mathcal{A}$, where $\mathcal{A}$ is the adjacency matrix and $\mathcal{D}$ is the degree matrix. We also use the following pinning matrix to define follower connections with the leader:

$$\mathcal{P}_{ij} = \begin{cases} 1 & \text{if } i = j \text{ and } \exists \text{ a edge between } v_i \text{ and } v_0 \\ 0 & \text{otherwise,} \end{cases} \quad (7)$$

where v_0 is the leader. Connections within the platoon's topology are represented by $\mathcal{L} + \mathcal{P}$, and the following platoon model is derived from prior work [10]:

$$A_c = [I_{N-1} \otimes A] - diag(\mathcal{L} + \mathcal{P})^{-1}(\mathcal{L} + \mathcal{P}) \otimes B\beta \quad (8)$$

$$\dot{X}_c = A_c X_c - diag(\mathcal{L} + \mathcal{P})^{-1}(\mathcal{P} \otimes B\beta) X_0 \quad (9)$$

where $\otimes$ is the Kronecker product, A_c the closed-loop system matrix, and β the gain determined by the controller which drives the vehicle dynamics, slightly modifying equations found in [10], [17]. The modified follower and leader state vectors X_c and X_0 are:

$$X_c = [\tilde{x}_{v_1}, \tilde{x}_{v_2}, ..., \tilde{x}_{v_{N-1}}]^T \quad (10)$$

$$X_0 = 1^T_{(N-1)} \tilde{x}_0 \quad (11)$$

$$\tilde{x} = x - [d(i-j), 0, 0]^T \quad (12)$$

where d is the front bumper to front bumper distance as shown in Figure 1. The variables i and j indicate the positional number of the ego vehicle and the connected vehicle. Given $\beta = [\beta_1, \beta_2, \beta_3]$, the input for each vehicle, using either CD or CTG to define d, is:

$$u_i(t) = -\frac{1}{diag(\mathcal{L} + \mathcal{P})_i} \sum_{j \in \mathbb{N}_i} [\beta_1(p_i(t) - p_j(t) + d(i-j)) + \beta_2(v_i(t) - v_j(t)) + \beta_3(a_i(t) - a_j(t))] \quad (13)$$

$$d = \begin{cases} L_v + d_d, & \text{CD} \\ L_v + v_i * t_g, & \text{CTG} \end{cases} \quad (14)$$

where d_d is the desired distance, t_g is the desired time gap [18], and L_v is the vehicle's length, as shown in Fig. 1.

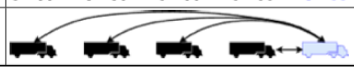
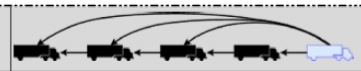
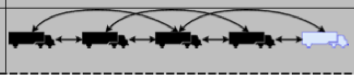
Topology Taxonomy	*Graphical Depiction*
Leader Following (LF)	
Leader Networking (LN)	
1-Predecessor Following (1PF)	
1-Nearest Neighbor Networking (1NNN)	
1-Predecessor Leader Following (1PLF)	
1-Nearest Neighbor Networking, Leader Following (1NNNLF)	
1-Nearest Neighbor Leader Networking (1NNLN)	
2-Predecessor Following (2PF)	
2-Nearest Neighbor Networking (2NNN)	

Fig. 2: Sampling of topology taxonomy. Arrows represent network edges, and the black trucks represent the followers.

Also, $\mathcal{L} + \mathcal{P}$ is used to normalize the input given number of contributing vehicles.

VI. Evaluation

We created a framework in MATLAB/Simulink to evaluate how changing controller and control policies impact attack effects when targeting one vehicle over another. Using our framework, we performed attack-free testing, selected metrics for evaluation, then executed a physical attack on the platoon while changing targeted vehicle across 60 controller-policy-topology configurations. We used the LQR-CD from prior work [5] as an attack baseline to which we added SMC-CD and LQR-CTG. We assumed onboard sensors were not available in order to isolate the impact of the network's control contribution.

A. Metrics

We focus on three aspects of platoon performance during physical attack: minimum inter-vehicle spacing to identify unsafe distances and collisions, maximum inter-vehicle spacing to identify excessive spacing which could split the platoon, and mean absolute error (MAE) to determine platoon sensitivity to attack. MAE was used instead of L_2 gain [5] because error was not injected into the model during attack and it helps compare with attack-free runs. MAE was calculated as follows:

$$\text{MAE}_p = \frac{\sum_{i=1}^{N-1} |\text{MAE}_i|}{N-1} \tag{15}$$

$$\text{MAE}_i = \frac{\sum_{j=0}^{t_{max}} |d_i - d_d|}{T_s} \tag{16}$$

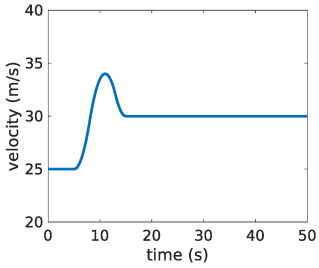


Fig. 3: Leader Velocity. The leader executes a longitudinal change by accelerating from 25 $\frac{m}{sec}$ to 34 $\frac{m}{sec}$, then decelerating back down to 30 $\frac{m}{sec}$.

where MAE_p is the MAE for the platoon, MAE_i is the MAE of each inter-vehicle spacing, i is the vehicle number, and d_i is the distance between v_i and v_{i-1}.

B. Experiment Setup

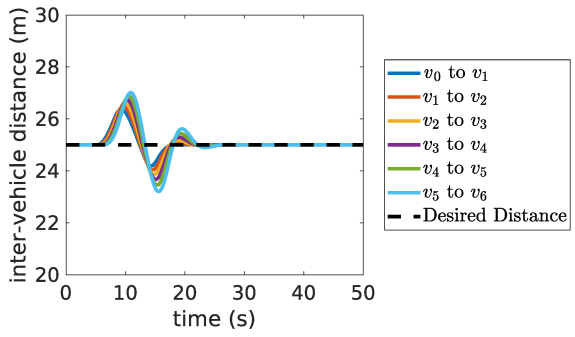
We use a platoon of size 7, which is large enough to evaluate error propagating through the platoon although less than the recommended maximum platoon size [19]–[21]. A platoon size of 7 has 20 unique network topologies, which we organize using the topology taxonomy from prior work [5]. A sampling of the taxonomy is shown in Fig. 2. The time constant τ used in simulations is 0.235 s [5]. We analyzed the step response rise time of each vehicle controller with τ and found the LQR to be 2.5 times more responsive than SMC. We set the parameters $d_d = 25$ meters for CD and $t_g = 1$ second for CTG.

C. Attack-Free Experiments

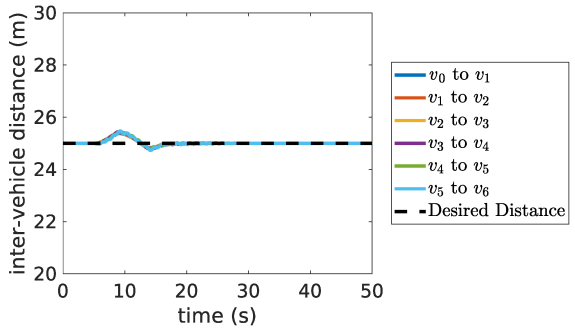
We executed attack-free baseline tests of all controller-policy-topology configurations using a longitudinal movement (inspired by Lyu et al. [22]) executed by the leader, as shown in Fig. 3. Fig. 4 presents a selection of performance results. Both controllers maintained the desired spacing dictated by the corresponding control policy over the maneuver; however, each performed differently. String instability was found in 1PF for LQR and SMC with amplification of error toward the rear of the platoon. The effect of string instability disappeared as more followers connected to the leader and for PF topologies where $k > 3$ for LQR and $k > 1$ for SMC. In addition, the CTG control policy was unstable with nearest neighbor undirected connections exceeding four (e.g., 3-Nearest Neighbor Networking (3NNN), -Nearest Neighbor Leader Networking (3NNLN)).

D. Attack Experiments

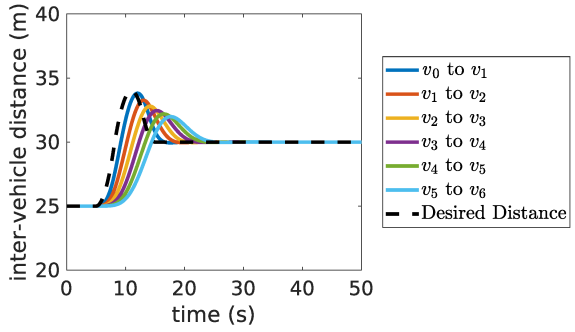
The physical attack was executed while the leader kept a constant velocity of 30 m/s for 50 seconds, simulating a highway cruising speed. Communication delays were not considered. All platoon members were initially spaced at 30 meters. Acceleration was bound to $7\frac{m}{s^2}$ as derived from the Bosch Automotive Handbook [23]. We dictate an unsafe distance between vehicles to be at 0.25 s time gap, which is



(a) LQR with CD Control Policy.

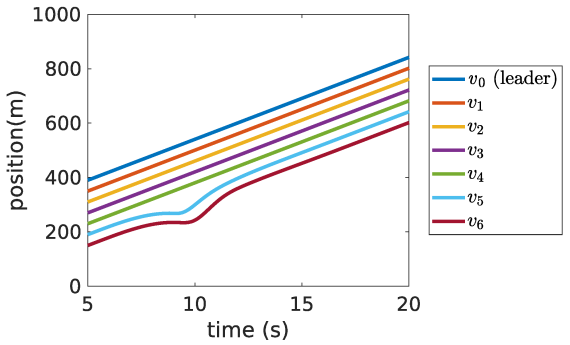


(b) SMC with CD Control Policy.

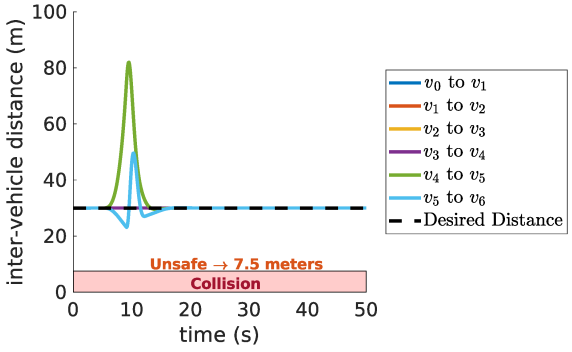


(c) LQR with CTG Control Policy.

Fig. 4: Inter-vehicle distance during Baseline testing of 1-Predecessor Following (1PF) topology.



(a) Platoon position over time.



(b) Platoon inter-vehicle distance over time.

Fig. 5: Physical attack targeting v_5 using LQR controller, CD control policy, and 1PF topology.

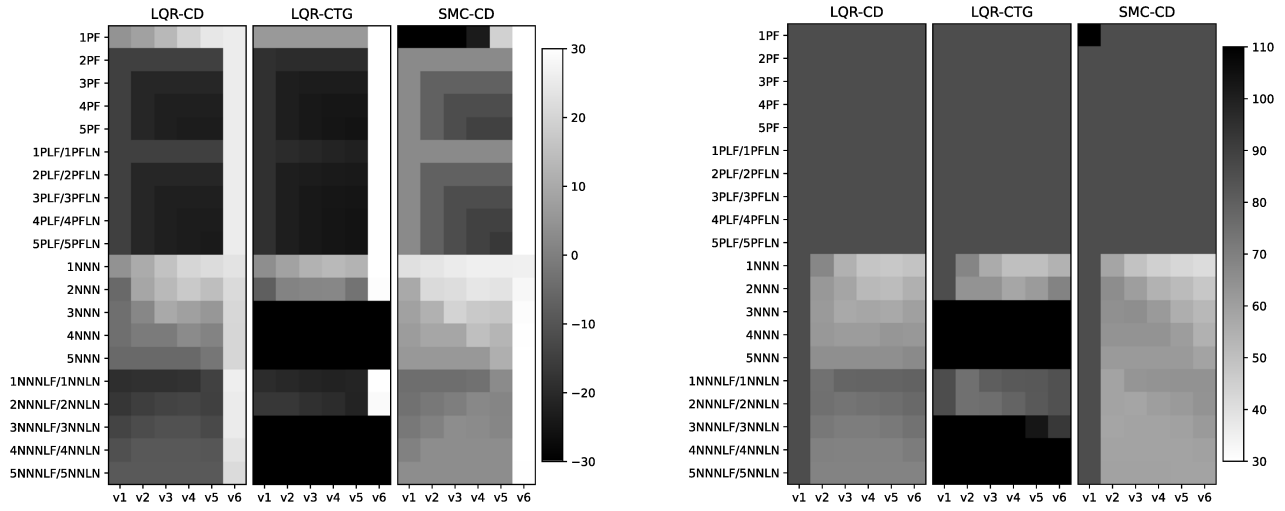
less than half of the shortest time gap identified for platoons by Shladover et al. [1]. For the targeted vehicle, the attack matrix from Equation 2 was set to $W = [0; 0; 1]$ and for Equation 1 we set $c_0 = 15$, $t_1 = 5$, and $t_2 = 9$. For all other vehicles, $W = [0; 0; 0]$.

1) Attack Effects and Platoon Sensitivity: One vehicle is attacked at a time across all controller-policy-topology configurations. As an example, Fig. 5a shows results for the 1PF topology, LQR controller, and CD control policy while vehicle v_5 was attacked. The resulting effect is v_5 increasing its inter-vehicle distance to 80 meters or to 2.67 seconds time gap. The tail vehicle v_6 reacts quickly, avoiding a collision with its predecessor, but also increasing its inter-vehicle distance with v_5 to 50 meters before re-establishing the 30-meter spacing.

We conducted all combinations of attacks varying targeted vehicle, topology, controller, and control policy. Effects from each attack are shown in Fig. 6a and 6b. In Fig. 6a, the minimum inter-vehicle distances provide indications of collisions. Fig. 6b shows the maximum inter-vehicle distances with large spacings between platoon members, i.e., splitting. These results show that a physical attack can prevent the platoon from operating as a unit.

Using the inter-vehicle spacing, MAE_p was calculated and compared across configurations. MAE_p results are shown in Fig. 7. These results are useful for evaluating resiliency by comparing attack effects. For example, a high MAE_p and low minimum distance indicates an error will be distributed throughout the platoon reducing chances for collision, therefore being more resilient but less robust. This trade-off coincides with findings from Pirani et al. using graph theory [9].

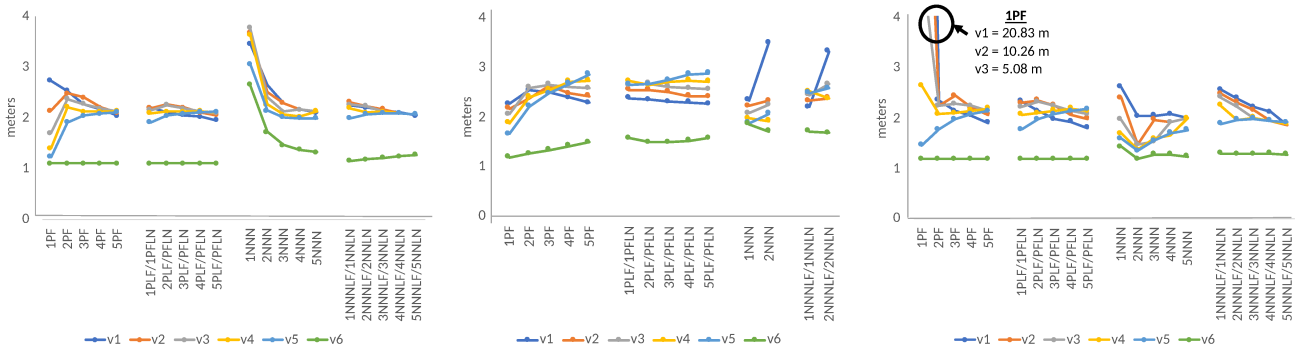
2) Controller Comparisons: In these experiments, we have reproduced prior work [5] using Simulink and extended it with some modifications. We increased the penalty for the position error in the LQR and doubled the braking amplitude and time braking to inject more error into the platoon. We confirmed that attacking followers toward the front of the platoon injects the most error into the platoon in all PF topologies. String instability in the 1PF topology will cause potential collisions at the rear of the platoon when v_1 is attacked. Using the 1NNN topology, distance errors constantly circulate between platoon members and takes the longest time to settle. We infer



(a) Physical attack minimum inter-vehicle spacing (meters). 0 meters between vehicles indicates a collision.

(b) Physical attack maximum inter-vehicle spacing (meters).

Fig. 6: Inter-vehicle spacing under physical attack given targeted vehicle and topology. 30 meters is the desired distance.



(a) MAE using LQR and CD control.

(b) MAE using LQR and CTG control.

(c) MAE using SMC and CD control.

Fig. 7: Attack mean absolute error (MAE) results.

this topology is the least robust using LQR-CD. In topologies where connections are undirected, attacking middle platoon members—which have the most connections—injects the most distance error into the platoon. In fully connected platoons, all following members move together more tightly, causing v_1 to separate more from the leader. Overall if the intent is to impact the platoon as a whole, the least connected topologies present a situation where the attacker would benefit more by targeting one follower over another.

We also compared results of changing the controller type while keeping the control policy. Overall, the SMC resulted in a more resilient setting using kNNN and kNNLN topologies. Using the 1PF topology, the responsiveness of the SMC controller amplified the effect of string instability. We attribute the amplification to the derivative action of the control paired with the aggressive braking action. We found the less responsive the controller, the less compatible with the 1PF topology, which is the least connected network configuration.

3) Control Policy Comparisons: The LQR using both control policies had similar effects across stable topologies, with the CD being more resilient to attack as determined by reduced effects, as shown from Fig. 6a-6b. For LQR using CTG, highly networked NNN topologies produced instability once any change in state was introduced. Performance degrades as k increases. Topologies without connections to the leader and having $k = 1$ were the most resilient against attack when using CTG policy.

Regardless of policy, the likelihood of collision is tied to the connectivity of the vehicle if the platoon uses an equally weighted control policy. For example in LQR-CD using 4PF topology, attacking v_1 causes v_2 to react dependent on states from the leader and v_1. Half of the control action comes from the attacked vehicle and the other half from the leader. However, if v_5 is attacked in the same configuration, the following vehicle v_6 would be slower to react because position data received from v_2, v_3, v_4, and v_5 reduces the control influence of v_5 braking. The responsiveness of v_6 decreases

resulting in a harder collision. Thus, the more connected the successor is, the less responsive to an attack on the preceding vehicle.

VII. Key Findings

From the experimental results we identify four key findings:

1) In general, differing effects occur given change in target regardless of configuration. As the number of connections increase in undirected topologies, the attacker's advantage diminishes. However, targeting followers after v_1 in a fully networked platoon yields similar MAE across the platoon with no clear advantage for the attacker.
2) In PF configurations, all predecessors of the targeted vehicle are unaffected by the attack. The platoon becomes less resilient to attack as members to the rear of the platoon are connected to more predecessors. The results show that the greater the network connections of the successor of the targeted member, the greater the chance of collision.
3) Regardless of topology, the impact of each platoon member on the platoon depends on the controller responsiveness. Using the SMC controller, which is less responsive of the two controllers, results in more resilient control in all topologies except 1PF when compared to the proportional control of the LQR. In kNNN topologies, using SMC increases platoon robustness and resiliency, as evidenced by lower MAE and by maximum and minimum distances. These results indicate a disadvantage exists when using a highly responsive controller in a topology with more connections.
4) We also found that changes in the control policy affected performance and resilience. The CTG control policy is more resilient in 1PF and 1NNN topologies. However, as k increased in NNN topologies, the resiliency to attack decreased and the platoon became unstable. Overall, the CD control policy was the most resilient. Although the addition of a leader connection in the kNNLN topologies reduces resiliency to attack, it also increases robustness.

VIII. Conclusion

In this paper, we investigated platoon resiliency under physical attack of specific member with multiple topology-controller-policy configurations. The impact of attack on the platoon differed depending on the configuration and platoon member targeted for attack. We also discovered instabilities using the CTG control policy when using a topology where there is a high number of connections. This phenomenon requires further study. Future work may also include the investigation of more resilient control policies and consider the balance of controller responsiveness and jerk.

References

[1] S. E. Shladover, X.-Y. Lu, S. Yang, H. Ramezani, J. Spring, C. Nowakowski, D. Nelson, D. Thompson, A. Kailas, and B. McAuliffe, "CACC For Partially Automated Truck Platooning: Final Report," FHA–Exploratory Advanced Research Program, Tech. Rep., Mar. 2018.

[2] C. Bergenhem, E. Hedin, and D. Skarin, "Vehicle-to-Vehicle Communication for a Platooning System," *Procedia - Social and Behavioral Sciences*, vol. 48, pp. 1222–1233, 2012.

[3] H. Olufowobi and G. Bloom, "Chapter 16 - Connected Cars: Automotive Cybersecurity and Privacy for Smart Cities," in *Smart Cities Cybersecurity and Privacy*. Elsevier, Jan. 2019, pp. 227–240.

[4] S. J. Taylor, F. Ahmad, H. N. Nguyen, and S. A. Shaikh, "Vehicular Platoon Communication," *Sensors*, vol. 23, no. 1, p. 134, Jan. 2023.

[5] C. D. Hendrix and G. Bloom, "Platoon vulnerability due to network topology and targeted vehicle," in *IEEE Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, Jan. 2024.

[6] L. Xiao, F. Gao, and J. Wang, "On scalability of platoon of automated vehicles for leader-predecessor information framework," in *2009 IEEE Intelligent Vehicles Symposium*, Jun. 2009, pp. 1103–1108.

[7] S. Wen and G. Guo, "Control of Connected Vehicles in Road Network via Traffic Flow Information Feedback," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 12, pp. 14 267–14 280, Dec. 2023.

[8] E. van Nunen, J. Reinders, E. Semsar-Kazerooni, and N. van de Wouw, "String Stable Model Predictive Cooperative Adaptive Cruise Control for Heterogeneous Platoons," *IEEE Transactions on Intelligent Vehicles*, vol. 4, no. 2, pp. 186–196, Jun. 2019.

[9] M. Pirani, S. Baldi, and K. Johansson, "Impact of Network Topology on the Resilience of Vehicle Platoons," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–12, 2022.

[10] Y. Zheng, S. E. Li, J. Wang, L. Y. Wang, and K. Li, "Influence of information flow topology on closed-loop stability of vehicle platoon with rigid formation," in *17th International IEEE Conference on Intelligent Transportation Systems (ITSC)*, Oct. 2014, pp. 2094–2100.

[11] Z. Wang, Y. Bian, S. Shladover, G. Wu, S. E. Li, and M. J. Barth, "A Survey on Cooperative Longitudinal Motion Control of Multiple Connected and Automated Vehicles," *IEEE Intelligent Transportation Systems Magazine*, vol. 12, no. 1, pp. 4–24, 2020.

[12] S. Dadras, R. M. Gerdes, and R. Sharma, "Vehicular Platooning in an Adversarial Environment," in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*. Singapore Republic of Singapore: ACM, Apr. 2015, pp. 167–178.

[13] G. Guo and W. Yue, "Autonomous Platoon Control Allowing Range-Limited Sensors," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 7, pp. 2901–2912, Sep. 2012.

[14] Y. Zheng, S. E. Li, K. Li, and W. Ren, "Platooning of Connected Vehicles With Undirected Topologies," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 5, pp. 1353–1364, 2018.

[15] H. K. Khalil, *Nonlinear Systems*, 3rd ed. Prentice Hall, 2002.

[16] H. Lee and V. I. Utkin, "Chattering suppression methods in sliding mode control systems," *Annual Reviews in Control*, vol. 31, no. 2, pp. 179–188, Jan. 2007.

[17] Y. Zheng, S. E. Li, K. Li, and L.-Y. Wang, "Stability Margin Improvement of Vehicular Platoon Considering Undirected Topology and Asymmetric Control," *IEEE Transactions on Control Systems Technology*, vol. 24, no. 4, pp. 1253–1265, Jul. 2016.

[18] D. Swaroop and K. Rajagopal, "A review of constant time headway policy for automatic vehicle following," in *IEEE Intelligent Transportation Systems Proceedings*, Aug. 2001, pp. 65–69.

[19] P. Varaiya, "Smart cars on smart roads: problems of control," *IEEE Transactions on Automatic Control*, vol. 38, no. 2, pp. 195–207, Feb. 1993.

[20] M. Amoozadeh, H. Deng, C. Chuah, H. Zhang, and D. Ghosal, "Platoon mgmt with cooperative adaptive cruise control enabled by VANET," *Vehicular communications*, vol. 2, no. 2, pp. 110–123, 2015.

[21] J. Zhou and F. Zhu, "Analytical analysis of the effect of maximum platoon size of connected and automated vehicles," *Transportation Research Part C: Emerging Technologies*, vol. 122, p. 102882, Jan. 2021.

[22] N. Lyu, Y. Wang, C. Wu, L. Peng, and A. F. Thomas, "Using naturalistic driving data to identify driving style based on longitudinal driving operation conditions," *Journal of Intelligent and Connected Vehicles*, vol. 5, no. 1, pp. 17–35, Feb. 2022.

[23] K.-H. Dietsche, K. Reif, and et al., *Automotive Handbook*, 11th ed. Germany: Robert Bosch, Jan. 2022.