Platoon Vulnerability due to Network Topology and Targeted Vehicle

Constance Hendrix
University of Colorado Colorado Springs, CO, USA
chendr12@uccs.edu

Gedare Bloom
University of Colorado Colorado Springs, CO, USA
gbloom@uccs.edu

***Abstract*—**
Vehicle platooning is a key application for intelligent transportation systems that brings the joint problem of maintaining safety and security as prioritized requirements. The complex and dynamic electromagnetic environment coupled with sophisticated adversarial threats motivate better understanding of platoon control resilience from traditional faults, disturbances, and attack injects. An open problem for this understanding is the impact that information flow (communication network) topologies have on the attack and defense strategies for vehicular platoons. As the topology changes, vulnerability amongst platoon members and their individual contributions to the overall platoon security also change. This paper evaluates the impact of member-specific targeting informed by topology and demonstrates that targeting one member over another can be advantageous to the attacker. Furthermore, we present a taxonomy to identify topologies by key characteristics as an option for an industry standard.

***Index Terms*—autonomous vehicle, platoon, security, topology**

I. Introduction

Vehicle platoon technology promises energy efficiency and road capacity increase to serve our increasing population and global climate initiatives. A vehicle platoon is a network of two or more vehicles that is led by the front vehicle, which is called the leader. The leader is assumed to be controlled by a human driver [1], and following vehicles are controlled by a distributed controller. The leader and followers cooperatively travel as a spatially compressed unit along a road or highway. A platoon is characterized by four components: 1) vehicle dynamics, 2) formation geometry, 3) distributed controller, and 4) information flow topology [2]. First, the vehicle dynamics can be defined for each node as unique or assumed the same across all nodes within a platoon, signifying heterogeneous or homogeneous respectively. While the former is more realistic, the latter is more commonly used to eliminate parameters or variations which are deemed negligible or insignificant to the problem. Dynamics are inherently nonlinear, capturing longitudinal and lateral motion; however, these systems are commonly linearized around a set of assumptions. Formation geometry accounts for how desired spacing between vehicles is defined, which is translated into a distance-based control policy by the controller. Common policies include constant distance, constant time headway, and nonlinear distance [3]. Distributed control methods used in platoon control include H_∞, sliding mode, and model predictive control [4]. Finally, the network itself is configured using one of many topologies to exchange information between platoon members including predecessor following, predecessor-leader following, bi-directional, bi-directional leader, and two-predecessors following [5]–[7]. However, the naming of topologies tend to vary in many papers. Taylor et al.'s recent survey [8] highlights the requirement for topology standardization.

Stability within these platoon formations is a prioritized safety consideration because of the human-in-the-loop. Environmental disturbances and attack injects such as false data injection (FDI) and jamming seek to disrupt or disable vehicular platoon control actions [6], [8], [9]. The impact of these attacks may depend on topology or targeted platoon member. In this paper, we study the impact of disturbances and attacks on stability and system robustness as it pertains to specific members of the platoon across a plethora of network topologies parameterized by a platoon size N. Our contributions are:

1) an information flow topology taxonomy that better covers topological choices;
2) a concise unified topology-dependent control policy;
3) evaluation of targeted attacks on platoon members;
4) and, identification of vulnerable information flow topologies based on inter-vehicle spacing and string stability.

II. Related Work

To begin, a standard topology taxonomy is missing from literature [8]. Topologies are important because they greatly impact performance and are used to bound platoon research. Zheng et al. [10] demonstrated a platoon's topology impacts internal stability. Switching topologies have been considered due to loss and recovery of communication channels [4]. Taylor et al. [8] discussed centralized, decentralized, and hybrid topologies in their survey, arriving at unique challenges given topology. The taxonomy presented addresses the problem of standardization and provides a platform for this paper's evaluation of platoon vulnerability given a targeted follower.

Prior work largely concentrated on leader or last vehicle attacks in one topology [11], whole platoon attack [1], or using a specific vehicle for attack to analyze detection and mitigation techniques [12]. Work covering platoon impact given a targeted vehicle across a large range of topologies is not

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

readily available. The most closely related work investigates the robustness of platoon topologies. Pirani et al. [5] studied the impact of topology design on resiliency using graph theory and found that k-nearest neighbor ($k > 2$) and leader-to-all topologies provide the best connectivity thus more resilience to attack. However, the work does not answer address the impact of the platoon if one member is attacked over another given a specific topology.

III. Platoon Attacks

Adversaries could try to delay, split, impair, or disable the platoon, disable or impair the leader, or separate the last vehicle, either from within the platoon or externally. Attacks target one or more of the platoon's attack seams: communication network channel, navigation signal, and sensors [8]. In addition to attacks by electronic means, physical attacks should be considered. A malicious actor can easily throw an object in front of the vehicle to create a disturbance or collision.

To account for these two types, we created two attack models: a physical attack and an electronic false data injection (FDI) attack. Since we are bounding our study to longitudinal motion, we will not consider all possible attacks, instead focusing on the effects of an attack on the states. The effects of these attacks are used to evaluate platoon response across topologies. A temporal disturbance signal is applied to a member's acceleration to model the effect of braking in response to a physical disturbance as

$$e_i(t) = \begin{cases} -c_1(t - t_1) & t_1 < t < t_2 | t = \{0 : dt : t_{max}\} \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

where i is the targeted vehicle, t_1 and t_2 are the time bounds on braking, dt is the time step, t_{max} is the maximum (simulation) time, and c_1 is a constant increase or decrease in acceleration. Equation 2 characterizes an FDI attack by injecting a position offset [13] that is distributed to connected members as

$$e_i(t) = \begin{cases} \pm c_2 & t_1 < t < t_2 | t = \{0 : dt : t_{max}\} \\ 0 & \text{otherwise} \end{cases} \quad (2)$$

where c_2 is a constant position adjustment. In this attack, the targeted vehicle's controller is constantly attacked, which we model by a step input for the bias in contrast to alternatives that could model gradual, more stealthy injections.

IV. Vehicle Dynamic Model and Control

A homogeneous platoon system where each vehicle uses Cooperative Adaptive Cruise Control (CACC) to maintain a constant distance spacing control policy is assumed. Furthermore once brakes are applied, manual control overrides the CACC system until the brakes are released. Our model is a common dynamic model used for analysis of longitudinal control [14], [15]. The state equations $\dot{p}_i(t) = v_i(t)$, $\dot{v}_i(t) = a_i(t)$, and $\dot{a}_i(t) = \frac{1}{\tau_i}[-a_i(t) + u_i(t)]$ were reconstructed into a state space linear system model is as follows:

$$\dot{x}_i(t) = A_i x_i(t) + B_i u_i(t) + W_i e_i(t) \quad (3)$$

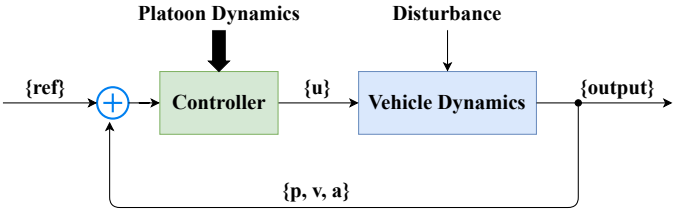


Fig. 1: Vehicle Closed-Loop System. The reference is the desired bumper-to-bumper distance.

$$y_i(t) = x_i(t) \quad (4)$$

$$A_i = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -1/\tau_i \end{bmatrix} B_i = \begin{bmatrix} 0 \\ 0 \\ 1/\tau_i \end{bmatrix} \quad (5)$$

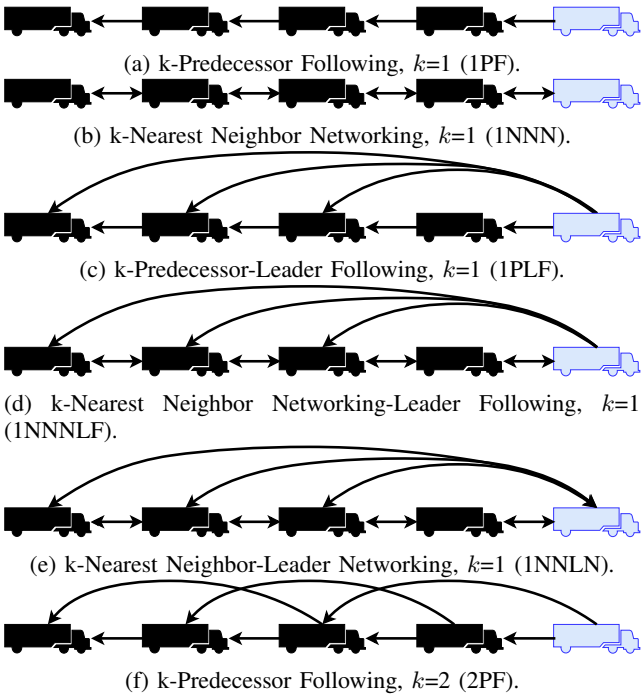
where the state vector is $x = \{p, v, a\}$—position, velocity, and acceleration—u is the control input, e is the error as discussed in Section III, i is the vehicle number, τ is the time delay, and W is solely dependent on the error injection due to attack. Perfect communication is assumed (i.e., no latency, noise, or propagation attenuation) to provide clarity to the results. A linear quadratic regulator (LQR) is used to control each vehicle. Given the zero-error state of Equation 3, the state-cost weight Q and input-cost weight R are selected heuristically using Bryson's rule in the infinite-horizon cost function, $J(u) = \int_0^\infty (x^T Q x + u^T R u) dt$. The input gain, β, in $u_i = \beta x_i$, is determined first by solving its algebraic Riccati equation, then its gain.

V. Taxonomy of Platoon Topologies

In this section, we introduce a novel taxonomy to characterize information flow topologies for platoons and use it to parameterize platoon control under attack. We begin by defining some key terms.

- Directed:
  - *Predecessor* (P): The nearest neighbor in the direction of the front of the platoon.
  - *Following* (F): Indicates half-duplex directional communication from the front of the platoon toward the rear.
- Undirected:
  - *Nearest Neighbor* (NN): The closest other vehicle in space within the platoon [16].
  - *Networking* (N): Indicates full-duplex or undirected communication channels between members.
- *Leader* (L): The vehicle, responsible for navigation and control, is normally the first or head vehicle of the platoon formation. If part of the topology name, communication channels (directed or undirected) will exist between the leader and all followers.
- k: The number of nearest neighbors or predecessors connected within the platoon.

We propose a taxonomy for platoons that covers the combinations of predecessor-following, nearest neighbor networking,



(a) k-Predecessor Following, k=1 (1PF).

(b) k-Nearest Neighbor Networking, k=1 (1NNN).

(c) k-Predecessor-Leader Following, k=1 (1PLF).

(d) k-Nearest Neighbor Networking-Leader Following, k=1 (1NNNLF).

(e) k-Nearest Neighbor-Leader Networking, k=1 (1NNLN).

(f) k-Predecessor Following, k=2 (2PF).

Fig. 2: Examples of Platoon Topology Taxonomy. The arrows represent the network edges, the light blue truck represents the leader, and the black trucks represent the followers.

leader following, and leader networking. Commonly used term *predecessor* is kept only to link research from previous papers with this proposed taxonomy. Also, k is used in almost all topologies, not just those with nearest-neighbor networking. Leader networking and leader following topologies would be the exception because intra-platoon communication between followers does not exist. Later in this paper, these two topologies are not considered because we seek to investigate the impact of intra-platoon communication between followers. Figure 2 shows the possible configurations of a platoon of size five using our taxonomy.

VI. Platoon Dynamic Model and Control

The platoon topology model is a graph $G = V, E$ where vehicles are nodes in V and the communication links between them are edges in E [2], [5]. In G, the adjacency matrix, Adj, and degree matrix, D, are used to calculate the Laplacian matrix, $L = D - Adj$, for each topology. The Laplacian matrix is lower triangular when connections are directed (i.e., Following topologies) and symmetric when connections are undirected (i.e., Networking topologies). For any topology in which a follower connects with the leader, we also use the diagonal pinning matrix

$$P_{ij} = \begin{cases} 1 & \text{if } i = j \text{ and } \exists \text{ a edge between } v_i \text{ and } v_0 \\ 0 & \text{otherwise,} \end{cases} \tag{6}$$

where v_0 is the leader. Any topology can be represented by $L + P$. A closed-loop system equation can then represent a homogeneous platoon with a rigid formation, including the topology's influence [10], as

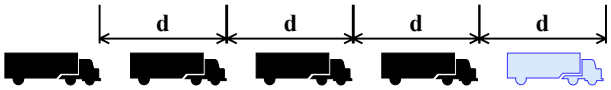


Fig. 3: Intra-Platoon Spacing Policy.

$$A_c = ([I_{N-1} \otimes A] - [(L + P) \otimes B\beta]) \tag{7}$$

$$\dot{X}_c = A_c X_c \tag{8}$$

where $\otimes$ is the Kronecker product, I the identity, A_c the closed-loop system matrix, and β the gain on the input which drives the dynamics, using method in [2], [10]. As an example for k-nearest neighbor topology with $k = 1$, the platoon state matrix becomes,

$$A_c = \begin{bmatrix} A & 0 & \cdots & 0 \\ 0 & A & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & A \end{bmatrix} - \begin{bmatrix} 2B\beta & -B\beta & \cdots & 0 \\ -B\beta & 2B\beta & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & B\beta \end{bmatrix} \tag{9}$$

Given $\beta = [\beta_1, \beta_2, \beta_3]$ represents the gain of each vehicle input u, and platoon homogeneity is assumed, Equation 10 better defines the input for each vehicle by including the leader and the constant distance linear control policy,

$$u_i(t) = -\frac{1}{diag(D+P)_i} \sum_{j \in \mathbb{N}_i} [\beta_1(p_i(t) - p_j(t) + d(i-j)) + \beta_2(v_i(t) - v_j(t)) + \beta_3(a_i(t) - a_j(t))] \tag{10}$$

where $D + P$ is used to scale the input and is dependent on the topology, and d is the setpoint distance between vehicles as shown in Figure 3.

VII. Evaluation

We focus on two aspects of platoon performance for evaluation: inter-vehicle spacing and string stability. All experimental data are obtained using MATLAB. For the purposes of this study, a platoon of size 7 is chosen, which is less than the maximum platoon size of 10, recommended across several studies [1], [17], [18], but large enough to study the impact of varying topologies while attacking different members of the platoon. A platoon size of 7 uses one of 20 unique communication configurations, out of 36 possible topologies, given our taxonomy and assumptions. Many LF and LN topologies produce the same $L+P$ matrix. Note that 5NNNLF, 5NNLN, 6NNN, 6NNNLF, and 6NNLN all represent a fully networked system. Ultimately, we found that with a platoon size of 7, $k \geq 5$ captures all possible unique configurations.

With the target inter-vehicle spacing set to 10 meters, we measure the inter-vehicle spacing to determine if the distance falls to 0, indicating a crash would occur. The distance between vehicles is therefore used as a primary metric for the safety of platoon topologies subject to attacks. Furthermore, we assume the leader maintains current acceleration and trajectory in response to an attack. Acceleration was held at a constant

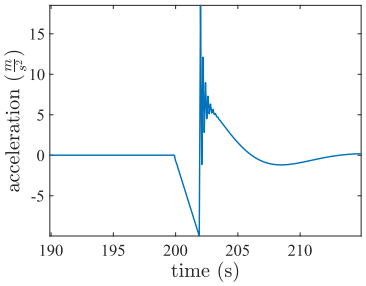


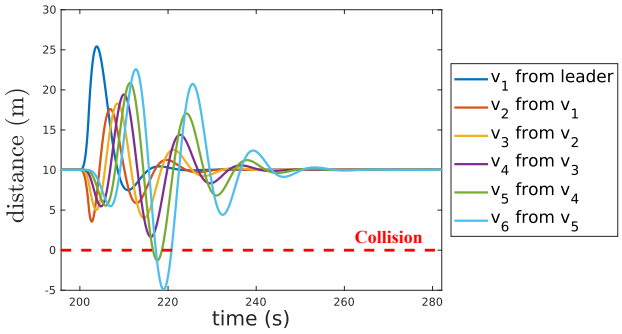
Fig. 4: Target Vehicle Acceleration. The target vehicle's braking response to a road obstruction applied for 2 seconds duration at 200 seconds.

$0.01\frac{m}{s^2}$, allowing the platoon's velocity to slowly increase over time. The time constant τ used in simulations (0.235 s) is derived from [19].

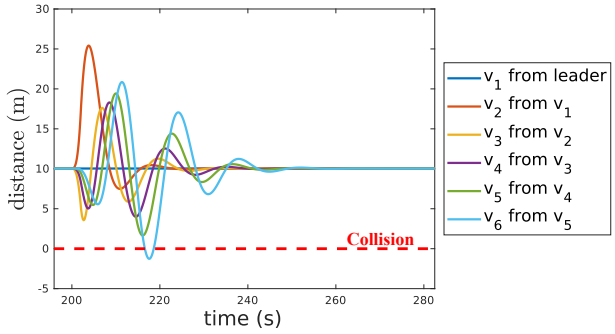
A. Physical (Obstacle) Attack Experiments

We add attack-induced ramp signal for braking in response to a physical obstacle in Equation 3. The effect of braking described in Equation 1 is applied to the acceleration of the targeted vehicle with $W_i = [0; 0; 1]$, as shown in Figure 4, to simulate a 2-second reaction to a physical obstruction. The controller reengages afterward to stabilize longitudinal motion. We applied the braking process individually across all members in each of the 20 topologies.

Figure 5 shows the disturbance applied to platoon members v_1 and v_2. In Figure 5a, distance between the leader and v_1 quickly increases from 10m to 25m, while other vehicle controllers react. Vehicles v_5 and v_6 collide with their predecessors, while large swings in spacing are created between remaining vehicles. If the disturbance is applied to v_2, collision only happens between v_5 and v_6. Analyzing the remaining responses for vehicle attacks using the the 1PF topology, the error amplifies down the platoon, suggesting string instability. If k is increased to 2 as shown in Figure 6a, this effect is diminished, but not eliminated, with the only collision occurring is between the targeted vehicle and its successor. For topology 1NNN (Figure 6b) the behavior changes. The first observation of interest is that v_2 collides with v_1. Although there were no other collisions, it takes longer for the platoon to return to a steady state in comparison to 1PF. As the disturbance was applied to each platoon member, the collision occurred between the targeted vehicle and its immediate successor except for v_5, which did not collide with v_6 because v_6 is the only vehicle which receives information from from its predecessor alone. The control action is strong enough to prevent a collision from occurring. For all other topologies, the collision only occurred between the targeted vehicle and its successor, duplicating the response shown in Figure 6a. The distance error was significantly reduced by the addition of leader networking and further reduced as k increased.



(a) Hard Braking from v_1.

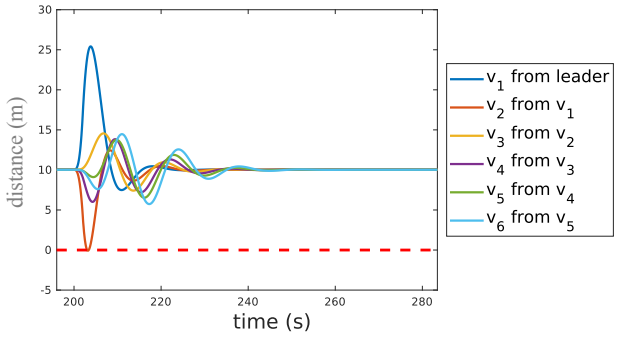


(b) Hard Braking from v_2.

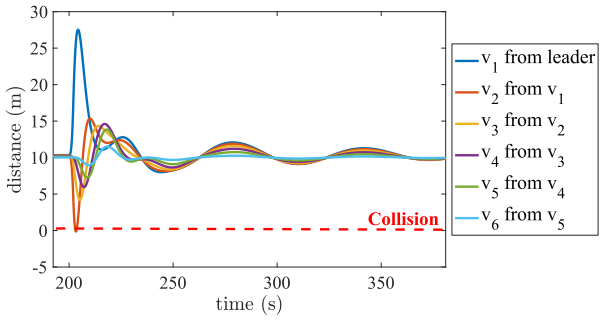
Fig. 5: 1PF Inter-Vehicle Spacing with Hard Braking.

B. FDI Attack Experiments

An FDI attack is simulated by adding a bias $W_i = [1; 0; 0]$ to the position state in Equation 3, as depicted in Equation 2 and shown in Figure 7. The simulation is run over 100 seconds. The attack occurs at 40 seconds and lasts for 10 seconds. During the attack, the controller remains engaged. The reaction of each platoon member was observed during attack of other platoon members for each topology. Figure 8 shows selected results from the FDI attacks. In general, most attacks targeting a particular vehicle caused the following vehicle to collide with it. For example, Figure 8a shows the inter-vehicle spacing between v_5 and v_6 in 1PF topology while each vehicle v_1-v_5 was attacked separately. Although the fastest (and apparently hardest) collision is when v_5 is attacked, the attacks on v_1 and v_2 also led to a collision. This coincides with the results in the previous subsection, demonstrating string instability. Surprisingly, in 5NNNLF and 5NNLN topologies all six platoon members are on equal standing with the leader, giving v_0's influence on v_1's control at $\frac{1}{6}$ of its influence as in the 1PF configuration. As shown in Figure 8b, the leader and v_1 collide with the same intensity regardless of which vehicle is attacked. Also, as k increased or a leader networking channel was added, the platoon as a whole reacted in more stable, non-oscillatory manner. At this point, we use a string stability metric to answer the questions of if and why the overall impact to the platoon varies based on topology and targeted follower.



(a) 2PF



(b) 1NNN

Fig. 6: Inter-Vehicle Spacing with Hard Braking from v_1.

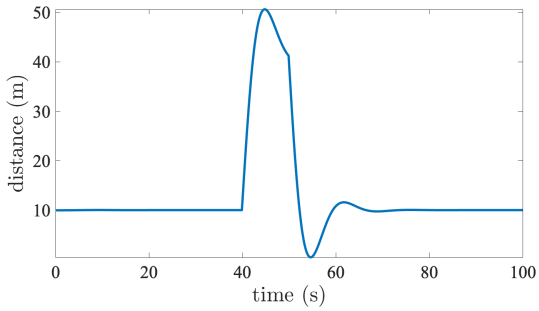
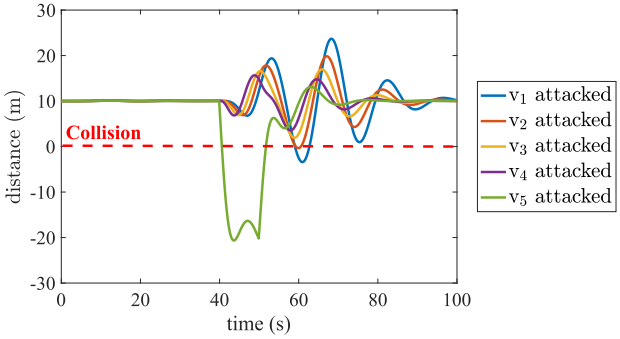
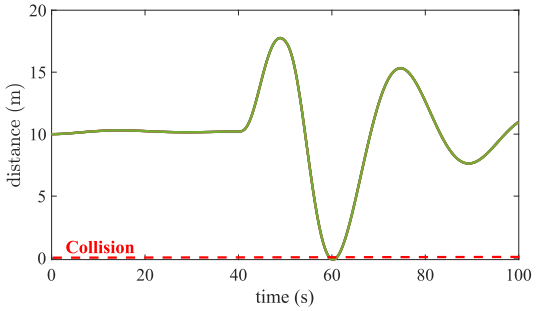


Fig. 7: Target Vehicle Position. Change in inter-vehicle spacing due to FDI attack against a targeted vehicle for 10 seconds at 40 seconds into the simulation.



(a) v_6 Behavior in 1PF based on target vehicle.



(b) v_1 Behavior in 5NNNLF and 5NNLN (regardless of target vehicle).

Fig. 8: Inter-Vehicle Spacing during FDI attack.

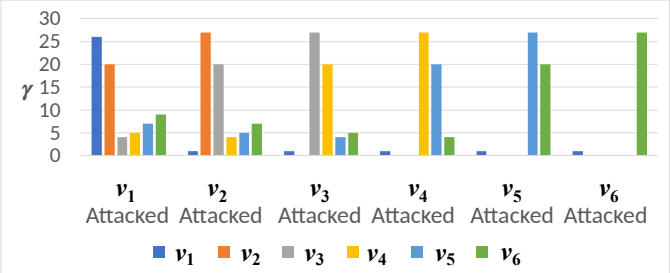
C. String Stability

String stability tracks the growth in error due to disturbances propagating through the platoon based on the magnitude output gain, γ, also known as L_2 Gain. This gain gives a measure of the platoon's sensitivity to an external disturbance [20]. We derive it as

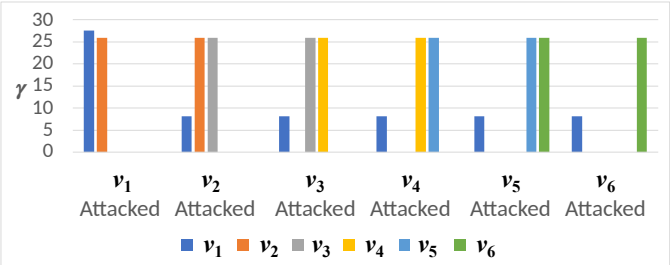
$$\gamma \text{ Gain} = \sup \frac{\|\Delta p(t)\|_{L_2}}{\|e(t)\|_{L_2}} \tag{11}$$

where Δp represents the position error, and e represents the external disturbance defined in Section III. The calculated gain is the maximum ratio between position error and disturbance over time. If a system is sensitive to errors, the γ gain will be high. Notable evidence of string instability in platoon size 7 was seen in the PF topologies in both attacks from the previous section, with the most amplification observed in 1PF, but this section's calculations are limited to the FDI attack due to its duration. Figure 9a shows the most impactful target to attack is v_1. The string instability inherent in 1PF causes the members toward the back of the platoon to be most vulnerable. We did not observe string instability in PLF and PFLN topologies, thus adding a leader channel appears to limit instability.

Figure 9 shows that in 5NNNLF and 5NNLN configurations, the middle members of the platoon are the most lucrative targets. This vulnerability stems from the number of connections those members have within the platoon. Error from attack propagates through the increased number of connections, making the overall impact to the platoon more substantial. Figure 10 shows the γ values averaged over each attack simulation per topology, which shows a few interesting trends. First, in NNN topologies, 1NNN displayed largest average error across the entire platoon. With this topology if v_2 is attacked, v_1 and v_3 receive the most error because both receive half of their platoon data from v_2. Second, v_6 is always the least impactful vehicle to target if disrupting the entire platoon is the goal. Third, for PF topology platoons, attacking v_1 has more impact to the platoon as whole when $k = 1$ and as k increases targeting v_1 becomes the least impactful (other than v_6). With the exception of 1PF, attacking v_1 with this inject would have the second least impact across the platoon. In general it is more impactful on the platoon to



(a) 1PF Topology.



(b) 5NNNLF and 5NNLN Topologies.

Fig. 9: γ Gains given an attack to a specific follower v_i.

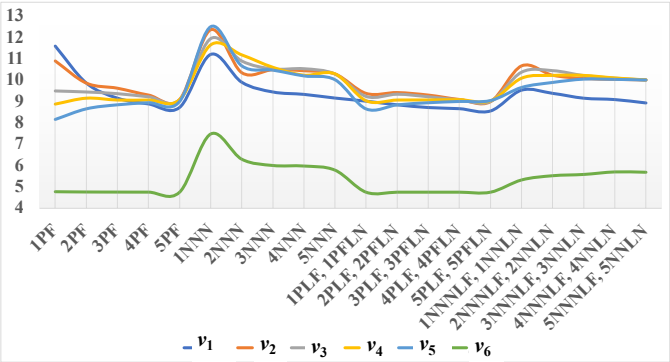


Fig. 10: Average γ Gains across the platoon given an attack to a specific follower v_i.

attack a middle member other than in 1PF. In NNNLF and NNLN topologies as k increases, all middle platoon members converge to the same value, suggesting the impact on the platoon would be similar despite which vehicle is attacked within the interior of the platoon.

VIII. Conclusion

In this paper, we presented a topology taxonomy to characterize information flow in platoons providing standardization that is currently lacking. We identified 20 unique topologies using platoon size 7 and evaluated the impact on the platoon given attacks against each platoon member for each topology. We discovered that attack-induced errors propagate differently through the platoon with changing topologies which results in differing platoon impact. In general, the first follower and the last follower have the least impact on the platoon in most topologies. Attacking middle members of the platoon is the most beneficial to the attacker except for 1PF and 2PF. The leader's decreasing influence on its follower (v_1) when using highly networked topologies causes it to be impacted the most when any other vehicle is attacked, with fully networked topologies showing the greatest impact. Future work could extend the understanding of topology-specific vulnerabilities on platoon formations by using different controllers and investigate methods to leverage the advantages of different formations in response to threats and changing conditions.

References

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

[2] Y. Zheng, S. Eben Li, J. Wang, D. Cao, and K. Li, "Stability and Scalability of Homogeneous Vehicular Platoon," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 1, pp. 14–26, Jan. 2016.

[3] S. Feng, Y. Zhang, S. E. Li, Z. Cao, H. X. Liu, and L. Li, "String stability for vehicular platoon control," *Annual Reviews in Control*, vol. 47, pp. 81–97, Jan. 2019.

[4] 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.

[5] 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.

[6] K. Kalogiannis, M. Khodaei, W. M. N. M. Bayaa, and P. Papadimitratos, "Attack Impact and Misbehavior Detection in Vehicular Platoons," in *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, May 2022, pp. 45–59.

[7] A. Ghosal, S. U. Sagong, S. Halder, K. Sahabandu, M. Conti, R. Poovendran, and L. Bushnell, "Truck platoon security: State-of-the-art and road ahead," *Computer Networks*, vol. 185, p. 107658, Feb. 2021.

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

[9] D. Ndambuki and H. Alhitmi, "Attack Mitigation and Security for Vehicle Platoon," *Journal of Cyber Security and Mobility*, pp. 497–530, Nov. 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] 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.

[12] H. Mokari, E. Firouzmand, I. Sharifi, and A. Doustmohammadi, "Deception Attack Detection and Resilient Control in Platoon of Smart Vehicles," in *2022 30th ICEE*, May 2022, pp. 29–35.

[13] Q. Luo, Y. Cao, J. Liu, and A. Benslimane, "Localization and Navigation in Autonomous Driving: Threats and Countermeasures," *IEEE Wireless Communications*, vol. 26, no. 4, pp. 38–45, Aug. 2019.

[14] 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.

[15] 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, May 2018.

[16] F. Preparata and M. Shamos, "Computational Geometry–An Introduction." *Mathematics of Computation*, vol. 47, no. 176, p. 763, Oct. 1986.

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

[18] 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.

[19] F. Gao, F.-x. Lin, and B. Liu, "Distributed H∞ Control Of Platoon Interacted by Switching and Undirected Topology," *International Journal of Automotive Technology*, vol. 21, no. 1, pp. 259–268, Feb. 2020.

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