2025 IEEE Intelligent Vehicles Symposium (IV)
June 22-25, 2025. Cluj-Napoca, Romania

Steering into Danger: Security Vulnerabilities in Steer-by-Wire and Steering Wheel-less Vehicles

Bhagawat Baanav Yedla Ravi and Sandip Ray
Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611, USA.
b.yedlaravi@ufl.edu, sandip@ece.ufl.edu.

2025 IEEE Intelligent Vehicles Symposium (IV) | 979-8-3315-3803-3/25/$31.00 ©2025 IEEE | DOI: 10.1109/IV64158.2025.11097437

***Abstract*—Steer-by-Wire (SbW) systems revolutionize automotive technology by eliminating the mechanical linkage between the steering wheel and tires, enhancing design flexibility and performance, especially in autonomous vehicles. However, this reliance on sensors and electronic data channels introduces critical security vulnerabilities. Exposed sensor locations in modern vehicles increase susceptibility to cyberattacks and physical interference, yet prior research has largely overlooked SbW-specific threats, particularly position encoders. This paper is the first to experimentally analyze SbW security vulnerabilities, presenting a novel attack methodology that disrupts SbW sensors. Our findings demonstrate how these vulnerabilities can compromise steering operations, posing severe risks to vehicle dynamics and occupant safety. As autonomous vehicles eliminate manual intervention, addressing these security risks becomes urgent. This study lays a foundation for developing more resilient SbW systems, ensuring safer and more secure automotive technologies.**

I. Introduction

Steer-by-wire (SbW) represents a transformative innovation in automotive technology, eliminating the mechanical linkage between the steering wheel and the tires. This shift offers numerous benefits for both drivers and manufacturers. By removing components like steering columns and hydraulic systems, SbW reduces vehicle weight, improving fuel efficiency and performance. It also provides enhanced design flexibility, allowing designers to optimize vehicle layouts, enhance interiors, and integrate innovative features such as collapsible steering columns. SbW enables precise steering adjustments tailored to driving conditions, supports customization [1] through variable steering ratios and sensitivities, and enhances safety by incorporating multiple layers of electronic and software redundancies. Integration with advanced driver-assistance systems (ADAS) further strengthens safety through features like lane-keeping assist and automatic collision avoidance. Moreover, SbW systems are ideally suited for autonomous vehicles [2], offering seamless integration with self-driving algorithms and control systems, while their electronic control architecture enables remote steering operations, critical for autonomous fleet management. Exposed SbW sensors in low ground clearance vehicle designs as shown in Fig.1 are highly vulnerable to malfunctions, cyberattacks, and targeted physical interference.

This paper analyzes security vulnerabilities in Steer-by-Wire systems with a focus on real-world experimentation. Following are the key contributions of this paper.

- We provide to our knowledge the first experimental demonstration of security vulnerabilities in SbW systems with real attack scenarios.
- We design and implement a configurable SbW setup that closely replicates real-world systems, ensuring accurate observations and practical relevance.
- We introduce a physical domain attack that manipulates the sensors in the SbW system that disrupts steering operations.
- We provide an extensive experimental evaluation of the impact of attacks in both static and dynamic steering conditions, providing insights to their severity and real-world implications.
- We develop a configurable platform for the exploration of SbW security, including attack propagation and vulnerabilities in other potential attack entryways.

The remainder of the paper is structured as follows: Section II discusses the typical functioning of Steer by Wire Systems. Section III discusses the challenges involved in Steer by Wire Systems. Section IV shows our custom designed SbW setup. Section V describes the attacks on SbW systems in detail and analyses the functioning of the system in both attack and benign scenarios. Section VI concludes the paper.

II. Steer by Wire Systems

SbW systems function by replacing the traditional mechanical connection between the steering wheel and the tires with an electronic control system. When the driver turns the steering wheel, sensors capture the input, such as the angle and torque applied. This data is processed by an electronic control unit (ECU), which calculates the appropriate response based on the vehicle's speed, road conditions, and other dynamic factors. The ECU then sends electrical signals to actuators located at the wheels, which adjust the steering angle accordingly. Feedback actuators in the steering wheel provide haptic feedback to the driver, simulating the feel of a traditional steering system by replicating road resistance and conditions [3]. Advanced SbW systems also integrate with other vehicle systems, such as suspension, braking, and stability control, to deliver precise and adaptive steering performance. This setup enables features like variable steering ratios, autonomous steering adjustments, and enhanced safety functionalities such as lane-keeping assistance and collision avoidance.

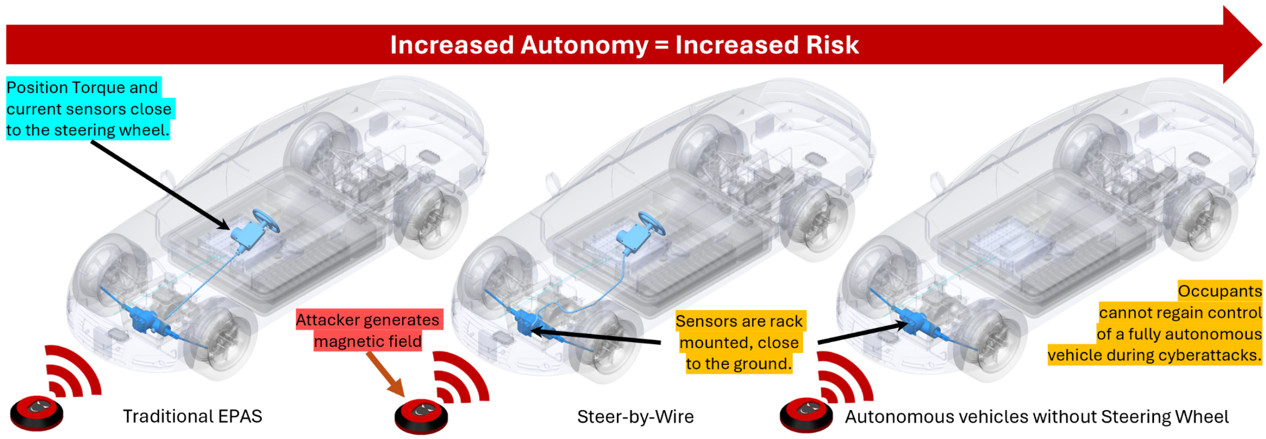

Figure 1. As vehicles transition toward full autonomy, the need for a steering wheel in the cabin is eliminated. However, this evolution significantly increases the risk of cybersecurity vulnerabilities. Sensors critical to steering, such as position and current sensors near the steering rack, are located closer to the ground, making them more accessible to adversaries for potential attacks. In the absence of a steering wheel, a fully autonomous vehicle becomes incapable of recovering from a compromised system, amplifying the consequences of such vulnerabilities.

Due to the absence of a mechanical connection between the Hand Wheel (HW) and the Road Wheel (RW) in SbW systems, achieving two critical functions—path tracking and realistic haptic feedback—requires proper control methods. Several approaches [4] are utilized for implementing SbW system control, which can be categorized into four main methods:

Model-Based Control Technique: This torque sensorless approach uses dynamic mathematical models [5], such as the bicycle model [6] or advanced multi-degree-of-freedom models, to optimize SbW control. Techniques like particle swarm optimization (PSO) enhance parameter tuning, but the method requires extensive computation and relies heavily on accurate modeling.

Torque Map Control Method: This method uses lookup tables [7] to determine steering wheel torque based on vehicle speed, yaw rate, and HW angle. It provides simple and efficient control with customization options like reactive torque maps [8] and variable gear ratios. However, its reliance on fixed maps limits flexibility.

Direct Current Measurement Control Method: By using inexpensive current sensors to measure motor phase currents [9] [10], this method calculates torque for artificial haptic feedback. It also provides fault diagnostics and employs a PID controller for RW motor control. While cost-effective, it is less accurate than other methods.

Torque Sensor-Based Control Approaches: This highly accurate method uses torque and angle sensors in various configurations [11] [12] for HW and RW control. Despite its reliability, it is costly and faces operational challenges but it remains the benchmark for precise SbW performance.

Each SbW control technique has unique advantages and trade-offs. Model-based control offers adaptability but is computationally demanding, torque map control is simple and customizable but inflexible, and direct current measurement is cost-effective but less precise. Torque sensor-based methods provide high accuracy but are expensive. All techniques rely on a position sensor in the RW steering rack for real-time feedback. Notably, the direct current measurement method uses Hall effect sensors to evaluate torque, making it susceptible to attacks that can compromise vehicle functionality.

III. Challenges in Steer by Wire Systems

Malfunctions in SBW systems can have catastrophic consequences [13], largely due to the absence of a mechanical shaft that provides direct feedback to the driver about wheel positions. Without this feedback, any system malfunction or cyberattack could cause the vehicle to behave contrary to the driver's input, leaving the driver unaware of the issue. This risk is particularly critical in scenarios requiring rapid responses, as drivers often lack the time to recognize and adapt to sudden, unexpected behavior [14]. Modern vehicles with rear-wheel steering, designed for tighter turns and smoother lane changes, face the same vulnerabilities, with potentially even more severe outcomes compared to front-wheel SbW systems. Sensors play a pivotal role in SbW functionality but also represent a significant source of vulnerability. Systems typically rely on Hall effect-based position sensors, current sensors, and voltage sensors [15], chosen for their robustness and reliability in automotive applications. However, Hall effect sensors are highly susceptible to external electromagnetic interference, a critical weakness that can compromise their performance. While previous research has focused on Hall effect sensor attacks in power systems, there has been little to no exploration of their vulnerabilities in position encoders or SbW systems. SbW systems rely on sensors in exposed areas like the steering rack (Fig. 1), making them vulnerable to attacks due to their proximity to the ground. Modern low-clearance vehicle designs further increase this risk, allowing easier placement of disruptive devices. SbW systems are also dependent on data from multiple sensors to determine key parameters such as steering feel, sensitivity, feedback,

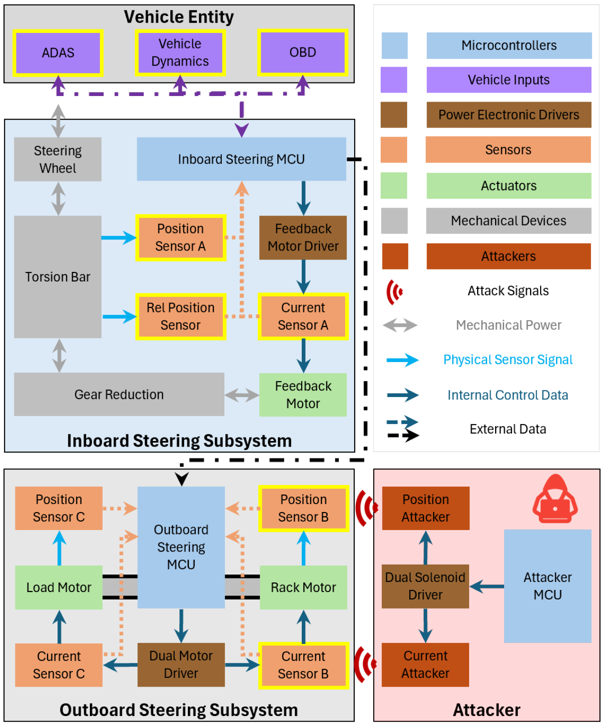

Figure 2. Steer by Wire system architecture showing inboard, outboard subsystems, and the attacker. Potential attack entryways are outlined in yellow.

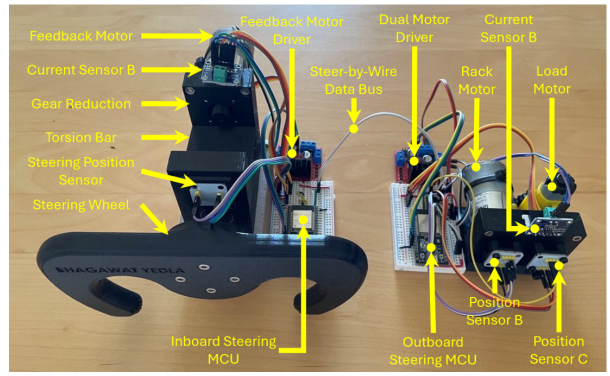

Figure 3. Steer by Wire system implementation showing inboard and outboard sub-systems.

and response, which creates additional vulnerabilities to data channel attacks. In a future dominated by self-driving taxis without steering wheels, such security breaches could leave occupants unable to respond to vehicle malfunctions, resulting in highly distressing and potentially dangerous situations.

IV. Steer by Wire Implementation

To perform experimentation, we architected a configurable Steer-by-Wire (SbW) system (Fig. 2). The system implementation (Fig. 3) focuses on realism to ensure that the results closely correlate with real-world scenarios. The system is configurable to accommodate all four previously mentioned control strategies. The system comprises two primary subsystems: the Inboard Steering Subsystem and the Outboard Steering Subsystem, which together emulate the core components and functionalities of a practical SbW system.

1) Inboard Steering Subsystem: The inboard steering subsystem is present inside the cabin. It consists of a steering wheel (Hand Wheel, HW), a steering angle sensor (Position Sensor A) to measure the angular position of the HW and a torsion bar or torque shaft that deforms angularly under the applied steering torque. At the opposite end of the torsion bar, another position sensor (Position Sensor B) measures the deformed angle, allowing for precise torque estimation. To provide realistic haptic feedback to the driver, a feedback motor is connected to the torsion bar via a gear reduction system. The feedback motor is controlled by a motor driver integrated with a current sensor (Current Sensor A) to measure the motor's power draw. The current measurement is crucial for estimating torque. A dedicated microcontroller (Inboard Steering MCU) controls the feedback motor, processes the position data from both position sensors, and monitors the motor current. Additionally, this microcontroller gathers critical vehicle data such as vehicle speed, driving mode, ADAS commands, and OTA updates, ensuring a realistic and adaptable system similar to real-world Steer-by-Wire (SbW) implementations.

2) Outboard Steering Subsystem: The outboard steering subsystem is present outside the cabin. It consists of a servo motor driving a pinion gear and a steering rack connected to the road wheels (RW). The servo is powered by a DC motor controlled via a motor driver. A current sensor (Current Sensor B) to determine the torque the motor is applying. A position sensor (Position Sensor C) tracks the angular position of the DC motor, providing feedback for precise control of the steering rack. To simulate the reaction forces experienced by the road wheels during steering, an additional DC motor is connected to the servo, emulating road conditions. This force-emulating motor works in conjunction with a redundant position sensor (Position Sensor D), which measures the true angle of the road wheel during a safety or security compromise. A dedicated microcontroller (Outboard Steering MCU) manages the outboard steering subsystem, controlling the servo motor and processing data from its sensors. This microcontroller also communicates live position and torque data to the inboard microcontroller. This exchange of data is crucial, for driving the feedback motor, enabling the driver to experience a realistic steering feel.

By ensuring accurate data exchange and control between the inboard and outboard steering subsystems, this experimental setup closely replicates the behavior of a real-world Steer-by-Wire system, allowing for meaningful experimentation and analysis. The system can also be calibrated and configured for relevant experiments. This way different control strategies could be implemented depending on the use case and also can replicate the strategies that different manufacturers employ. Although our implementation supports the

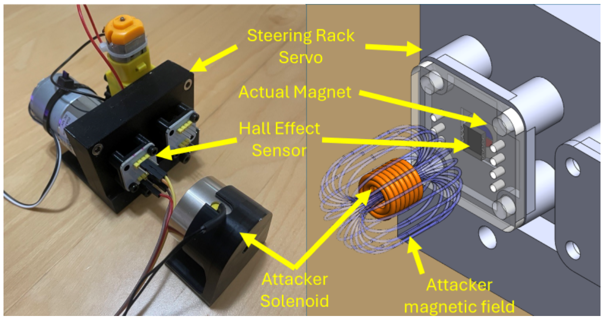

Figure 4. A solenoid is used to disrupt the original magnetic field, causing the encoder to misread position values, which leads to incorrect servo operation. Actual Implementation and CAD image of the attack.

use of the previously mentioned SbW techniques due to its configurability, our experiments employ the *Torque Sensor-Based Control Approach* for this paper.

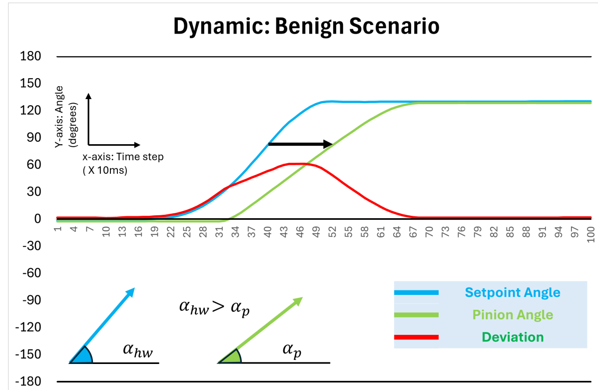

Figure 5. Benign scenario: The steering input angular acceleration is intentionally made higher than the servo angular acceleration to better understand the characteristics of the SbW system. However, this can be configured by controlling the resistance provided by the feedback motor to improve steering feel and accuracy.

V. Steer-by-Wire Attacks

As described earlier, the outboard steering subsystem is a servo mechanism designed to maintain the position setpoint commanded by the inboard system. The control system relies on feedback from a Hall effect-based position sensor, which serves as an absolute encoder utilizing a diametrically magnetized field to determine the pinion gear's position. This pinion drives a rack connected to the road wheels via an upright, making the pinion position a key reference for the outboard steering state. In this work, we demonstrate an approach to disrupt this system by creating an artificial magnetic field that overshadows the original magnetic field shown in Fig.4. This manipulation induces false position readings in the encoder, causing the servo motor to reach a setpoint other than the intended one, leading to incorrect steering responses.

1) Benign Scenario: SbW systems exhibit some form of delay. Manufacturers try to reduce this delay as much as possible in two major ways. They either increase the response of the slave actuator or increase the resistance provided by the feedback motor thereby reducing the rate of rotation of the input. This inherent delay exists in our platform too. In Fig.5 we observe this delay in response of the pinion wheel. We also notice that the handwheel rotational acceleration α_{hw} is higher than the servo/pinion rotational acceleration α_p. We can notice this through the slope of the setpoint curve and the pinion curve. This characteristic was part of the initial requirement to simulate the effect of response on increasing voltage to make the motor accelerate faster. This was made to demonstrate the limitations of SbW systems. Hence there is a requirement for higher Low Voltage (LV) architecture in modern cars, 48V instead of 12V, to allow SbW to function effectively. In the benign scenario, there is no abnormal behavior in the system. The outboard system reaches the setpoint given by the inboard steering subsystem with the inherent delay.

2) Attack Scenario: In this attack scenario, a solenoid is strategically positioned near the steering system to interfere with the operation of the pinion position sensor. The solenoid generates a magnetic field directed toward the sensor, aiming to overshadow the magnetic field of the encoder's original magnet. As a result, the sensor may incorrectly read the magnetic field generated by the attacker's solenoid instead of the genuine magnetic field. This manipulation can lead to erroneous position readings, causing the steering system to exhibit unexpected behavior or a complete loss of control, compromising the safety and reliability of the vehicle.

Static Condition: In this condition, the steering wheel is held stationary while the attack is executed on the outboard steering system. The steering can be positioned at any point within the steering lock range. Importantly, the static condition refers solely to the motion of the steering wheel and not the vehicle. Even when the vehicle is in motion, if the steering wheel remains fixed at a particular angle, it is still considered a static condition with respect to the steering. Under such circumstances, when the attacker generates a constant magnetic field, it induces a deviation from the intended setpoint in the position sensor readings. This deviation compromises the accuracy of the steering system, potentially causing the vehicle to deviate from its intended trajectory, posing significant safety hazards.

Dynamic Condition: In this condition, the steering wheel is actively moved from one position to another, introducing a dynamic aspect to the steering system's operation. It is important to note that the term "dynamic" in this context solely refers to the motion of the steering wheel and is independent of the vehicle's movement. A dynamic condition can still occur even if the vehicle remains stationary, as the focus is on the changing position of the steering wheel. During a dynamic condition, the steering system continuously processes inputs from the steering wheel to adjust the outboard steering subsystem accordingly. If an attacker

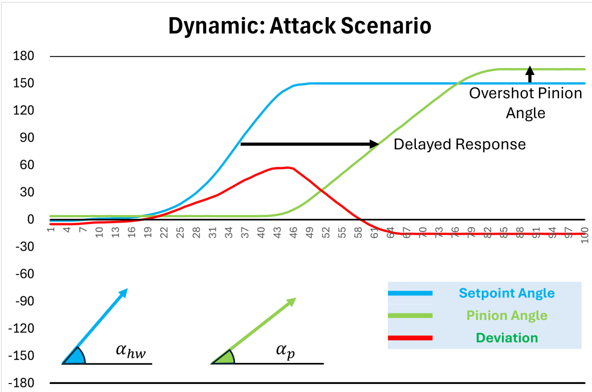

Figure 6. Attack Scenario: There is a noticeable shift in the servo curve. There is also an overshoot in the pinion position. If a vehicle is about to take a sharp corner, that could lead the car to an oversteer.

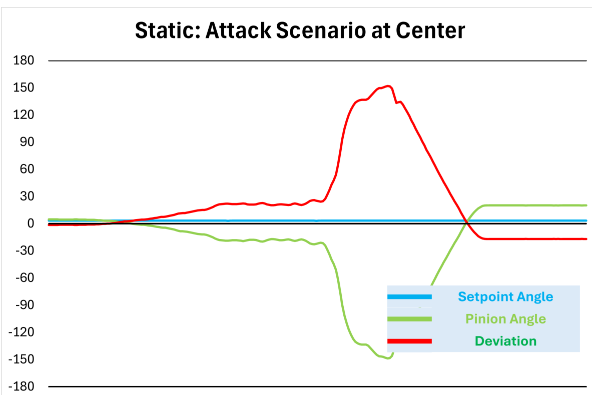

Figure 7. Attack scenario while the steering wheel is centered: There is a sudden change in vehicle heading while going straight.

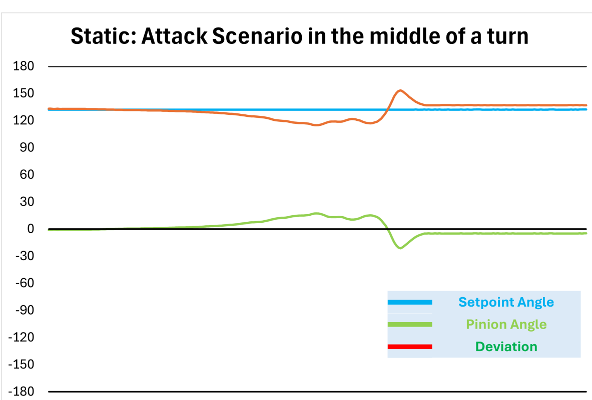

Figure 8. Attack scenario while the vehicle is cornering: The vehicle is negotiating a turn with the steering angle at 130 degrees. The vehicle can exhibit behavior as though it is correcting itself when there is a loss of traction. In the worst case, this behavior could lead to loss of traction at extreme corners or chicanes.

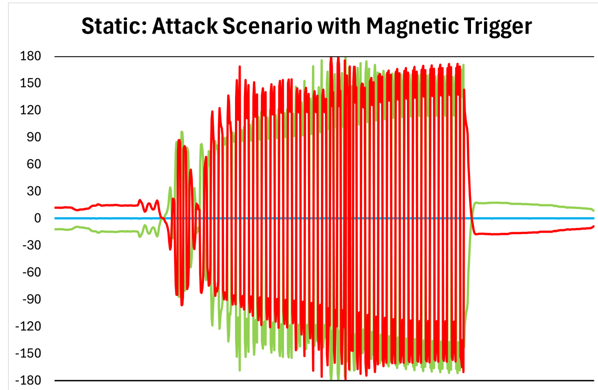

Figure 9. Attack scenario employing a fluctuating magnetic field and with the steering centered: The servo vibrates erratically. This could lead to collisions at low-speed maneuvers

introduces a time-varying magnetic field during this motion, it can interfere with the position sensor readings, leading to unpredictable deviations in the steering response. This interference can result in inaccurate tracking of the intended trajectory, causing the steering system to either overcompensate or underperform. Such disruptions could compromise the integrity of the steering mechanism, potentially leading to unsafe vehicle behavior, even in stationary conditions. The dynamic condition highlights the heightened complexity of maintaining control and accuracy in scenarios where steering inputs are constantly changing.

In Fig. 6, it is evident that the servo in the attacked scenario responds with a noticeable delay compared to the benign scenario. Additionally, the servo overshoots the intended setpoint angle, resulting in a false pinion angle. This behavior could lead to a situation where the vehicle steers more than intended, with a delayed response, creating significant safety risks. From the driver's perspective, this delayed and exaggerated steering behavior could be particularly unsettling, especially during critical maneuvers such as lane changes or cornering on hilly roads. From the attacker's perspective, sustaining this attack would require deploying multiple hardware devices along the road to maintain the attack's duration and effectiveness.

In another scenario shown in Fig. 7, when the vehicle moves in a straight line with the hand wheel held stationary, passing over the attacker's hardware causes a sudden change in the pinion position. This abrupt shift could cause the vehicle to deviate from its intended path, potentially heading in the wrong direction and continuing that way. An offset is observed in the pinion angle compared to the setpoint, which could result in the vehicle veering off the road or cutting across lanes before leaving the roadway entirely. Although the attack duration is only a few milliseconds, its impact can be devastating.

A similar effect is observed when the vehicle is cornering. In this case, shown in Fig. 8, the setpoint is maintained at 130 degrees, and the attack occurs while the vehicle is negotiating the turn. The attack causes the servo to reduce the steering angle abruptly, followed by an attempt to regain the setpoint. During this recovery process, the servo overshoots before stabilizing at the setpoint. This erratic behavior may lead the driver—or the adaptive vehicle dynamics system—to incorrectly assume that the vehicle has slipped while cornering due to a sudden and jerky movement, creating a dangerous misinterpretation of the situation. Such disruptions during critical maneuvers highlight the severity of these vulnerabilities and the potential for catastrophic outcomes.

In another special scenario, if a vehicle is stationary—such as at a traffic intersection, stop sign, or while backing out of a parking lot—an attacker can introduce a magnetic field with a specific trigger frequency. This frequency is designed to align the artificial magnetic field at a particular orientation or angle relative to the original sensor's magnetic field. The concept is analogous to using a duty cycle in a DC-DC converter to achieve a voltage level between maximum and minimum potential values. This manipulation can cause the servo to vibrate at a specific frequency shown in Fig. 9, leading to a shaky start when the vehicle begins to move. Such vibrations can result in erratic vehicle movements, increasing the risk of collisions, especially during critical maneuvers like 90-degree turns or U-turns. This behavior can also confuse other drivers, vehicles, or pedestrians, creating dangerous and unpredictable traffic situations.

This attack is not limited to stationary vehicles and can also be executed while the vehicle is in motion. However, to sustain the attack for a longer duration, multiple attacker devices would need to be strategically placed along the road to maintain the attack window and its disruptive effects. Such scenarios underline the potential hazards of exploiting vulnerabilities in the steering system, especially in critical or high-traffic environments.

VI. Conclusion

This study highlights the critical security vulnerabilities inherent in Steer-by-Wire (SbW) systems, particularly in the context of modern and autonomous vehicles. By eliminating the mechanical linkage between the steering wheel and tires, SbW systems introduce a heavy reliance on sensors and electronic data channels, making them susceptible to cyberattacks and physical disruptions. Our custom-built SbW setup, designed to replicate real-world systems with accurate sensor functionality and control techniques, has enabled a comprehensive investigation of these vulnerabilities. Through targeted experimentation under various conditions—both static and dynamic—we have demonstrated how attacks on position, torque, current, and voltage sensors can disrupt steering operations, leading to unsafe and unpredictable vehicle behavior.

The findings underscore the potential for catastrophic consequences, especially in future scenarios involving autonomous vehicles where manual intervention is not possible. This work provides a foundational framework for understanding these security challenges and highlights the urgent need for robust countermeasures. By addressing these vulnerabilities, the automotive industry can move toward more resilient and secure SbW systems, ensuring both vehicle safety and occupant trust as the era of autonomous driving advances.

In future work, we will investigate how the attack propagates to the handwheel and its impact on steering feedback. Further planned exploration includes vulnerabilities in Hall effect-based current sensors and other attack entry points. Additionally, we plan to extend this work into hands-on platforms for cybersecurity education and research, enabling deeper exploration of SbW system threats and mitigation strategies.

References

[1] K. Polmans, A. Mitterrutzner, M. Dähler, and Y. Thoma, "Steer-by-wire systems safety, comfort and individuality," *ATZ worldwide*, vol. 120, no. 6, pp. 30–35, 2018.

[2] A. Kirli, C. E. Okwudire, and A. G. Ulsoy, "Limitations of torque vectoring as a backup safety strategy for steer-by-wire vehicles due to vehicle stability control," in *Dynamic Systems and Control Conference*, vol. 58271. American Society of Mechanical Engineers, 2017, p. V001T45A008.

[3] A. Balachandran and J. C. Gerdes, "Designing steering feel for steer-by-wire vehicles using objective measures," *IEEE/ASME transactions on mechatronics*, vol. 20, no. 1, pp. 373–383, 2014.

[4] S. A. Mortazavizadeh, A. Ghaderi, M. Ebrahimi, and M. Hajian, "Recent developments in the vehicle steer-by-wire system," *IEEE Transactions on Transportation Electrification*, vol. 6, no. 3, pp. 1226–1235, 2020.

[5] S. Achyuthan and N. K. Prakash, "Modelling of a steer-by-wire system with force feedback and active steering," in *2017 International Conference on Intelligent Computing and Control Systems (ICICCS)*. IEEE, 2017, pp. 676–680.

[6] P. Yih and J. C. Gerdes, "Modification of vehicle handling characteristics via steer-by-wire," *IEEE transactions on control systems technology*, vol. 13, no. 6, pp. 965–976, 2005.

[7] S. Fankem and S. Müller, "A new model to compute the desired steering torque for steer-by-wire vehicles and driving simulators," *Vehicle System Dynamics*, vol. 52, no. sup1, pp. 251–271, 2014.

[8] P. Zhai, H. Du, and Z. Li, "Bilateral control of vehicle steer-by-wire system with variable gear-ratio," in *2013 IEEE 8th Conference on Industrial Electronics and Applications (ICIEA)*. IEEE, 2013, pp. 811–815.

[9] S. Anwar and L. Chen, "An analytical redundancy-based fault detection and isolation algorithm for a road-wheel control subsystem in a steer-by-wire system," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 5, pp. 2859–2869, 2007.

[10] K. Scicluna, C. S. Staines, and R. Raute, "Torque feedback for steer-by-wire systems with rotor flux oriented pmsm," in *2017 19th International Conference on Electrical Drives and Power Electronics (EDPE)*. IEEE, 2017, pp. 188–193.

[11] B.-H. Nguyen and J.-H. Ryu, "Direct current measurement based steer-by-wire systems for realistic driving feeling," in *2009 IEEE international symposium on industrial electronics*. IEEE, 2009, pp. 1023–1028.

[12] P. Yih, J. Ryu, and J. C. Gerdes, "Vehicle state estimation using steering torque," in *Proceedings of the 2004 American Control Conference*, vol. 3. IEEE, 2004, pp. 2116–2121.

[13] M. Hales and K. Pattok, "Safety standards for steer-by-wire systems," in *12th International Munich Chassis Symposium 2021: chassis. tech plus*. Springer, 2022, pp. 675–692.

[14] O. Özçetin and M. T. Emirler, "Threat analysis and risk assessment and countermeasures against threat scenarios for steer-by-wire system," in *2024 International Conference on Smart Systems and Technologies (SST)*. IEEE, 2024, pp. 83–88.

[15] J. Iqbal, K. M. Zuhaib, C. Han, A. M. Khan, and M. A. Ali, "Adaptive global fast sliding mode control for steer-by-wire system road vehicles," *Applied Sciences*, vol. 7, no. 7, p. 738, 2017.