# Invited: Waving the Double-Edged Sword: Building Resilient CAVs with Edge and Cloud Computing

Xiangguo Liu[1], Yunpeng Luo[2], Anthony Goeckner[1], Trishna Chakraborty[2], Ruochen Jiao[1], Ningfei Wang[2], Yixuan Wang[1], Takami Sato[2], Qi Alfred Chen[2], Qi Zhu[1]

2023 60th ACM/IEEE Design Automation Conference (DAC) | 979-8-3503-2348-1/23/$31.00 ©2023 IEEE | DOI: 10.1109/DAC56929.2023.10247809

***Abstract*—The rapid advancement of edge and cloud computing platforms, vehicular ad-hoc networks, and machine learning techniques have brought both opportunities and challenges for next-generation connected and automated vehicles (CAVs). On the one hand, these technologies can enable vehicles to leverage more computing power from edge and cloud servers and to share information with each other and surrounding infrastructures for better situation awareness and more intelligent decision making. On the other hand, the more distributed computing process and the wireless nature of V2X (vehicle-to-everything) communication expose vulnerabilities to various disturbances and attacks. In this paper, we discuss the security and safety challenges for edge- and cloud-enabled CAVs, particularly when they are under environment interferences, execution errors, and malicious attacks, and we will introduce our recent work and future directions in developing system-driven, end-to-end methodologies and tools to address these challenges and ensure system resiliency under uncertainties.**

***Index Terms*—connected and autonomous vehicles, edge computing, cloud computing, V2X, safety, security**

## I. Introduction

Machine learning techniques, especially neural network-based ones, are widely leveraged in autonomous driving (AD) for perception [1], prediction [2], planning [3], etc. Significant progress has been made to improve AD performance in various traffic scenarios, including more challenging ones such as unprotected left turn, highway merging and lane changing. Meanwhile, connected vehicle (CV) technologies via vehicular ad-hoc networks enable information sharing among vehicles and surrounding infrastructures. This provides a great complementary to the perception and prediction capabilities of individual vehicles, e.g., by sharing out-of-sight information or intentions that cannot be accurately predicted.

However, adopting these techniques requires significant amount of computational resources, which could be challenging to deploy on future production vehicles, considering the additional cost, energy overhead, hardware maintenance, etc. The advancement of edge and cloud computing provides an appealing way to overcome the computational resource limitation on individual vehicles. More specifically, for connected and autonomous vehicles (CAVs), they can communicate with edge devices that are roadside units (RSUs) and leverage their affiliated local sensors and servers, as well as with cloud devices that are far away and can connect to the internet for more information. The tasks with high resource demands and without real-time requirements, e.g., neural network model training, can be uploaded to the cloud, while the tasks with mild resource demands but requiring real-time communication, e.g., perception of the environment and coordination with other vehicles, can be handled by edge computing. Individual vehicles only need to equip the necessary hardware to maintain normal operation and ensure safety when edge and cloud computing are not available occasionally.

In the following, Section II discusses the promises of edge and cloud computiong for CAVs, while Section III presents the challenges brought by them. Section IV presents our system-driven integrated solutions for addressing the challenges.

## II. The Promises

Many works have shown that autonomous driving pipelines may perform poorly in long-tailed traffic scenarios (e.g., extreme weather conditions) and are vulnerable to various input noises and attacks such as stained traffic signs or dirty patches on the road [4]–[6]. Some methods and frameworks are proposed to enhance the safety of individual modules [7], [8] and the AD pipeline [9] of a single autonomous vehicle. With V2X communication, the safety of individual vehicles as well as the transportation systems can be further enhanced. Previous works have shown the promises of developing safety-assured and safety-driven frameworks for autonomous systems [10] by control invariant computation [11], by verification-guided control learning [12], and by joint certification and policy optimization in RL [13], [14]. With V2X communication, each vehicle can gather the intentions and state information of the surroundings to generate safety constraints, which can be ensured or optimized by reachability analysis and (control) barrier functions, as in [15].

With connectivity technology, vehicles can share their driving attitude [16], planned behavior, and trajectory, and may use this data to cooperate with each other. In this way, some challenging tasks, e.g., lane changing in dense traffic scenarios, can be executed safely and successfully in less time [17]–[19]. [17] points out that the system performance can be further improved as the number of connected and cooperative vehicles increases. Connectivity can also be incorporated with the sensor fusion module in vehicles, and such redundancy can increase the precision of state estimation, thus improving

This work is supported in part by NSF grants CNS-1834701, CNS-1724341, CNS-2038853, CNS-1850533, CNS-1929771, CNS-2145493, ONR grant N00014-19-1-2496, and USDOT under grant 69A3552047138.

[1]Department of Electrical and Computer Engineering, Northwestern University, USA. {xg.liu@u., anthony.goeckner@, ruochen.jiao@u., yixuanwang2024@u., qzhu@}northwestern.edu.

[2]Department of Computer Science, University of California, Irvine, USA. {yunpel3, trishnac, ningfei.wang, takamis, alfchen}@uci.edu.

system performance and robustness [18]. An edge device, as a local centralized coordinator, can collect information from multiple vehicles and send out motion suggestions more efficiently because it has a more comprehensive view of the dynamic environment and may avoid time-consuming consensus processes among vehicles.

However, edge and cloud computing also create new CAV security design opportunities, ranging from attack detection/prevention to data privacy and access control, as discussed below.

*Secure perception of infrastructure-authoritative information in AD:* Today, most existing works on attacks against AD systems target the detection/recognition of road information that is authoritative to the infrastructure side [20], for example the detection of traffic signs [4], [21]–[23] and traffic lights [24], [25]. With infrastructure-side communication devices such as RSUs, such a class of AD attacks can be greatly mitigated (if not directly eliminated) since CAVs can now directly obtain such authoritative information from the infrastructure side.

*Secure perception of dynamic road objects in AD:* Besides infrastructure-authoritative information, various existing AD attacks focus on dynamic road objects such as cars and pedestrians, for example hiding them from victims to cause crashes [26]–[42], or creating phantom ones in the road to cause emergency brake [25], [29], [39], [43]–[46]. If edge devices such as RSUs can have sensing capabilities (e.g., road-side cameras [47] and LiDAR, they can help defend against such attacks by sharing the infrastructure-side sensing results with CAVs so that the victim vehicles can have new fusion/cross-checking opportunities for attack detection/prevention.

*Secure self-localization in AD:* Various existing attack works also have demonstrated that the localization of AD vehicles can be vulnerable to external attacks such as sensor spoofing [5], [25], [48]. With information from other vehicles and edge devices such as RSU, the victim can have new chances in detecting and reacting to such attacks. For example, the other vehicles or the infrastructure can help localize the victim and thus help the victim detect the localization output deviations during attack. Also, since GPS signals from receivers in different positions may help identify GPS spoofing [49], the vehicles in proximity can share the raw GPS signals to allow new opportunities against existing GPS spoofing-based AD localization attacks [48].

*Enhanced road data privacy:* Collecting real-time traffic information can greatly benefit city-level information sharing and decision-making, but inevitably raise individual data privacy concerns. With edge computing devices such as RSUs, there exist new opportunities to process the real-time traffic data locally and share aggregated information (e.g., partial data, updated model parameters, calculated loss, etc.) to the city-level decision-making backend (e.g., traffic management center). For instance, several studies [50] [51] envision Federated Learning in CAVs that leverages the collaborative local training to minimize the individual privacy concern.

## III. The Challenges

Disturbance-prone communication may lead to significant challenges in ensuring system safety. While the use of edge and cloud computing in CAVs has potential to improve safety and security through information sharing and coordinated decision making, we highlight the following challenges:

*Communication latency:* If edge or cloud devices are part of a decision loop, latency in the network must be minimized such that the round-trip time is sufficient to avoid deadline misses in real-time decision making [52]. This is complicated by intermittent delays associated with the wireless V2X network, which we highlight in our previous works on CAV performance and safety [53]–[55]. However, many works such as [17] assume perfect communication and coordination between vehicles in planning, while others such as [18] consider possible message delay and loss in the planner design, but must be overly conservative to ensure safety.

*Communication reliability:* Due to their wireless medium, V2X networks are subject to both natural and malign disturbances which prevent message reception. This may manifest as either intermittent disturbance, with a few lost messages, or steady disturbance, where the channel is blocked for a long period of time (e.g. jamming or flooding attacks). This vector is further explored in our prior work on weakly-hard communication models [56]. CAV applications must successfully recognize and adapt to such situations.

*Network bandwidth:* Current V2X networks have strict bandwidth constraints. This significantly limits the amount of real-time data which may be transmitted and limits the options available for message authentication or encryption. In congested scenarios, the inter-packet gap between safety messages may be several seconds [57], resulting in periods during which safety information is outdated. For safe control, such gaps may need to be filled using predictions [2], [17].

There are many other security challenges, ranging from new threat actors and new attack surfaces at both cyber- and physical- layers to new privacy challenges.

*New threat from malicious/compromised RSUs/CAVs:* Since the core benefits of V2X come from making use of the road information shared by other entities (e.g., RSUs and other CAVs), edge- and cloud-enabled CAVs face a new security threat in which such other entities can be malicious/compromised such that attackers can turn information-sharing channels into attacking channels. For example, if the ego CAV blindly trusts the information shared by other CAVs, the attacker can exploit this trust by sharing falsified information to cause erroneous driving behaviors of the victim, e.g., by sending a spoofed message reporting that a pedestrian out of the sensing range of the ego CAV is about to quickly enter the road (e.g., from behind a bus) to trigger an unnecessary emergency brake.

*New cyber-layer attack surface:* As a networking technology, the deployment of V2X by nature introduces new cyber-attack surfaces to the participating vehicles and transportation systems. For example, a network attacker in the V2X communication range can violate the confidentiality, integrity, and

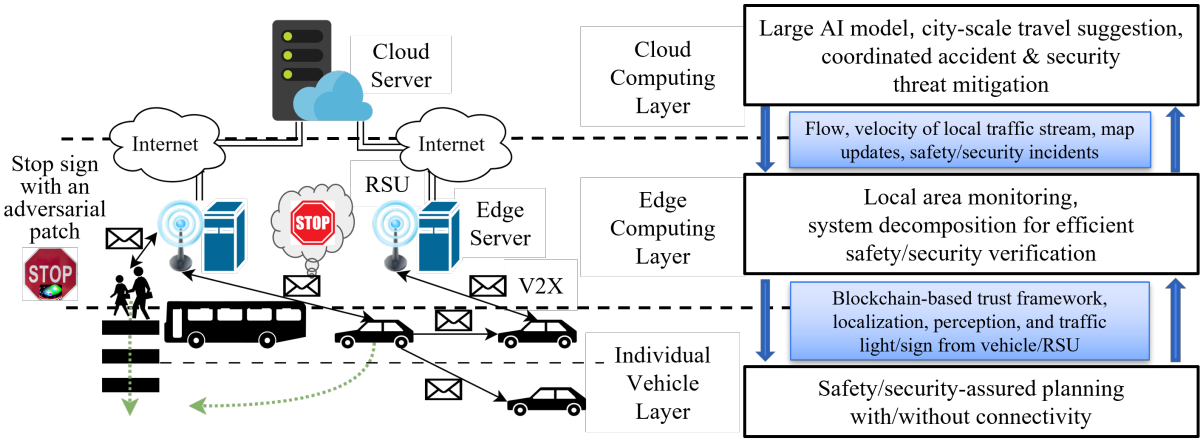


Fig. 1. Our proposed cross-layer framework for assured edge and cloud computing for CAVs.

authenticity of the real-time road information shared via V2X by exploiting V2X protocol design flaws or implementation bugs [58], [59], and may disrupt the V2X availability using network denial-of-service (DoS) attacks such as jamming. The newly-introduced edge devices such as RSUs can also become new attack entry points for breaking into the internal transportation infrastructure systems.

*New physical-layer attack surface:* Recent works have discovered a wide range of physical-layer attacks against the AI stack in AD systems (e.g., adversarial physical patches [5], [22], [23], [60], obstacles [6], [26], [61], laser blinding [26], [45], & GPS spoofing [24], [48]). In the edge- and cloud-enabled CAV ecosystem, the newly-introduced edge devices can become new physical-layer attack targets, for example by performing sensor attacks against RSU-mounted cameras/LiDARs instead of (or in combination with) the CAV-mounted ones. Since the RSU-mounted sensor locations are fixed, they are actually more vulnerable to such attacks, since the attacks no longer suffer from the complication of moving targets [5]. What's worse, as the RSU's sensing results can now be shared with multiple CAVs via V2X, one adversarial attack can now propagate and affect multiple victims simultaneously.

*New privacy challenges to road users:* In edge- and cloud-enabled V2X settings, each CAV needs to frequently share information about itself (e.g., identity, location, speed, and heading) and the surrounding physical environment to other vehicles, edge devices, and transportation infrastructure, which poses unprecedented privacy concerns for road users. For example, prior works point out that such broadcast V2X information may be used to infer sensitive information such as home addresses and whereabouts of drivers and passengers [62].

## IV. The Solutions

In light of these challenges, we propose a cross-layer framework to provide *assured edge and cloud computing for CAVs*. This may be seen in Fig. 1. At the cloud computing layer, large AI models for perception, prediction, and planning will be trained and maintained on cloud servers, and offline reachability analysis for systems using these models can be conducted for safety assurance. The cloud computing layer will also provide city-scale travel suggestions and coordinated accident and security threat mitigation strategies based on the local traffic status shared by edge devices. At the edge computing layer, edge servers (RSUs) will directly coordinate with surrounding traffic participants, including monitoring the communication channel and physical motion status of vehicles, and will decompose the dynamic system into many subsystems for more efficient safety and security verification. At the individual vehicle layer, every vehicle is responsible for preventing collisions with others, even if the communication channel and edge devices are occasionally unavailable for assistance.

The information shared across adjacent layers is also presented in Fig. 1. Between the cloud computing and edge computing layers, the shared status of local traffic streams and map updates supports timely city-scale coordination and planning. Reported safety and security incidents mitigate impacts and help to improve the models. Between the edge computing and individual vehicle layers, information related to localization, perception, and traffic signals can be shared. For instance, with the shared information, we can build a Sybil attack detection system [63] based on a credibility-enhanced temporal graph convolutional neural network to defend edge computing servers against Sybil attacks. At the same time, a cyber-physical credibility framework based on blockchain technology and vehicles' physical sensing capabilities can be maintained to build trust for connected vehicles [64], enabling quick reaction to attacks in a large-scale vehicular network with low resource overhead. Initial studies of such techniques have demonstrated effectiveness in defense against spoofing attacks, bad-mouthing attacks, and Sybil and voting attacks.

## V. Conclusion

In this work, we have presented a high-level view onto the challenges and promises of edge and cloud computing for CAVs. We hope that our work will inspire others to pick up the double-edged sword of edge & cloud computing for CAVs.

## REFERENCES


[1] R. Qian, X. Lai, and X. Li, "3d object detection for autonomous driving: a survey," *Pattern Recognition*, vol. 130, p. 108796, 2022.

[2] R. Jiao, X. Liu *et al.*, "Tae: A semi-supervised controllable behavior-aware trajectory generator and predictor," in *IROS*. IEEE, 2022.

[3] X. Liu, C. Huang *et al.*, "Physics-aware safety-assured design of hierarchical neural network based planner," in *ICCPS*, 2022.

[4] S.-T. Chen, C. Cornelius *et al.*, "Shapeshifter: Robust physical adversarial attack on faster r-cnn object detector," in *ECML PKDD 2018*.

[5] T. Sato, J. Shen *et al.*, "Dirty Road Can Attack: Security of Deep Learning based Automated Lane Centering under Physical-World Attack," in *USENIX Security*, 2021.

[6] Q. Zhang, S. Hu *et al.*, "On Adversarial Robustness of Trajectory Prediction for Autonomous Vehicles," in *CVPR*, 2022.

[7] B. Yang, R. Guo *et al.*, "Radarnet: Exploiting radar for robust perception of dynamic objects," in *ECCV*. Springer, 2020, pp. 496–512.

[8] R. Jiao, X. Liu *et al.*, "Semi-supervised semantics-guided adversarial training for trajectory prediction," *arXiv preprint arXiv:2205.14230*.

[9] R. Jiao, H. Liang *et al.*, "End-to-end uncertainty-based mitigation of adversarial attacks to automated lane centering," in *2021 IEEE IV*.

[10] Q. Zhu, C. Huang *et al.*, "Safety-assured design and adaptation of learning-enabled autonomous systems," in *26th ASP-DAC*, 2021.

[11] Y. Wang, C. Huang, and Q. Zhu, "Energy-efficient control adaptation with safety guarantees for learning-enabled cyber-physical systems," in *ICCAD*, 2020.

[12] Y. Wang, C. Huang *et al.*, "Design-while-verify: correct-by-construction control learning with verification in the loop," in *DAC*, 2022.

[13] ——, "Joint differentiable optimization and verification for certified reinforcement learning," *arXiv preprint arXiv:2201.12243*, 2022.

[14] Y. Wang, S. S. Zhan *et al.*, "Enforcing hard constraints with soft barriers: Safe reinforcement learning in unknown stochastic environments," *arXiv preprint arXiv:2209.15090*, 2022.

[15] H. S. Ahmad, E. Sabouni *et al.*, "Evaluations of cyberattacks on cooperative control of connected and autonomous vehicles at bottleneck points."

[16] X. Liu, N. Masoud, and Q. Zhu, "Impact of Sharing Driving Attitude Information: A Quantitative Study on Lane Changing," in *IEEE IV*.

[17] X. Liu, R. Jiao *et al.*, "Connectivity enhanced safe neural network planner for lane changing in mixed traffic," *arXiv preprint arXiv:2302.02513*.

[18] K. K.-C. Chang, X. Liu *et al.*, "A safety-guaranteed framework for neural-network-based planners in connected vehicles under communication disturbance," in *2023 DATE*.

[19] X. Liu, R. Jiao *et al.*, "Safety-driven interactive planning for neural network-based lane changing," in *28th ASP-DAC*, 2023.

[20] J. Shen, N. Wang *et al.*, "SoK: On the Semantic AI Security in Autonomous Driving," *arXiv preprint arXiv:2203.05314*, 2022.

[21] G. Lovisotto, H. Turner *et al.*, "SLAP: Improving Physical Adversarial Examples with Short-Lived Adversarial Perturbations," in *USENIX Security*, 2021.

[22] Y. Zhao, H. Zhu *et al.*, "Seeing isn't believing: Towards more robust adversarial attack against real world object detectors," in *CCS*, 2019.

[23] W. Jia, Z. Lu *et al.*, "Fooling the Eyes of Autonomous Vehicles: Robust Physical Adversarial Examples Against Traffic Sign Recognition Systems," in *NDSS*, 2022.

[24] K. Tang, J. Shen *et al.*, "Fooling Perception via Location: A Case of Region-of-Interest Attacks on Traffic Light Detection in Autonomous Driving," in *AutoSec*, 2021.

[25] W. Wang, Y. Yao *et al.*, "I Can See the Light: Attacks on Autonomous Vehicles Using Invisible Lights," in *CCS*, 2021.

[26] Y. Cao, N. Wang *et al.*, "Invisible for both Camera and LiDAR: Security of Multi-Sensor Fusion based Perception in Autonomous Driving Under Physical-World Attacks," in *IEEE S&P*, 2021.

[27] L. Ding, Y. Wang *et al.*, "Towards Universal Physical Attacks on Single Object Tracking," in *AAAI*, 2021.

[28] Z. Hau, K. T. Co *et al.*, "Object removal attacks on lidar-based 3d object detectors," *arXiv:2102.03722*, 2021.

[29] X. Ji, Y. Cheng *et al.*, "Poltergeist: Acoustic Adversarial Machine Learning against Cameras and Computer Vision," in *IEEE S&P*, 2021.

[30] Y. Li, C. Wen *et al.*, "Fooling lidar perception via adversarial trajectory perturbation," *arXiv:2103.15326*, 2021.

[31] K. K. Nakka and M. Salzmann, "Indirect Local Attacks for Context-Aware Semantic Segmentation Networks," in *ECCV*, 2020.

[32] J. Tu, H. Li *et al.*, "Exploring Adversarial Robustness of Multi-Sensor Perception Systems in Self Driving," *arXiv:2101.06784*, 2021.

[33] J. Tu, M. Ren *et al.*, "Physically Realizable Adversarial Examples for LiDAR Object Detection," in *CVPR*, 2020.

[34] J. Wang, A. Liu *et al.*, "Dual Attention Suppression Attack: Generate Adversarial Camouflage in Physical World," in *CVPR*, 2021.

[35] R. Wiyatno and A. Xu, "Physical Adversarial Textures That Fool Visual Object Tracking," in *ICCV*, 2019.

[36] Z. Wu, S.-N. Lim *et al.*, "Making an invisibility cloak: Real world adversarial attacks on object detectors," in *ECCV*, 2020.

[37] C. Xiao, D. Yang *et al.*, "MeshAdv: Adversarial Meshes for Visual Recognition," in *CVPR*, 2019.

[38] K. Xu, G. Zhang *et al.*, "Adversarial t-shirt! evading person detectors in a physical world," in *ECCV*, 2020.

[39] C. Yan, W. Xu *et al.*, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," *DEFCON*, 2016.

[40] Y. Zhang, H. Foroosh *et al.*, "CAMOU: Learning physical vehicle camouflages to adversarially attack detectors in the wild," in *ICLR*, 2018.

[41] Y. Zhu, C. Miao *et al.*, "Can We Use Arbitrary Objects to Attack LiDAR Perception in Autonomous Driving?" in *CCS*, 2021.

[42] X. Zhu, X. Li *et al.*, "Fooling thermal infrared pedestrian detectors in real world using small bulbs," in *AAAI*, 2021.

[43] Y. Cao, C. Xiao *et al.*, "Adversarial Sensor Attack on LiDAR-based Perception in Autonomous Driving," in *CCS*, 2019.

[44] B. Nassi *et al.*, "Phantom of the ADAS: Securing Advanced Driver-Assistance Systems from Split-Second Phantom Attacks," in *CCS*, 2020.

[45] J. Sun, Y. Cao *et al.*, "Towards Robust LiDAR-based Perception in Autonomous Driving: General Black-box Adversarial Sensor Attack and Countermeasures," in *USENIX Security*, 2020.

[46] K. Yang, T. Tsai *et al.*, "Robust Roadside Physical Adversarial Attack Against Deep Learning in LiDAR Perception Modules," in *CCS*, 2021.

[47] "Siemens Mobility, Bosch introduce fully integrated V2X collective perception system," Mar. 2021.

[48] J. Shen, J. Y. Won *et al.*, "Drift with Devil: Security of Multi-Sensor Fusion based Localization in High-Level Autonomous Driving under GPS Spoofing," in *USENIX Security*, 2020.

[49] N. O. Tippenhauer, C. Pöpper *et al.*, "On the requirements for successful GPS spoofing attacks," in *CCS '11*, 2011, p. 75.

[50] J. Posner, L. Tseng *et al.*, "Federated learning in vehicular networks: Opportunities and solutions," *IEEE Network*, 2021.

[51] S. R. Pokhrel and J. Choi, "A decentralized federated learning approach for connected autonomous vehicles," in *IEEE WCNCW*, 2020.

[52] Z. Wang, H. Liang *et al.*, "Cross-Layer Design of Automotive Systems," *IEEE Design Test*, vol. 38, no. 5, pp. 8–16, Oct. 2021.

[53] B. Zheng, C.-W. Lin *et al.*, "Delay-Aware Design, Analysis and Verification of Intelligent Intersection Management," in *2017 SMARTCOMP*.

[54] ——, "Design and Analysis of Delay-Tolerant Intelligent Intersection Management," *ACM T-CPS*, vol. 4, no. 1, pp. 3:1–3:27, Nov. 2019.

[55] ——, "CONVINCE: A cross-layer modeling, exploration and validation framework for next-generation connected vehicles," in *ICCAD*, 2016.

[56] C. Huang, K. Wardega, W. Li, and Q. Zhu, "Exploring weakly-hard paradigm for networked systems," in *DESTION*, 2019.

[57] H. I. Abbasi, R. Gholmieh *et al.*, "LTE-V2X (C-V2X) Performance in Congested Highway Scenarios," in *ICC 2022*.

[58] S. Hu, Q. A. Chen *et al.*, "Automated Discovery of Denial-of-Service Vulnerabilities in Connected Vehicle Protocols," in *Usenix Security*.

[59] Q. A. Chen, Y. Yin *et al.*, "Exposing Congestion Attack on Emerging Connected Vehicle based Traffic Signal Control," in *NDSS*, 2018.

[60] Y. Jia, Y. Lu *et al.*, "Fooling Detection Alone is Not Enough: Adversarial Attack against Multiple Object Tracking," in *ICLR*, 2020.

[61] Z. Wan, J. Shen *et al.*, "Too Afraid to Drive: Systematic Discovery of Denial-of-Service Vulnerability in Autonomous Driving Planning under Physical-World Attacks," in *NDSS*, 2022.

[62] Z. Cai and A. Xiong, "Understand Users' Privacy Perception and Decision of V2X Communication in Connected Autonomous Vehicles," in *Usenix Security Symposium*, 2023.

[63] B. Luo, X. Liu, and Q. Zhu, "Credibility enhanced temporal graph convolutional network based sybil attack detection on edge computing servers," in *2021 IEEE IV*.

[64] X. Liu, B. Luo *et al.*, "Securing connected vehicle applications with an efficient dual cyber-physical blockchain framework," in *2021 IEEE IV*.