RESEARCH ARTICLE

A Physics-Informed Context-Aware Approach for Anomaly Detection in Tele-Driving Operations Under False Data Injection Attacks

SUBHADIP GHOSH, (Senior Member, IEEE),
AYDIN ZABOLI, (Member, IEEE), **JUNHO HONG**, (Senior Member, IEEE),
AND JAEROCK KWON, (Senior Member, IEEE)
Department of Electrical and Computer Engineering, University of Michigan–Dearborn, Dearborn, MI 48128, USA

Corresponding author: Junho Hong (jhwr@umich.edu)

ABSTRACT Tele-operated driving (ToD) systems are special types of cyber-physical systems (CPSs) where the operator remotely controls the steering, acceleration, and braking actions of the vehicle. Malicious actors may inject false data in communication channels to manipulate the tele-operator's driving commands to cause harm. Hence, protection of this communication is necessary for the safe operation of the target vehicle. However, according to the National Institute of Standards and Technology (NIST) cybersecurity framework, protection merely is not enough and the detection of an attack is necessary. Moreover, UN R155 mandates that security incidents across vehicle fleets be detected and logged. Thus, cyber-physical threats of ToD are modeled with an attack-centric approach in this paper. Then, an attack model with false data injection (FDI) on steering control commands is created from real vehicle data. The risk of this attack model is assessed for a last-mile delivery (LMD) application. Finally, a physics-informed context-aware anomaly detection system (PCADS) is proposed to detect such false injection attacks, and preliminary experimental results are presented to validate the model.

I. INTRODUCTION

In recent years, autonomous driving has been one of the key areas of attention among the automotive researchers. Numerous innovations and cutting-edge technologies have emerged to bring full autonomy in road vehicles. Vehicle teleportation is one such technology that originated to provide emergency assistance to autonomous vehicles (AVs) in unusual or difficult driving scenarios [1], [2], [3]. However, this technology is also being targeted for tele-operated taxis and delivery services [4], [5], [6], [7]. The National Institute of Standards and Technology (NIST) vehicle tele-operation forum and 5G blueprint project are leading the research in this area in the United States and Europe, respectively

The associate editor coordinating the review of this manuscript and approving it for publication was Byung-Seo Kim.

[8] and [9]. Some start-up companies (e.g., Zoox, Ottopia, Faction, DriveU.auto) have started testing their prototypes of tele-operated vehicles for the mobility services for some specific use cases [10], [11], [12], [13], [14].

A. PROBLEM STATEMENT

In general, the driving function of a vehicle can be viewed as a combination of longitudinal control (i.e., acceleration, braking) and lateral control (i.e., steering) of a vehicle to reach from start to destination in various traffic scenarios. Tele-operated drivers can monitor, control, or provide guidance to the driving function from a remote operating station [1], [15]. Typically, the perception and localization are information sent by the vehicle to the operating station via cloud and fog infrastructure using wireless or cellular networks. Similarly, control commands transmitted from the

operating station are sent to the vehicle. This poses a potential exposure of perception data and control commands outside the vehicle boundary and can make the ToD vulnerable against cyberattacks. Attackers can target the ToD system with denial-of-service (DoS) attacks, FDI attacks, man-in-the-middle (MITM) attacks, and other attacks similar to the attacks detected in other CPSs [16], [17]. A malicious control of ToD may result in the vehicle crash, disruption in tele-operation service, legal consequences, and financial loss. Hence, a robust cybersecurity strategy is critical to prevent, detect, and mitigate such attacks for a safe ToD. Although cybersecurity is a common practice in information technology (IT) and many other internet of things (IoT) devices, cybersecurity for road vehicles has gained attention in recent years since a researcher in this field hacked a vehicle in 2016 [18]. In 2020, UNECE World Forum for Harmonization of Vehicle Regulations (UNECE WP.29) has adopted UN Regulation No. 155 on Cyber Security and Cyber Security Management Systems, which requires managing cyber risks to vehicles in 54 countries from 2024 [19]. Typically, cryptography, chain of trust, firewall and access control are some of the common techniques to protect security assets in cyber domains [20], [21], [22], [23], [24], [25], [26]. However, with evolving threats on these methods, protection from all potential attacks cannot be guaranteed [27], [28], [29]. Moreover, insider attacks increase the vulnerability of a system by inadequate security measures in the system design and improper implementation of cryptography algorithms which are exploited by zero-day attacks. To address this challenge, security by design needs to be followed that is the defense-in-depth (DiD) principle [30], [31], where security strategies are applied at multiple layers. One of the critical features of DiD is the detection mechanism [32]. Further, UN R155 requires monitoring and reporting of security incidents for vehicle fleets for automotive applications [19]. Conventional cybersecurity detection methods are primarily in the cyber domain and have limitations in addressing the security requirements of CPSs [33], [34], [35]. To address this, recent research in other CPSs has demonstrated an extension of DiD and detection methods to physical domains [36], [37], [38], [39], [40]. Currently, ToD is an emerging technology within restricted operational design domain (ODD) and prototype phase. When this technology gets deployed at large on public roads, a cyber-physical DiD strategy will be necessary to reduce risks from cyberattacks. However, to our knowledge, there is no study to show threat analysis for cyberattacks on driver's control commands transmitted from tele-operator stations to the target vehicles. Moreover, methods to detect such attacks in tele-operated vehicle's physical domain have not been explored.

B. RELATED WORK

An intrusion detection system (IDS) is one of the techniques recommended by various standards (e.g., ISO 27039, NIST, Open Web Application Security Project (OWASP)) to monitor activities in the system or network for malicious behavior. Several automotive communities and researchers are considering an automotive specific IDS as a fundamental solution for vehicle cyber incidents detection and reporting, which has the potential to be extended to intrusion detection and prevention systems (IDPSs) [41], [42], [43]. Automotive Open System Architecture (AUTOSAR) organization has released a specification for vehicle intrusion detection systems in 2020 that provides a standardized interface to report on-board security events for a vehicle electronic control unit (ECU) and network environment [44]. Basically, IDS methods in cyber domains are of three types, including signature-based, behavior-based, and anomaly-based approaches [45], [46], [47]. Other IDS methods are inspired or combined by these basic methods. In the automotive industry, IDSs are typically software components deployed in the network, host, or as a distributed system. These types of IDS are mainly focused on messages in vehicle network protocols (e.g., CAN, automotive Ethernet) [48], [49], [50] and lack utilizing the application specific knowledge. Other than IDSs, an anomaly detection (AD) process is also used in other applications (e.g., sensor AD [51], [52], vehicle traffic AD [53], [54], in-vehicle monitoring for AVs [55]). In science, an anomaly is described when there is a difference between actual observation and expected outcome developed based on the original scientific idea [56]. In the statistics and data mining field, outliers in the dataset are considered as anomalies. For physical systems, detecting anomalies in AV sensors, aerial systems, and intelligent traffic systems are examples of some important applications. An AD process for IDSs was introduced in the 1980s to detect security violations by recognizing abnormal patterns in system logs [57]. Recent research on cyber-physical attack detection is presented in Table 1. According to this table, the current AD techniques for automotive IDSs primarily focus on finding anomalies based on a data-driven analysis of the network and less consideration of physical behavior. Table 1 shows research on other CPSs found for detecting cyber-physical attacks, hybrid approaches by combining data-driven models and physics-based models. The recent growth in ML research and its applications is largely driven by two key factors. Firstly, the digital creation and storage of extensive datasets plays a crucial role. Secondly, the accessibility of cost-effective high-performance computing devices that can process these extensive datasets acts as a vital accelerator. These datasets are often developed for particular applications, including prediction, recognition, recommendation systems, and language processing [63]. Solaas et al. [64] performed a comprehensive literature review encompassing 203 papers concerning anomaly detection in Connected and Autonomous Vehicles. Their study highlighted LSTM, CNN, and autoencoders as the primary AI techniques and delved into the training methodologies and evaluation metrics utilized. Their evaluation revealed significant limitations: notably, only 9 out of 203 studies

TABLE 1. A literature survey on AD process in CPSs.

Author	Method	Application	Contributions
Rahul et al. [58]	Physics guided machine learning (ML) techniques	General CPSs	- Classified the hybrid models into physics-based pre-processing, physics-based network architectures, physics-based regularization, and miscellaneous categories based on the way the model-based is brought into the hybrid architecture. - Proposed five metrics for all-round performance evaluation of a hybrid CPS model.
Cody et al. [59]	Hybrid physics model-based data-driven framework	Smart grid real-time monitoring	- Presented a hybrid framework with physics-based and data-driven ensemble CorrDet (ECD) algorithm. - Tested the results on IEEE 118-bus system which shows 6.75% improvement from the physic-based solution.
Faris et al. [60]	Statistical learning and kinematic model	Adaptive cruise control for AVs	- Proposed generalized extreme studentized deviate with sliding chunks (GESD-SC) approach, which is applied at each vehicle in the platoon to detect anomalies in real-time based on the vehicle's own speeding decisions.
Jie et al. [61]	Spatio-temporal correlation based a long short-term memory (LSTM) method	Autonomous Aerial Vehicles (AAVs)	- Suggested an An spatio-temporal convolutional (STC)-LSTM algorithm which can accurately locate the anomalies of AAV flight data and provide high-precision recovery prediction values.
Bin et al. [62]	Physics-informed neural networks (PINNs)	Power systems	- Several paradigms of PINNs (e.g., PI loss function, PI initialization, PI design of architecture, and hybrid physics-DL models) are summarized.

offered open-source availability; there was a deficiency in real-world deployment data; and there was an absence of standardized benchmarking datasets. Moreover, the research did not delve into the vulnerabilities associated with on-demand tele-operation or the use of mission-specific driving contexts for context-aware detection. Additionally, it did not investigate approaches informed by physics for the validation of vehicle behavior signatures. Mansourian et al. [65] developed a framework for forecasting temporal events that utilizes LSTM and ConvLSTM models to detect anomalies in Controller Area Networks (CAN) through the analysis of patterns across both space and time. This approach showcased remarkable accuracy when tested on established datasets. However, the supervised approach limits flexibility against new attacks, overlooks vulnerabilities related to remote operations, and fails to incorporate validation within the context of specific missions. Additionally, the system lacks physics-based behavioral authentication and addresses only internal network security rather than comprehensive remote operation threats. A physics-informed anomaly detection framework by Guo et al. [66] embedded AAV dynamics into neural detection models, demonstrating enhancements in performance, achieving increases of up to 17.77% in ROC-AUC scores in countering spoofing attacks. Despite this, the approach continues to be limited to the validation of spoofing incidents and wind disturbance, failing to address the vulnerabilities associated with remote operations and the integration of operation contexts that are specific to particular routes. Moreover, while the efficiency of training is enhanced by smoothing the loss landscape, the framework did not include thorough physics-based behavioral verification and primarily targets internal AAV anomalies, neglecting the broader range of threats related to remote operations. Makridis and Kouvelas [67] introduced an adaptive physics-informed model that reconstructs vehicle paths by integrating constraints from vehicle dynamics with patterns of driver behavior, effectively filtering out noise from sensor data. However, their methodology focuses primarily

on smoothing trajectories in an offline manner, rather than the crucial real-time anomaly detection necessary for the ToD security. Although they utilize constraints grounded in physics with effectiveness, their system lacks context recognition to determine that vehicle tasks correspond with the prescribed mission pathways. Moreover, the framework considers all anomalies to be sensor noise, neglecting to account for malicious cyber-physical threats such as FDI attacks targeting steering mechanisms. While their method shows promise for trajectory reconstruction, it necessitates precise vehicle specifications, which might not be obtainable in real-world ToD implementations. Furthermore, it lacks threat modeling and risk assessment features, which are essential for securing connected vehicle systems. Shi et al. [68] developed a physics-informed deep learning (PIDL) framework with fundamental diagram learning (i.e., PIDL + FDL) for estimating traffic states and learning flow-density relationships in highway scenarios. While their methodology focuses on typical traffic reconstruction, it did not tackle the unique security issues associated with ToD. Although the framework successfully integrates physics-based models with neural networks, it fails in validating context specific to the mission and neglects considerations for harmful cyber-physical threats such as FDI attacks on steering controls. While appropriate for highway traffic analysis, it lacks both the threat assessment and real-time anomaly detection needed to protect ToD systems against adversarial manipulations. A physics-informed learning framework for autonomous screw-driving proposed by Manyar et al. [69] that characterizes rotational motion dynamics and handles position through active and passive compliance mechanisms. Although their method effectively incorporates physics-based modeling to ensure dependable assembly processes in the presence of positional uncertainties, it focuses on automating manufacturing instead of addressing ToD security issues. While the architecture includes mechanisms for identifying mechanical failures, such as cross-threading and jamming, it is deficient in
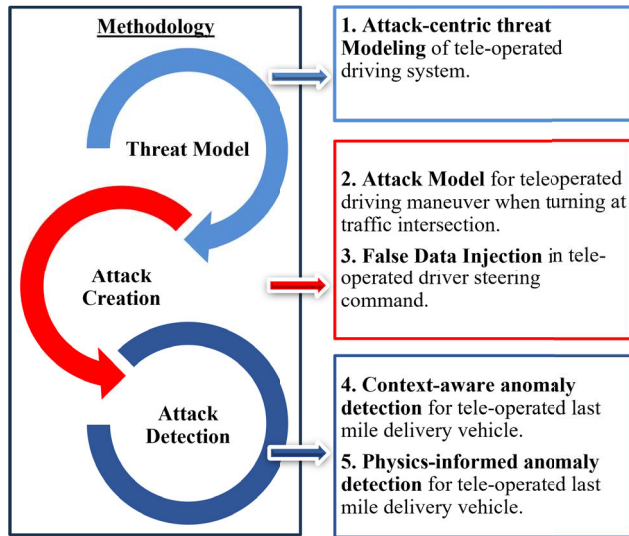
FIGURE 1. A workflow of the paper's contributions.

functionalities for detecting sophisticated cyber-physical threats, specifically FDI attacks targeting the steering commands. Fan et al. [70] constructed an advanced anomaly detection framework utilizing unsupervised Generative Adversarial Networks (GANs) in combination with LSTM networks. The proposed framework is meticulously crafted to identify adversarial threats directed at trajectory prediction algorithms. It accomplishes this through an extensive evaluation of two types of losses: the reconstruction loss, which measures the performance of the model in reproducing input data, and the discrimination loss, which assesses the model's capability to distinguish between legitimate and adversarial inputs. Nonetheless, their approach primarily concentrates on detecting malicious trajectories specific to prediction models, without fully addressing the protection of ToD operations in a holistic manner. Although the method proficiently detects adversarial trajectories by examining temporal-spatial characteristics, it is deficient in context-aware validation that would confirm maneuvers against planned mission paths. Further, the framework fails to tackle FDI attacks aimed at steering directives and lacks a physics-based validation mechanism for vehicle behavior verification. According to the provided challenges and gaps in this domain, the contributions of this research will be presented in the next section.

C. CONTRIBUTIONS
The primary contribution of this work is the development of a novel Physics-informed Context-Aware Anomaly Detection System (PCADS), designed to secure Tele-operation on Demand (ToD) systems against critical cyber-physical threats. The workflow culminating in these contributions is illustrated in Fig. 1. To establish the necessity for this system, this paper first introduces a foundational threat model for ToD, an area previously unaddressed in the literature. This

analysis identifies False Data Injection (FDI) on steering commands as a high-risk vulnerability. Building on this, we contribute a detailed FDI attack model, formulated and implemented by injecting noise into steering data from the D2CAV real-world driving dataset during turning maneuvers [71]. The core contribution is the PCADS framework itself, which pioneers a dual-pronged detection strategy by integrating two innovative concepts: a context-aware module that leverages the vehicle's mission-specific Driving Contexts (DCs) and a physics-informed module that learns the vehicle's physical response signatures during maneuvers. The principal contributions are therefore:

- **A foundational cyber-physical threat analysis and risk assessment for ToD systems,** identifying previously uncatalogued vulnerabilities.
- **A novel FDI attack model targeting steering control,** completed with its mathematical formulation and validation on real-world driving data.
- **A context-aware anomaly detection method** that uniquely utilizes mission-specific driving contexts to validate vehicle maneuvers against intended routes.
- **A physics-informed anomaly detection method** that learns and verifies the physical signatures of vehicle behavior, providing a robust, model-based layer of security.

D. ASSUMPTIONS AND SCOPE
- This work is focused on a specific use case of ToD which is last-mile delivery (LMD).
- For DCs, a solution of the vehicle routing plan (VRP) to find optimal routes for the fleet of vehicles is not in the scope of this paper and it is assumed the VRP is accurate and robust to address real-time traffic density, road conditions, weather and vehicle maintenance schedule.
- A dynamic alert generation is out of scope in this research which it is simulated as a binary flag.
- For the physical parameter learning, left turn, right turn and U-turn maneuvers are considered.
- Experimental results are based on the dataset mentioned in experiment section.
- The proposed methodology assumes the vehicle configuration and physical parameter values for left turn, right turn and U-turn maneuvers of the target vehicle that are known to AD system.

E. PAPER STRUCTURE
The rest of this paper is organized as follows: Section II provides cyber-physical threat models for ToD and attack models for injecting noise on steering control command for left turn, right turn, and U turn actions at a traffic intersection. Section III describes the proposed AD method, PCADS, and the corresponding mathematical modeling. The experimental setup and results are discussed in Section IV. Finally, the paper is concluded in Section V, and the supplementary material is given in Section VI.
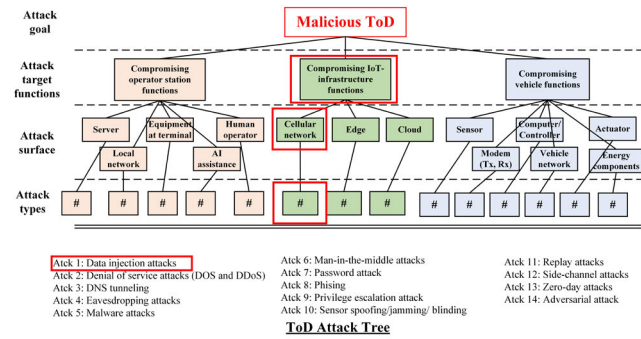
FIGURE 2. An attack tree for a ToD event.

FIGURE 3. A tele-operated vehicle attack likelihood vs impact.

II. A TOD THREAT ANALYSIS

Tele-operation on Demand (ToD), or tele-operation, provides remote driving or assistance to piloted and autonomous vehicles (AVs) and is a critical component of the AV ecosystem, enabling services like tele-operated taxis and deliveries [72], [73], [74]. This technology allows a remote operator to passively monitor and, if necessary, take full control of semi-autonomous and autonomous vehicles. The automotive industry categorizes ToD into three main types of control. As described in Table 2, in direct control, the remote operator manages most driving functions, including planning and decision-making. With indirect control, the operator guides the vehicle by providing or selecting trajectories. Shared control involves a division of decision-making and vehicle control between the automated driving system and the remote operator [75], [76].

A. THREAT MODELING OF TELE-OPERATED DRIVING

A threat modeling, also referred to as threat analysis and risk assessment (TARA) model, is generally viewed as the starting point for designing a cyber-secure system [77]. Given the extensive and dispersed attack surface of vehicle tele-operation, an attack-tree based method is employed for the threat analysis. In this study, TARA of the ToD system is carried out with the following steps. The first step involves identifying the components of a ToD system. According to Table 2, ToD functions can be distributed in three categories of components (e.g., operator station, IoT infrastructure, and vehicle). An operator station must include human operator, operator terminal, server, and local communication network. It might also have artificial intelligence (AI) assistance to the terminal. An IoT infrastructure can be divided into three primary sub-components including cellular network, cloud, and edge. From the ToD perspective, the vehicle needs to have sensing devices for perception, localization, inertia, and vehicle diagnostics. A vehicle also requires an in-vehicle communication network to communicate between multiple ECUs and a modem to communicate using cellular channels. For vehicle motion, it needs the drive-train, controller, and actuators. In the second step, all of these components are organized in a tree format as shown in Fig. 2. In the third step, the attack tree is created with potential attacks on the ToD
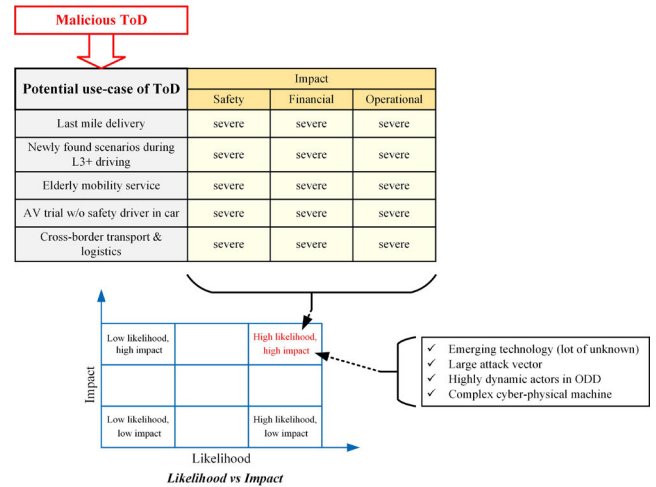
system. The attack tree in Fig. 2 illustrates the variety of attacks that can be aimed at different components from the vehicle to the operator station, potentially leading to malicious ToD. These attacks are determined based on the literature review for other CPSs and MITRE ATT&CK(R)matrices [78]. In the 4th step, most promising applications of ToD are analyzed for an impact on safety, finance, and legality due to malicious ToD, as illustrated in Fig. 3. This analysis is carried out with a subjective approach considering that malicious ToD can disrupt lateral and longitudinal motions, and suspension control of the tele-operated vehicle. Such incidents can interrupt ToD service and even jeopardize the safety of passengers and other road users. In [79], [80], [81] and [82], researchers have discussed various consequences of disrupting cross-border transportation, LMD, and mobility services. According to these papers, disruption of these applications has major adverse effects on road safety and the regional economy. As these are the potential applications for ToD, it can be argued that a malicious ToD event can inflict serious harm on these applications. Finally, in the 5th step of the TARA, a risk is assessed based on the likelihood of attacks causing a malicious ToD and the impact on the ToD application. At present, ToD for public roads is still a developing technology. However, when ToD is implemented on public roads, attack surface and the number of impacted users will expand. As a result, the risk will also escalate, which is demonstrated as a high risk in Fig. 3.

B. ATTACK MODEL FOR LAST-MILE DELIVERY

According to the attack tree analysis, an attacker can cause a malicious ToD event by compromising the IoT infrastructure. In this section, firstly, an attack model is developed for one of the potential use cases of the ToD event on public roads, known as "last-mile delivery (LMD)". Secondly, an attack formulation is implemented for an FDI attack on the steering wheel angle command from the tele-operator. The LMD

TABLE 2. Functions and data flows for various ToD events.

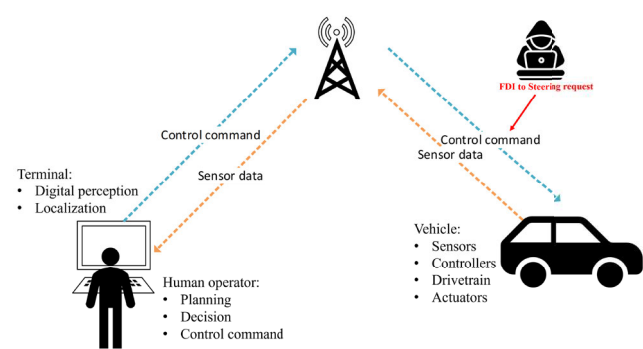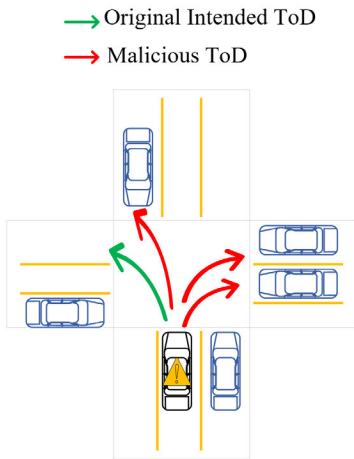|		Data Flow		Function						
		Vehicle to Operating Station	Operating Station to Vehicle	Sensing	Perception	Localization	Planning	Decision	Control	Actuation
Direct Control		Sensor data	Control command via steering, brake, acceleration pedal operation by remote operator.	Vehicle	Operator station	Operator station	Operator station	Operator station	Hi level: Operator station Lo level: Operator station	Vehicle
Shared Control		Object list or a representation of the free space.	Desired control command via steering, brake, acceleration pedal operation by remote operator.	Vehicle	Vehicle	Vehicle	Operator station	Vehicle and Operator station	Hi level: Vehicle Operator station Lo level: Vehicle	Vehicle
Indirect Control	**Trajectory Guidance**	Sensor data	Control command as trajectory	Vehicle	Vehicle/Operator station	Vehicle/Operator station	Operator station	Operator station	Hi level: Operator station Lo level: Vehicle	Vehicle
	Waypoint Guidance	Sensor data	Discrete waypoints	Vehicle	Vehicle/Operator station	Vehicle/Operator station	Operator station	Operator station	Vehicle	Vehicle
	Interactive Path Planning	Object list and a grid map	Optimized path	Vehicle	Vehicle	Vehicle	Vehicle and Operator station	Operator station	Vehicle	Vehicle
	Perception Modification	Object list and a grid map	Bounding box	Vehicle	Vehicle and Operator station	Vehicle	Vehicle	Vehicle	Vehicle	Vehicle

FIGURE 4. An FDI attack on communication between remote operators and the vehicle.

A ToD left turn at a traffic intersection.

FIGURE 5. A traffic light intersection attack scenario.

represents the concluding stage in a business-to-customer (B2C) delivery process where the package is transported to the recipient, either directly to their home or to a designated pickup location [83]. Fig. 4 illustrates the performance of the tele-operated LMD vehicle. This illustration showcases the essential framework of the remote vehicle operation system, which serves as the primary motivation for this study into tele-operated vehicles. The inclusion of this diagram is essential to understanding the attack surface which is investigated throughout this work. The system functions within a two-way communication framework, wherein the vehicle's onboard sensors consistently gather environmental data and transmit this information to a remote operator station through cellular or wireless networks. At the terminal, the human operator leverages advanced digital perception systems and localization technologies to evaluate the driving environment. Utilizing this remote visual interface, the operator conceives navigational strategies and develops control instructions, which are conveyed to the vehicle via the identical communication framework. Upon receiving these directives, the vehicle's integrated systems which include controllers, drivetrain components, and actuators, carry out the designated movements. Critically, this architectural design reveals a potential security weakness, as indicated

by the red arrow. FDI attacks can target steering control commands during transmission. This security risk grows increasingly relevant in LMD scenarios, where AVs regularly maneuver through complex urban landscapes that demand accurate steering modifications, particularly during turning maneuvers at intersections as they follow specified delivery pathways [84]. However, an attack on the steering command can execute an undesired driving action and trajectory, causing an accident that is depicted in Fig. 5. According to this diagram, the normal trajectories for vehicle A are shown with green arrows, but the vehicle follows the path shown in red arrows under a cyberattack. This malicious behavior can be a potential cause of frontal or angled collisions with other stationary and moving road users. Based on US NSC data 2020, angled collisions and head-on collisions are the top two reasons for deaths and fatal crashes in the U.S. [85]. The analysis of damage patterns and severity of impact for passenger cars presented by Kurebwa et. al shows that the probability of damage and severity is significantly higher at
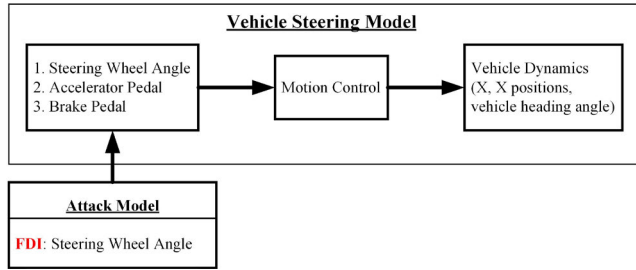
FIGURE 6. A system model for the vehicle's steering angle under attacks.
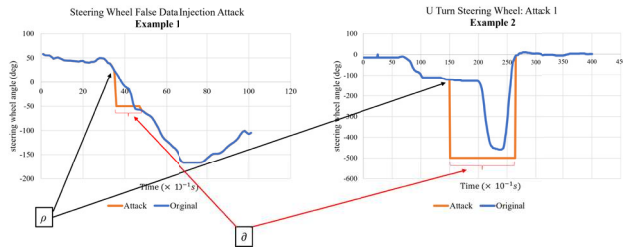

FIGURE 7. FDI attacks on steering wheel angle commands demonstrating two distinct attack scenarios with varying injection points and durations.

the front and front corner zones as compared to other points of impact on a vehicle [86]. Hence, an FDI attack on the steering command from the tele-operator is selected for the case study of the attack model. An attack model designed for this study is presented in Fig. 6. As depicted, driver inputs for steering wheel angle, accelerator pedal, and brake pedal determine the motion control logic of a tele-operated vehicle. Furthermore, motion control signals determine the vehicle heading angle and vehicle dynamics. Therefore, it can be derived that an FDI attack on driver input for steering wheel angle will impact the vehicle heading angle and dynamics. In order to create this attack, an attack formula is developed for the FDI on steering wheel angle. For this purpose, ISO/SAE 21434 is reviewed for recommended core factors to assess the attack feasibility. Empirical data illustrating the execution and effects of FDI attacks on steering wheel angle directives are depicted in Fig. 7. Incorporating this figure is crucial for illustrating the dynamics of the attack and for clarifying the practical implications embedded in this theoretical framework. The figure illustrates two separate attack scenarios, each demonstrating a unique strategy of exploitation. In Example 1, a moderate steering maneuver is observed where the vehicle's steering angle transitions from approximately 50 degrees to −170 degrees. The attack signal (depicted in orange) introduces a sharp rectangular pulse deviation at the critical moment when the steering angle begins its reduction, specifically around the 30–40 time unit mark. The timing strategy illustrates the method by which adversaries can take advantage of transitional steering phases to achieve maximum disruption while minimizing the duration of the injection. Example 2 demonstrates a more intense situation featuring a U-turn maneuver, characterized

by steering angles that vary between 0 and −450 degrees. In this scenario, the attack is characterized by the injection of a continuous rectangular pulse within the 150 to 250 time unit interval, resulting in an extended simulated steering command of −500 degrees. This instance showcases that extended attack durations may be utilized in complex maneuvers to possibly trigger significant deviations in the trajectory. These attacks are grounded in a mathematical framework that is effectively represented through Eq. (1), where $\hat{\alpha}$ represents the falsified steering command, α denotes the legitimate command, ϵ indicates the injected fault magnitude, and $\bar{\omega}$ defines the window of opportunity (*WoO*) as a function of the injection point (ρ) and duration.

$$\hat{\alpha} = f(\alpha, \epsilon, \bar{\omega}) \tag{1}$$

The graphical visualizations reveal that an effective attack depends on the precise coordination of the injection timing with the dynamics of the vehicle's steering. The varying approaches, i.e., short and precisely timed as seen in Example 1 as opposed to the extended approach in Example 2, highlight the wide range of attack methodologies that adversaries could utilize in targeting tele-operated vehicle systems.

III. PROPOSED PHYSICS-INFORMED CONTEXT-AWARE ANOMALY DETECTION SYSTEM

In this section, a Physics- and Context-Aware Anomaly Detection System (PCADS) is proposed to detect anomalies during left, right, and U-turns in Last Mile Delivery (LMD) vehicles, focusing on False Data Injection (FDI) attacks against the steering wheel angle. The method, outlined in Fig. 8, requires vehicle-specific Driving Contexts (DCs) and time-series patterns of physical parameters. As depicted, the method has two stages:

- A context-aware anomaly detection (PCADS-CA).
- A physics-informed anomaly detection (PCADS-PI).

The PCADS-CA stage compares the intended maneuver, inferred from DCs, with the actual driving command from the teleoperator. The PCADS-PI stage monitors the vehicle's physical parameter patterns during a turn and compares them against learned patterns to detect deviations. The following sections detail the PCADS-CA and PCADS-PI models.

A. STAGE 1: PCADS-BASED CONTEXT-AWARE ANOMALY DETECTION FRAMEWORK

The context-aware anomaly detection module suggests that the environmental and situational conditions around a vehicle can effectively anticipate expected driving actions. This framework establishes a predictive chain where driving contexts (DCs) inform the intended maneuver (IM), which subsequently corresponds to the actual control inputs (D_I) from the tele-operated driver. This hierarchical framework constitutes the foundational structure of the anomaly detection strategy. DC is mathematically expressed as Eq. (2), a function of
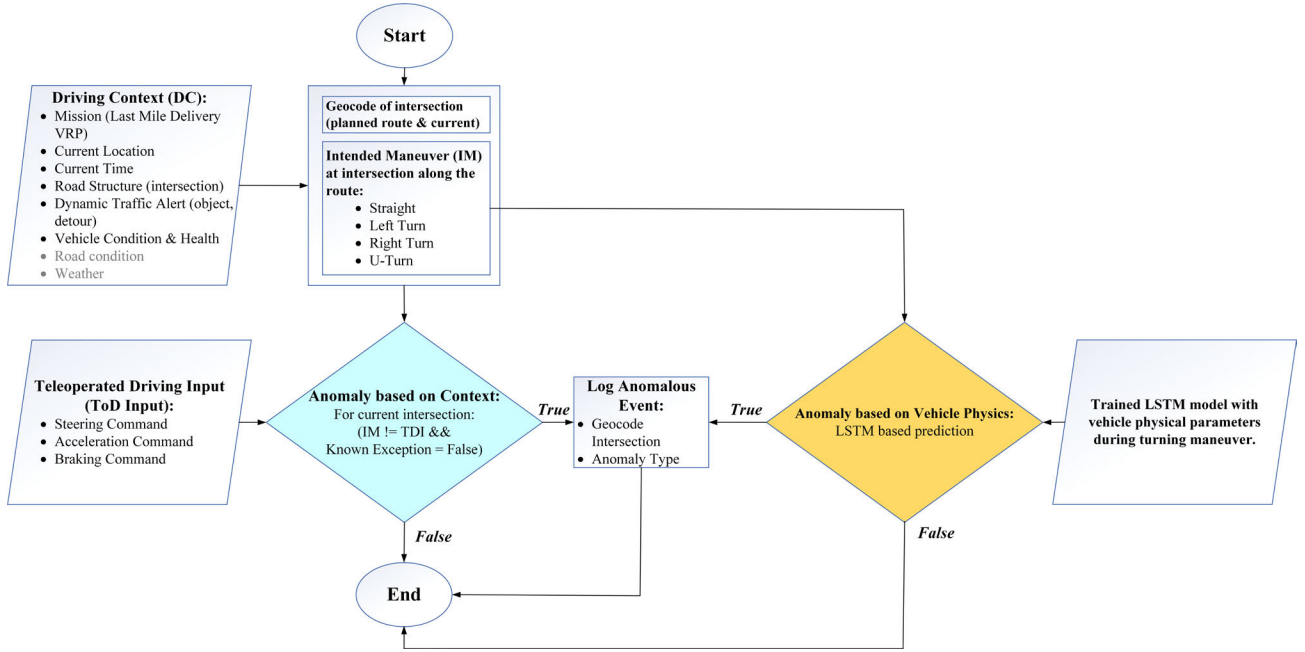
FIGURE 8. An LMD ToD anomaly detection framework.

multiple environmental and operational parameters:

$$D_C = f_1(m, \gamma, t, \omega, \tau, l, \varepsilon) \tag{2}$$

Here, the DC incorporates the mission parameters (m), current road conditions (γ), traffic congestion levels (t), weather conditions (ω), temporal information (τ), geographical location (l), and various dynamic factors (ε) that may influence driving decisions. Furthermore, the system takes into account the predetermined route (R) as well as the intersection points (f) along the trajectory. The IM prediction follows from the DC through Eq. (3):

$$D_M \in \{st, lt, rt, ut\} = f_2(D_C) \tag{3}$$

This function maps the contextual information to specific maneuver types: continuing straight (st), executing a left turn (lt), performing a right turn (rt), or making a U-turn (ut). Subsequently, these IMs translate into specific vehicle control commands that are illustrated in Eq. (4):

$$D_I \in \{Cmd_{str}, Cmd_{accl}, Cmd_{Brk}\} = f_3(D_M) \tag{4}$$

These commands encompass steering inputs (Cmd_{str}), acceleration commands (Cmd_{accl}), and braking instructions (Cmd_{Brk}), with vehicle health status ($\hat{H}$) and context-based anomaly flags (A'_C) being monitored throughout. This detection framework implements three distinct verification mechanisms to identify potential security breaches or system malfunctions as follows:

1) INCORRECT MANEUVER DETECTION AT INTERSECTIONS
The initial detection mechanism continuously observes the vehicular behavior at designated intersection locations. When the vehicle (V) operates under an active mission (m), the

system initializes tracking for the vehicle's lateral position ($D_{I_{Lat}}$), longitudinal position ($D_{I_{Long}}$), and executed maneuver ($D_{I_{Mnvr}}$). As the vehicle navigates the planned route, the system locates all intersection features and establishes a reference database (E) containing expected lateral positions, expected longitudinal positions, and anticipated maneuvers. Throughout the operational phase, the system persistently evaluates the actual vehicle position and maneuver relative to the anticipated parameters. In the event that an inconsistency is identified, particularly when the maneuver executed at the current location deviates from the expected maneuver at the corresponding position, an anomaly flag (A'_C) is activated and documented within the database.

2) TEMPORAL WINDOW VALIDATION
The second verification layer implements temporal constraints on the anomaly detection process. This layer enhances spatial validation by integrating time-dependent parameters (τ). The system assesses whether maneuvers are executed within acceptable time frames by correlating the actual timing of maneuvers with predefined temporal limits. In instances where a vehicle executes a maneuver at the correct spatial location but beyond the expected temporal window, this temporal deviation activates an anomaly alert. This method efficiently detects attacks that might exploit timing manipulations to trigger hazardous conditions while preserving spatial integrity.

3) DYNAMIC ALERT FILTERING AND FALSE POSITIVE REDUCTION
The third component mitigates the issue of false positives through the implementation of intelligent filtering. This mechanism considers dynamic environmental factors (ε) and

vehicle health status ($\hat{H}$) before confirming an anomaly. The system conducts standard positional and temporal validations, further ensuring the absence of dynamic factors and confirming the vehicle's health status as indicating normal operation. The system confirms the anomaly flag exclusively when two criteria are met: there is no dynamic interference ($\varepsilon = \text{NULL}$), and the vehicle's health status is verified as satisfactory ($\hat{H} = \text{OK}$). This comprehensive verification approach effectively minimizes the occurrence of false positives, yet continues to preserve the sensitivity required to detect authentic security threats.

This extensive context-aware methodology guarantees effective anomaly detection by utilizing environmental insights, temporal limitations, and advanced filtering to differentiate between authentic operational deviations and possible security breaches within tele-operated vehicle systems.

B. STAGE 2: PCADS-PHYSICS-INFORMED ANOMALY DETECTION

The PCADS-PI method leverages the vehicle's physical elements (e.g., power transfer, vehicle dynamics) to validate cyber-element commands (e.g., steering, acceleration). As shown in Fig. 9, the detection mechanism is divided into a vehicle physics domain and a learning/prediction domain. ToD inputs are fed into the vehicle physics model, whose output is then passed to an ML algorithm that learns the correlation between physical responses and specific maneuvers to predict deviations.

1) PROPOSED MATHEMATICAL MODELING
The PCADS-PI framework is modeled as follows.

a: INPUTS
Time-series ToD inputs include acceleration-pedal-position (APP), steering-wheel-angle (SW), and brake-pedal-status (BP) over a time window of size N.

$$\text{APP} \rightarrow \{APP_{t-N}, \ldots, APP_t\} \tag{5}$$

$$\text{SW} \rightarrow \{SW_{t-N}, \ldots, SW_t\} \tag{6}$$

$$\text{BP} \rightarrow \{BP_{t-N}, \ldots, BP_t\} \tag{7}$$

b: VEHICLE MODEL & CONFIGURATION
The vehicle model translates inputs into motion based on its configuration, including drivetrain (D), steering system, and tires.

- **Drivetrain Dynamics:** $T_{output} = f(APP_t, D)$
- **Steering Dynamics:** $\theta_{steer} = g(SW_t)$
- **Braking Dynamics:** $a_{deceleration} = h(BP_t)$

The overall motion is determined by integrating these dynamics into the vehicle's equations of motion:

$$\frac{d(\text{Vehicle State})}{dt} = \Psi(T_{output}, \theta_{steer}, a_{deceleration},$$

$$\text{Vehicle Configuration}) \tag{8}$$

c: MODEL PARAMETERS
The model integrates control inputs with physical responses from the Energy Storage System (ESS), Motors (M), and Vehicle Dynamics (VD).

- **ESS Dynamics:** Battery power $P_{battery}$ is the sum of motor power consumption.
- **Motor Dynamics:** Torque and speed are functions of APP and vehicle state.
- **Vehicle Dynamics:** Parameters like Wheel Angle (WA), Roll (R), Pitch (PT), and Yaw are derived from steering, braking, and acceleration forces.

2) MACHINE LEARNING FRAMEWORK
Various ML methods were reviewed, including Naive Bayes, Decision Tree, SVM, and KNN. The Long Short-Term Memory (LSTM) algorithm, a type of RNN, was selected as the base model due to its efficacy in learning from complex sequential data [87], [88]. An LSTM unit (Fig. 10) uses a cell state and gates (input, forget, output) to regulate information flow, enabling it to capture long-term dependencies in time-series data. For this research, the LSTM model is applied to data from a full-electric vehicle model, using parameters from the ESS and traction motors.

a: A VEHICLE MODEL INTEGRATION INTO THE LSTM FRAMEWORK
The architecture for processing temporal sequences employs an LSTM, which at each timestep, t, processes a feature vector as its input, defined as $\mathbf{x}_t = [E_t, M_t, VD_t]$. These components represent the ESS parameters (E_t), motor characteristics (M_t), and vehicle dynamics measurements (VD_t), respectively. The LSTM network navigates this information utilizing a sequence of gating mechanisms, which are analytically represented in different parts. The **input gate** controls information flow into the cell state, which can be illustrated as $i_t = \sigma(W_{xi} \cdot x_t + W_{hi} \cdot h_{t-1} + b_i)$. The **forget gate** as $f_t = \sigma(W_{xf} \cdot x_t + W_{hf} \cdot h_{t-1} + b_f)$ determines which previous information to retain. The **cell state update** combines new and retained information which can be presented as $g_t = \tanh(W_{xg} \cdot x_t + W_{hg} \cdot h_{t-1} + b_g)$ and $c_t = f_t \cdot c_{t-1} + i_t \cdot g_t$. The **output gate** produces the final hidden state through $o_t = \sigma(W_{xo} \cdot x_t + W_{ho} \cdot h_{t-1} + b_o)$ and $h_t = o_t \cdot \tanh(c_t)$. In this context, σ signifies the sigmoid activation function, with W matrices indicating the acquired weights, b vectors serving as bias components, and h_{t-1} along with c_{t-1} denoting the prior hidden and cell states, respectively.

The PCADS-PI methodology utilizes a trained LSTM network to assess sequential vehicular parameter information and categorizes turning maneuvers into separate types, such as left turns, right turns, and U-turns. The approach to anomaly detection is grounded in probabilistic principles, allowing for the calculation of logarithmic probability scores for each classification of turns based on the observed physical
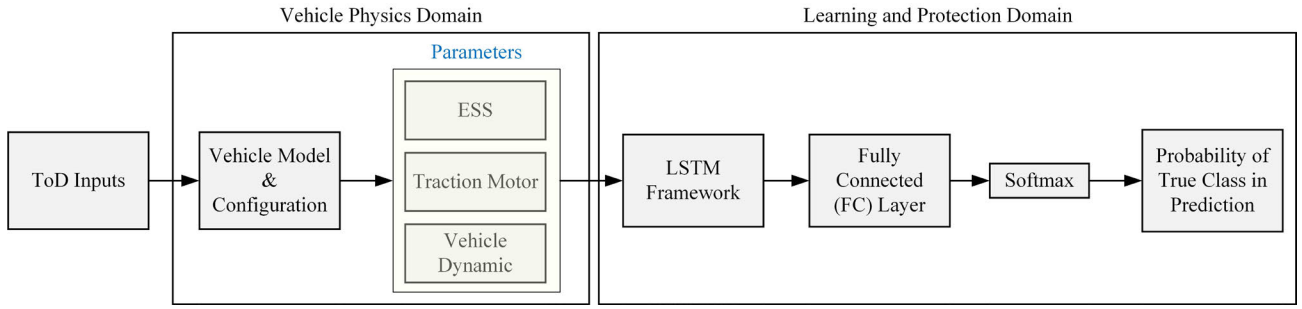
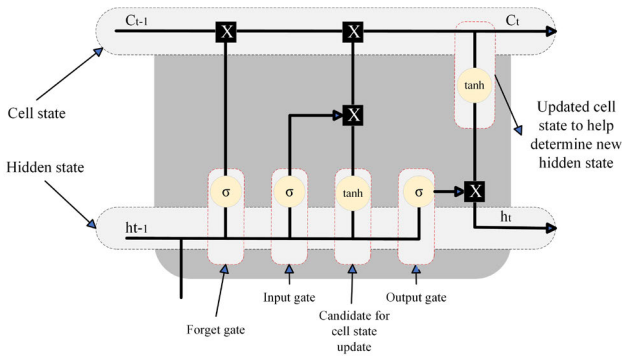**FIGURE 9.** A vehicle physics informed anomaly detection framework.

FIGURE 10. A standard LSTM cell showing forget, input, and output gates with σ/tanh activations and state propagation paths [89].

Latitude	Longitude	Action	Alert
42.3296	-83.04723	START	NULL
42.32925	-83.04804	RT	NULL
42.33012	-83.04877	LT	NULL
42.32971607	-83.04983611	NO	DETOUR
42.32933352	-83.0507632	LT	VEH_HEALTH
42.3284566	-83.05003838	RT	NULL
42.3281031	-83.05090448	STOP	OBJECT

FIGURE 11. Results for the PCADS-CA incorrect maneuvers.

parameters. The process of detection adheres to the following statement.

Given an expected turn type based on system inputs or driver commands, $\log P(\text{Turn}_{\text{Expected}})$ can be calculated and compared against $\log P(\text{Turn}_{\text{Other}})$ for all alternative turn classifications. An anomaly indicator A'_P is initiated upon meeting the condition:

$$\log P(\text{Turn}_{\text{Expected}}) < \log P(\text{Turn}_{\text{Other}}) \qquad (9)$$

The physical behavior of the vehicle appears more aligned with an unexpected type of turn than initially expected, indicating possible system anomalies or the presence of malicious interference. This probabilistic methodology guarantees the detection of anomalies whenever there are substantial deviations in the observed vehicle behavior from the anticipated dynamics, thereby offering a validation mechanism that is grounded in physics. The next section will thoroughly validate this detection method experimentally.

IV. EXPERIMENT AND RESULTS

This section presents the experimental setup and the resulting outcomes to assess the effectiveness of the proposed PCADS model. In order to demonstrate the two stages of the PCADS model, this section is divided into two parts, including the PCADS-CA method and the PCADS-PI method.
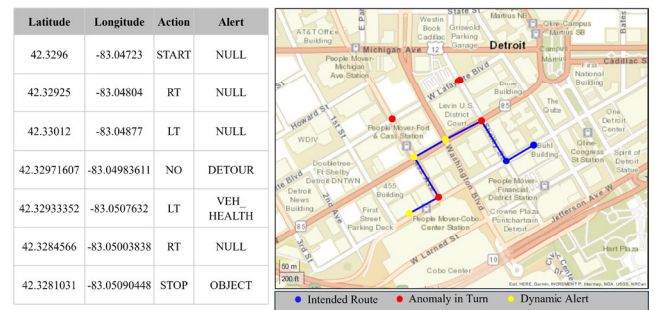
A. PCADS-CA MODEL

The experiment with the PCADS-CA stage has three steps. First, an original route plan for a delivery vehicle is created with a web-based route planning service from *MyRouteOnline* [90]. This provides the IM at each intersection along the delivery route derived from DCs. This corresponds to IM and DC processes in Fig. 8. Secondly, the ToD input is created by altering the original route, which includes the expected turn at certain intersections along the route and the modification of the expected time window of the turn. Additionally, an input is added to indicate if there is any dynamic alert on a particular intersection. In the final step, IM from step 1 and altered ToD input and dynamic alert from step 2 are passed to the PCADS-PI algorithm proposed in Section III-B. This algorithm is implemented using a MATLAB script such that the results of this experiment are presented in Fig. 11. According to this figure, the table shows the DC including the original intended maneuvering action for intersections along the selected delivery route. The most column shows the dynamic alert for an intersection. The diagram shows the results of the PCADS-CA detection. According to this diagram, the blue line indicates the original route and blue dots denote the intersections along the route. The red dots indicate that the PCADS-CA method's detected anomalies in an actual maneuver from the intended action. However, the results also notify about the dynamic alerts at intersections along the route. Generally, the results illustrate that the PCADS-CA model can detect the first stage of anomalies based on the DC. Further, it also provides notification of
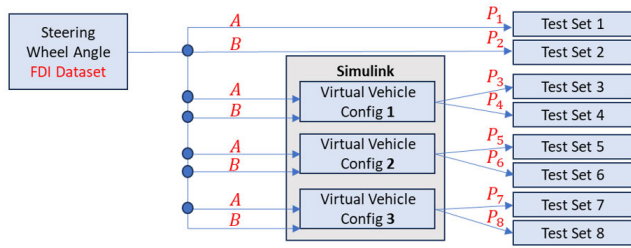
A = (point of injection before turing, duration 2 seconds)
B = (point of injection middle of turing, duration 2 second)

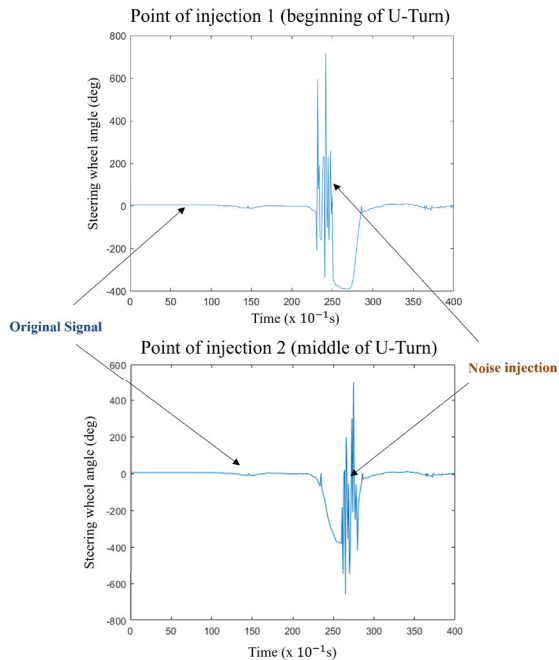**FIGURE 12.** Results for the PCADS-CA incorrect maneuvers.

FIGURE 13. An attack on the steering wheel command.

dynamic alerts to reduce FPs. In the next part, experiments and results for the second stage of the PCADS model are discussed.

B. PCADS-PI MODEL

This section elaborates on the experiment and results with the physics-informed AD stage of the PCADS model. This experiment has two primary steps, including data generation and the AD process, that are described below.

1) DATA GENERATION

An experimental dataset for the PCADS-PI model is generated based on the real dataset known as "D2CAV." The dataset contains 75 left turn, 78 right turn, and 62 U-turn scenarios. As per the scope of this paper, steering wheel angle, accelerator pedal, and brake pedal signals are extracted from this dataset. The signals are recorded every 100 ms. This

TABLE 3. A Comparison of ML algorithms for good dataset.

Classifier Type	Class	Accuracy	Precision	Recall	F1-score
Tree	Left Turn	0.85	0.78	0.83	0.80
	Right Turn	0.94	0.92	0.92	0.92
	U-Turn	0.89	0.84	0.77	0.81
Narrow NN	Left Turn	0.80	0.73	0.68	0.70
	Right Turn	0.89	0.83	0.88	0.86
	U-Turn	0.86	0.76	0.76	0.76
Medium NN	Left Turn	0.87	0.88	0.75	0.81
	Right Turn	0.92	0.84	0.97	0.90
	U-Turn	0.91	0.85	0.82	0.84
Wide NN	Left Turn	0.87	0.86	0.75	0.80
	Right Turn	0.91	0.82	0.97	0.89
	U-Turn	0.93	0.91	0.84	0.87
Bi-layered NN	Left Turn	0.81	0.74	0.69	0.72
	Right Turn	0.89	0.82	0.88	0.85
	U-Turn	0.88	0.80	0.79	0.80
Tri-layered NN	Left Turn	0.82	0.75	0.72	0.73
	Right Turn	0.87	0.83	0.82	0.83
	U-Turn	0.86	0.74	0.79	0.77
LSTM	Left Turn	0.99	0.99	0.99	0.99
	Right Turn	0.95	0.99	0.89	0.94
	U-Turn	0.95	0.83	0.99	0.91

TABLE 4. The LSTM prediction probability score.

Left Turn	Right Turn	U-Turn	Prediction	Test	Status
0.05	0.92	0.03	'RT'	'RT'	TRUE
0.86	0.08	0.07	'LT'	'LT'	TRUE
0.05	0.03	0.91	'UT'	'UT'	TRUE
0.10	0.85	0.04	'RT'	'UT'	FALSE
0.05	0.93	0.02	'RT'	'UT'	FALSE
0.94	0.01	0.05	'LT'	'RT'	FALSE

dataset is referred to as a good ToD input dataset. In the next step, this dataset is used as inputs to simulate virtual vehicle models. One dataset of the vehicle physical parameters is created with the good ToD input dataset and another is created for the attack dataset as an input. The data generation of vehicle parameters with steering wheel angle FDI injection is illustrated in Fig. 12. In this diagram, steering wheel input is shown as FDI noise at two different points, A and B during the turning action. It can be noted that the good data generation for vehicle physical parameters is a similar process except for the FDI in any input. The configuration of the virtual vehicle model and the set of vehicle physical parameters recorded by simulating the virtual vehicles are the same for good ToD input and ToD input with noise. To generate the good dataset of vehicle physical parameters, the virtual vehicle model is simulated without the good ToD input dataset. The virtual vehicle models are selected from three potential electric drive train configurations with six degrees of freedom. Virtual Vehicle Config 1, 2, 3 refer to a single motor, dual motor, and quad motor used as propulsion motors. Vehicle physical parameters are selected from three subsystems including the energy storage system, traction motor, and vehicle dynamics. The virtual vehicle model is configured and simulated in MATLAB/SIMULINK software. To inject the noise, the attack formula, shown in Eq. (1) is implemented using MATLAB. As illustrated in

TABLE 5. An AD rate against 8 test sets (TSs) of FDI attacks.

TS#	A.1	A.2	B.1	B.2	C.1	C.2	D.1	D.2
No. of anomaly detected	10	9	16	15	20	11	30	30
No. of FDI tested	30	30	30	30	30	30	30	30
ADR (%)	33.33	30	**53.33**	50	**66.67**	36.67	**100**	33.33

Fig. 13, an attack dataset consists of two points of injection in the steering wheel angle command and the duration of the injected noise is 2 s. The points of injection are at the beginning of turns and during the mid-point of turning. The attack dataset is created by injecting noise into the steering wheel angle in 30 randomly selected observations of the left turn, right turn, and U-turn scenarios. In the final step of data generation, the good dataset and attack dataset of vehicle physical parameters generated from the virtual vehicle model are formatted to train and test the anomaly detection model.

2) ANOMALY DETECTION

An anomaly in trajectory patterns of turning maneuvers is formulated as a sequence to a classification problem. For that reason, the experiment is divided into two steps. Initially, the experiment is conducted to train the ML model with a good dataset and predict 3 classes (i.e., left turn, right turn, and U-turn). A tree-based classifier and 7 NN architectures are trained using the MATLAB DL tool in this case, and the performance is evaluated with standard metrics (i.e., accuracy, precision, recall, F1-score). A value for each metric can range between 0 and 1, where a higher value shows better performance, and the results are presented in Tables 3. According to this table, the LSTM performance is as follows: minimum accuracy: 0.95, lowest precision: 0.83, lowest recall: 0.89 and lowest F1-score: 0.91. This shows that LSTM predicted left turn, right turn, and U-turn with higher true positive values and true negative values as compared to other neural network architectures employed in this experiment. Based on this observation, an LSTM algorithm is chosen as a base model for the PCADS-PI method.

The resulting data is subjected to an in-depth analysis, the aim of which is to determine the probability density score associated with both correctly and incorrectly predicted observations. An illustrative instance of this analytical approach is exhibited within Table 4.

It might be noted that the probability score ranges from 0 to 1. As shown in Table 4, the highest probability score observed by an ML classifier for a particular class is reported as a predicted class. When the predicted class matches the true class provided in a test sample, the prediction is TRUE (shown with a green color) while the prediction is FALSE when the probability score of the true class is not the highest one (shown with a red color). This observation verifies that the LSTM model is able to capture the temporal dependencies

and effectively learns the pattern of physical parameters for a valid maneuver. The probability score analysis also shows that the model lowers the probability score when the sequence is anomalous. In the final step, the trained LSTM model with a good dataset is tested with the attack dataset generated in Section IV-B1 and the results are presented in Table 5.

Each TS# column provides an anomaly detection rate (ADR) for a set of tests with 30 samples of FDI turning maneuvers. 'A', 'B', 'C' and 'D' indicate what kind of data is used to train the model in TS#. 'A' means the trained LSTM model with a ToD input. 'B' shows the trained LSTM model with vehicle physical parameters for a single motor electric vehicle. The trained LSTM model with vehicle physical parameters for dual and quad motor electric vehicles is mentioned by 'C' and 'D', respectively. The number 1 in TS# indicates the point of noise injection at the beginning of turning and 2 means noise is injected at the middle of the turning. As detailed in Table 5, the Anomaly Detection Rate (ADR) progressively increases with the complexity of the vehicle's drivetrain model. The model trained on single-motor parameters (TS B.1, 53.33% ADR) outperforms the baseline ToD input model (TS A.1, 33.33% ADR). This performance is further enhanced with dual-motor parameters (TS C.1, 66.67% ADR) and culminates in a 100% ADR for the quad-motor configuration (TS D.1). This demonstrates that parameters related to the drivetrain—specifically individual motor torque, speed, and power consumption—are the most critical for detection. These parameters provide a high-fidelity, difficult-to-spoof fingerprint of the vehicle's physical state. A quad-motor configuration offers the most granular data, as an attacker would need to simultaneously spoof the complex, differential torque distribution across all four motors to remain undetected, which is a significantly more challenging task.

V. CONCLUSION AND FUTURE DIRECTIONS

A foundational framework for the cyber-physical security of ToD systems was established by this paper. Through a TARA, FDI attacks on steering commands were identified as a high-risk vulnerability. Subsequently, a novel attack model was developed, and, most critically, a PCADS was proposed and validated to mitigate this threat. The core hypothesis of this work is validated by the experimental results. A model based solely on control inputs is outperformed by a physics-informed detection model that uses an LSTM

architecture, which is adept at capturing temporal patterns, to effectively learn the physical signature of a valid maneuver from vehicle physical parameters.

A foundation for research to develop robust and intrinsic security layers for ToD, extending the Defense-in-Depth (DiD) paradigm into the vehicle's physical domain, is provided by the contributions presented here—the ToD threat model, the FDI attack formulation, and the PCADS framework. This is critical for a comprehensive cyber-physical security roadmap. As part of future work, a holistic dataset for FDI attacks on ToD control with various combinations of noise, points of injection, and attack durations is planned to be developed. As an extension of the PCADS model, other AD approaches will be explored, and a comparative performance analysis will be carried out on this extensive attack dataset.

APPENDIX
DATA AVAILABILITY AND SUPPLEMENTARY MATERIAL

The source codes, datasets, and additional supplementary materials supporting the findings of this study are publicly available through the GitHub repository (https://github.com/ghostsubha/TODS_LMD_AD). This repository contains comprehensive implementation details, experimental scripts, datasets, and detailed instructions for reproducing all results.

REFERENCES

[1] S. Lu, R. Zhong, and W. Shi, "Teleoperation technologies for enhancing connected and autonomous vehicles," in *Proc. IEEE 19th Int. Conf. Mobile Ad Hoc Smart Syst. (MASS)*, Oct. 2022, pp. 435–443.

[2] A. Davies, "Self-driving cars have a secret weapon: Remote control," *Wired, Feb*, Feb. 2018. [Online]. Available: https://www.wired.com/story/phantom-teleops/

[3] A. Zaboli, J. Hong, J. Kwon, and J. Moore, "A survey on cyber-physical security of autonomous vehicles using a context awareness method," *IEEE Access*, vol. 11, pp. 136706–136725, 2023.

[4] (2021). *Tele-Operated Driving Use Cases, System Architecture and Bus. Considerations*. [Online]. Available: https://5gaa.org/content/uploads/2021/12/5GAA_Tele_operated_Driving_White_Paper.pdf

[5] O. Amador, M. Aramrattana, and A. Vinel, "A survey on remote operation of road vehicles," *IEEE Access*, vol. 10, pp. 130135–130154, 2022.

[6] G. Ayfantopoulou et al., "Enabling innovation in transport & logistics: A 5G approach," in *Proc. Netw. Commun. (EuCNC), Eur. Conf.*, 2023, pp. 1–5.

[7] P. M. D'Orey, A. Hosseini, J. Azevedo, F. Diermeyer, M. Ferreira, and M. Lienkamp, "Hail-a-drone: Enabling teleoperated taxi fleets," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2016, pp. 774–781.

[8] (2022). *Teleoperation Expanding the Solution Space for Automated Driving*. [Online]. Available: https://www.nist.gov/news-events/news/2022/09/teleoperation-expanding-solution-space-automated-driving

[9] *5G-Blueprint Forum on Teleoperation—Event Highlights*. Accessed: May 2, 2024. [Online]. Available: https://5gblueprint.eu/5g-blueprint-forum-on-teleoperation-event-highlights/

[10] *Faction Announces Commercial Expansion of DriveLink and TeleAssist Technologies to Simplify Self-Driving Systems for OEMs and other Customers*. Accessed: Feb. 14, 2024. [Online]. Available: https://www.businesswire.com/news/home/20230227005249/en/Faction-Announces-Commercial-Expansion-of-DriveLink-and-TeleAssist-Technologies-to-Simplify-Self-Driving-Systems-for-OEMs-and-other-Customers

[11] DriveU. *Auto Solution in Level 4 Autonomous Shuttle Operations*. Accessed: Jun. 25, 2024. [Online]. Available: https://driveu.auto/blog/driveu-autos-solution-deployed-in-level-4-autonomous-shuttle-operations/

[12] *Ottopia And Hyundai Mobis Team For Automotive Grade Teleoperation Platform*. Accessed: Feb. 3, 2024. [Online]. Available: https://www.forbes.com/sites/samabuelsamid/2022/12/20/ottopia-and-hyundai-mobis-team-for-automotive-grade-teleoperation-platform/

[13] *Amazon's Zoox Robotaxi Drives on Public Roads in California for the First Time*. Accessed: Oct. 25, 2023. [Online]. Available: https://www.cnn.com/2023/02/14/tech/amazon-zoox-robotaxi/index.html

[14] (2024). *Vay Launches Commercial Driverless Mobility Service With Remotely Driven Cars in Las Vegas, Nevada*. [Online]. Available: https://vay.io/press-release/vay-launches-commercial-driverless-mobility-service-with-remotelydriven-cars-in-las-vegas-nevada/

[15] T. Zhang, "Toward automated vehicle teleoperation: Vision, opportunities, and challenges," *IEEE Internet Things J.*, vol. 7, no. 12, pp. 11347–11354, Dec. 2020.

[16] V. S. Mai, R. J. La, T. Zhang, and A. Battou, "End-to-end quality-of-service assurance with autonomous systems: 5G/6G case study," in *Proc. IEEE 19th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2022, pp. 644–651.

[17] C. Cai, Y. Zhang, and Q. Chen, "Adaptive control of bilateral teleoperation systems with false data injection attacks and attacks detection," in *Proc. 41st Chin. Control Conf. (CCC)*, Jul. 2022, pp. 4407–4412.

[18] *How Jeep Hackers Took Over Steering And Forced Emergency Stop At High Speed*. Accessed: Nov. 3, 2023. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2016/08/02/charlie-miller-chris-valasek-jeep-hackers-steering-brake/

[19] *Three Landmark UN Vehicle Regulations Enter into Force*. Accessed: Oct. 8, 2022. [Online]. Available: https://unece.org/sustainable-development/press/three-landmark-un-vehicle-regulations-enter-force

[20] M. T. Rahman, M. S. Rahman, H. Wang, S. Tajik, W. Khalil, F. Farahmandi, D. Forte, N. Asadizanjani, and M. Tehranipoor, "Defense-in-depth: A recipe for logic locking to prevail," *Integration*, vol. 72, pp. 39–57, May 2020.

[21] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang, "A survey on access control in the age of Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 4682–4696, Jun. 2020.

[22] Q. Tang, O. Ermis, C. D. Nguyen, A. D. Oliveira, and A. Hirtzig, "A systematic analysis of 5G networks with a focus on 5G core security," *IEEE Access*, vol. 10, pp. 18298–18319, 2022.

[23] B. Hu and X. Heng, "Research on 5G security protection system for industry," in *Proc. Int. Conf. Informat., Netw. Comput. (ICINC)*, Oct. 2022, pp. 142–146.

[24] *NSA'S Top Ten Cybersecurity Mitigation Strategies*. Jul. 20, 2023. [Online]. Available: https://www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf

[25] *Our Living, Function-Based Approaches Help Manage Vehicle Cyber Risk*. Accessed: Sep. 25, 2023. [Online]. Available: https://automotiveisac.com/best-practice-guides

[26] *High-Performance Computing Security: Architecture, Threat Analysis, and Security Posture*. Accessed: Jun. 25, 2024. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/223/final

[27] H. Gupta, S. Mondal, R. Majumdar, N. S. Ghosh, S. Suvra Khan, N. E. Kwanyu, and V. P. Mishra, "Impact of side channel attack in information security," in *Proc. Int. Conf. Comput. Intell. Knowl. Economy (ICCIKE)*, Dec. 2019, pp. 291–295.

[28] J. Kaur and K. R. Ramkumar, "The recent trends in cyber security: A review," *J. King Saud University-Computer Inf. Sci.*, vol. 34, no. 8, pp. 5766–5781, 2021.

[29] G. Tsochev, R. Trifonov, O. Nakov, S. Manolov, and G. Pavlova, "Cyber security: Threats and challenges," in *Proc. Int. Conf. Automatics Informat. (ICAI)*, Oct. 2020, pp. 1–6.

[30] *Defense-In-Depth*. Accessed: May 25, 2024. [Online]. Available: https://csrc.nist.gov/glossary/term/defense_in_depth

[31] *Secure Product Design Cheat Sheet*. Accessed: Jul. 12, 2024. [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Secure_Product_Design_Cheat_Sheet.html

[32] National Institute of Standards and Technology (NIST). (Jun. 2013). *Improving Critical Infrastructure Cybersecurity Executive Order 13636: Preliminary Cybersecurity Framework*. [Online]. Available: https://www.nist.gov/sites/default/files/documents/itl/-cybersecurity-framework.pdf

[33] J.-P.-A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli, "Cyber-physical systems security: Limitations, issues and future trends," *Microprocessors Microsystems*, vol. 77, Sep. 2020, Art. no. 103201.

[34] F. Alrefaei, A. Alzahrani, H. Song, M. Zohdy, and S. Alrefaei, "Cyber physical systems, a new challenge and security issue for the aviation," in *Proc. IEEE Int. IoT, Electron. Mechatronics Conf. (IEMTRONICS)*, Apr. 2021, pp. 1–5.

[35] S. U. Rehman, C. Allgaier, and V. Gruhn, "Security requirements engineering: A framework for cyber-physical systems," in *Proc. Int. Conf. Frontiers Inf. Technol. (FIT)*, Dec. 2018, pp. 315–320.

[36] M. Elnour, N. Meskin, K. Khan, and R. Jain, "A dual-isolation-forests-based attack detection framework for industrial control systems," *IEEE Access*, vol. 8, pp. 36639–36651, 2020.

[37] J. Ye, L. Guo, B. Yang, F. Li, L. Du, L. Guan, and W. Song, "Cyber–Physical security of powertrain systems in modern electric vehicles: Vulnerabilities, challenges, and future visions," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 4, pp. 4639–4657, Aug. 2021.

[38] X. Ning and J. Jiang, "Defense-in-depth against insider attacks in cyber-physical systems," *Internet Things Cyber-Phys. Syst.*, vol. 2, pp. 203–211, Jan. 2022.

[39] C. Wang, B. Wang, H. Liu, and H. Qu, "Anomaly detection for industrial control system based on autoencoder neural network," *Wireless Commun. Mobile Comput.*, vol. 2020, pp. 1–10, Aug. 2020.

[40] H. Zhang, B. Liu, and H. Wu, "Smart grid cyber-physical attack and defense: A review," *IEEE Access*, vol. 9, pp. 29641–29659, 2021.

[41] *Vehicle Cybersecurity*. Jun. 25, 2024. [Online]. Available: https://www.nhtsa.gov/research/vehicle-cybersecurity#the-topic-cybersecurity-protection-methods

[42] *Immune System for Vehicle Computers*. Accessed: Sep. 25, 2024. [Online]. Available: https://www.etas.com/ww/en/products-services/cybersecurity-products/escrypt-intrusion-detection-and-prevention-solution/

[43] *Welcome to Auto-ISAC! Monthly Virtual Community Call*. Accessed: Aug. 25, 2024. [Online]. Available: https://static1.squarespace.com/static/618a9a805a5be466f28052a2/t/6230a6cae113133b09fa0374/1647355596988/2022_02_02_Auto-ISAC_02Feb22_CC_FINAL-1.pdf

[44] *Specification of Intrusion Detection System Protocol*. Accessed: Aug. 15, 2024. [Online]. Available: https://www.autosar.org/fileadmin/standards/R20-11/FO/AUTOSAR_PRS_IntrusionDetectionSystem.pdf

[45] H.-J. Liao, C. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 16–24, 2012.

[46] A. Milenkoski, M. Vieira, S. Kounev, A. Avritzer, and B. D. Payne, "Evaluating computer intrusion detection systems: A survey of common practices," *ACM Comput. Surveys*, vol. 48, no. 1, pp. 1–41, Sep. 2015.

[47] A. Zaboli, S. Lok Choi, T.-J. Song, and J. Hong, "ChatGPT and other large language models for cybersecurity of smart grid applications," 2023, *arXiv:2311.05462*.

[48] C. Young, J. Zambreno, H. Olufowobi, and G. Bloom, "Survey of automotive controller area network intrusion detection systems," *IEEE Design Test*, vol. 36, no. 6, pp. 48–55, Dec. 2019.

[49] J. Xiao, L. Yang, F. Zhong, H. Chen, and X. Li, "Robust anomaly-based intrusion detection system for in-vehicle network by graph neural network framework," *Int. J. Speech Technol.*, vol. 53, no. 3, pp. 3183–3206, Feb. 2023.

[50] S. Rajapaksha, H. Kalutarage, M. O. Al-Kadri, A. Petrovski, G. Madzudzo, and M. Cheah, "AI-based intrusion detection systems for in-vehicle networks: A survey," *ACM Comput. Surveys*, vol. 55, no. 11, pp. 1–40, Nov. 2023.

[51] S. Rajendar and V. Kumar Kaliappan, "Sensor data based anomaly detection in autonomous vehicles using modified convolutional neural network," *Intell. Autom. Soft Comput.*, vol. 32, no. 2, pp. 859–875, 2022.

[52] F. van Wyk, Y. Wang, A. Khojandi, and N. Masoud, "Real-time sensor anomaly detection and identification in automated vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 3, pp. 1264–1276, Mar. 2020.

[53] A. Aboah, M. Shoman, V. Mandal, S. Davami, Y. Adu-Gyamfi, and A. Sharma, "A vision-based system for traffic anomaly detection using deep learning and decision trees," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jun. 2021, pp. 4207–4212.

[54] S. S. Sarikan and A. M. Ozbayoglu, "Anomaly detection in vehicle traffic with image processing and machine learning," *Proc. Comput. Sci.*, vol. 140, pp. 64–69, Jan. 2018.

[55] F. Caetano, P. Carvalho, and J. Cardoso, "Deep anomaly detection for in-vehicle monitoring—An application-oriented review," *Appl. Sci.*, vol. 12, no. 19, p. 10011, Oct. 2022.

[56] *Glossary: Anomaly*. Accessed: Apr. 24, 2024. [Online]. Available: https://undsci.berkeley.edu/glossary/anomaly/

[57] D. E. Denning, "An intrusion-detection model," *IEEE Trans. Softw. Eng.*, vols. SE–13, no. 2, pp. 222–232, Feb. 1987.

[58] R. Rai and C. K. Sahu, "Driven by data or derived through physics? A review of hybrid physics guided machine learning techniques with cyber-physical system (CPS) focus," *IEEE Access*, vol. 8, pp. 71050–71073, 2020.

[59] C. Ruben, S. Dhulipala, K. Nagaraj, S. Zou, A. Starke, A. Bretas, A. Zare, and J. McNair, "Hybrid data-driven physics model-based framework for enhanced cyber-physical smart grid security," *IET Smart Grid*, vol. 3, no. 4, pp. 445–453, Aug. 2020.

[60] F. Alotibi and M. Abdelhakim, "Anomaly detection for cooperative adaptive cruise control in autonomous vehicles using statistical learning and kinematic model," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3468–3478, Jun. 2021.

[61] J. Zhong, Y. Zhang, J. Wang, C. Luo, and Q. Miao, "Unmanned aerial vehicle flight data anomaly detection and recovery prediction based on spatio-temporal correlation," *IEEE Trans. Rel.*, vol. 71, no. 1, pp. 457–468, Mar. 2022.

[62] B. Huang and J. Wang, "Applications of physics-informed neural networks in power systems—A review," *IEEE Trans. Power Syst.*, vol. 38, no. 1, pp. 572–588, Jan. 2023.

[63] I. H. Sarker, "Machine learning: Algorithms, real-world applications and research directions," *Social Netw. Comput. Sci.*, vol. 2, no. 3, p. 160, May 2021.

[64] J. R. V. Solaas, E. Mariconti, and N. Tuptuk, "Systematic literature review: Anomaly detection in connected and autonomous vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 26, no. 1, pp. 43–58, Jan. 2025.

[65] P. Mansourian, N. Zhang, A. Jaekel, and M. Kneppers, "Deep learning-based anomaly detection for connected autonomous vehicles using spatiotemporal information," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 12, pp. 16006–16017, Dec. 2023.

[66] Y. Guo, K. A. Pant, and I. Hwang, "Physics-informed anomaly detection for unmanned aerial vehicles," *IEEE Robot. Autom. Lett.*, vol. 10, no. 10, pp. 9948–9955, Oct. 2025.

[67] M. A. Makridis and A. Kouvelas, "Adaptive physics-informed trajectory reconstruction exploiting driver behavior and car dynamics," *Sci. Rep.*, vol. 13, no. 1, p. 1121, Jan. 2023.

[68] R. Shi, Z. Mo, K. Huang, X. Di, and Q. Du, "A physics-informed deep learning paradigm for traffic state and fundamental diagram estimation," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 8, pp. 11688–11698, Aug. 2022.

[69] O. M. Manyar, S. V. Narayan, R. Lengade, and S. K. Gupta, "Physics-informed learning to enable robotic screw-driving under hole pose uncertainties," in *Proc. IEEE/RSJ Int. Conf. Intell. Robots Syst. (IROS)*, Oct. 2023, pp. 2993–3000.

[70] J. Fan, Z. Wang, and G. Li, "A novel unsupervised anomaly detection method on adversarial attacks for autonomous vehicles trajectory prediction," in *Proc. IEEE 22nd Int. Conf. Ind. Informat. (INDIN)*, Aug. 2024, pp. 1–18.

[71] B. Toghi, D. Grover, M. Razzaghpour, R. Jain, R. Valiente, M. Zaman, G. Shah, and Y. P. Fallah, "A maneuver-based urban driving dataset and model for cooperative vehicle applications," in *Proc. IEEE 3rd Connected Automated Vehicles Symp. (CAVS)*, Nov. 2020, pp. 1–6.

[72] *Teleoperation Consortium*. Accessed: Apr. 1, 2024. [Online]. Available: https://www.teleoperation.org/press-releases

[73] *NIST Vehicle Teleoperation Forum*. Accessed: May 18, 2024. [Online]. Available: https://www.nist.gov/news-events/events/2020/11/nist-vehicle-teleoperation-forum

[74] *5G Blueprint Remote Stations for Teleoperated Driving*. Accessed: Oct. 13, 2023. [Online]. Available: https://5g-ppp.eu/5g-blueprint-remote-stations-for-teleoperated-driving/

[75] D. Majstorovic, S. Hoffmann, F. Pfab, A. Schimpe, M.-M. Wolf, and F. Diermeyer, "Survey on teleoperation concepts for automated vehicles," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2022, pp. 1290–1296.

[76] D. Bogdoll, S. Orf, L. Töttel, and J. M. Zöllner, "Taxonomy and survey on remote human input systems for driving automation systems," in *Proc. Future Inf. Commun. Conf.*, 2022, pp. 94–108.

[77] S. Ghosh, A. Zaboli, J. Hong, and J. Kwon, "An integrated approach of threat analysis for autonomous vehicles perception system," *IEEE Access*, vol. 11, pp. 14752–14777, 2023.

[78] *Mitre Attck Matrices*. Accessed: May 15, 2024. [Online]. Available: https://attack.mitre.org/

[79] S. Soroushian, S. Khademi Sharifabad, M. Parsaee, and A. R. Afshari, "Toward a modern last-mile delivery: Consequences and obstacles of intelligent technology," *Appl. Syst. Innov.*, vol. 5, no. 4, p. 82, Aug. 2022.

[80] B. Anderson, M. Leardi-Anderson, and L. Tannous, "Automated trucking and border crossings," Cross-Border Inst., Univ. Windsor, Windsor, ON, Canada, Tech. Rep. 040318-V2, 2018.

[81] J. E. Muriel, L. Zhang, J. C. Fransoo, and R. Perez-Franco, "Assessing the impacts of last mile delivery strategies on delivery vehicles and traffic network performance," *Transp. Res. C, Emerg. Technol.*, vol. 144, Nov. 2022, Art. no. 103915.

[82] P. Penmetsa, P. Sheinidashtegol, A. Musaev, E. K. Adanu, and M. Hudnall, "Effects of the autonomous vehicle crashes on public perception of the technology," *IATSS Res.*, vol. 45, no. 4, pp. 485–492, Dec. 2021.

[83] N. Tiwapat, C. Pomsing, and P. Jomthong, "Last mile delivery: Modes, efficiencies, sustainability, and trends," in *Proc. 3rd IEEE Int. Conf. Intell. Transp. Eng. (ICITE)*, Sep. 2018, pp. 313–317.

[84] N. Goodall, "Non-technological challenges for the remote operation of automated vehicles," *Transp. Res. A, Policy Pract.*, vol. 142, pp. 14–26, Dec. 2020.

[85] *Overview: Type of Crash*. Accessed: Oct. 25, 2023. [Online]. Available: https://injuryfacts.nsc.org/motor-vehicle/overview/type-of-crash/

[86] J. Kurebwa and T. Mushiri, "A study of damage patterns on passenger cars involved in road traffic accidents," *J. Robot.*, vol. 2019, pp. 1–12, Jan. 2019.

[87] X. Li and F.-Y. Wang, "Scenarios engineering: Enabling trustworthy and effective AI for autonomous vehicles," *IEEE Trans. Intell. Vehicles*, vol. 8, no. 5, pp. 3205–3210, May 2023.

[88] H. Chu, H. Zhuang, W. Wang, X. Na, L. Guo, J. Zhang, B. Gao, and H. Chen, "A review of driving style recognition methods from short-term and long-term perspectives," *IEEE Trans. Intell. Vehicles*, vol. 8, no. 11, pp. 4599–4612, Nov. 2023.

[89] A. Zaboli, S. R. Kasimalla, K. Park, Y. Hong, and J. Hong, "A comprehensive review of behind-the-meter distributed energy resources load forecasting: Models, challenges, and emerging technologies," *Energies*, vol. 17, no. 11, p. 2534, May 2024.

[90] *MyRouteOnline*, 2009. [Online]. Available: https://www.myrouteonline.com

AYDIN ZABOLI (Member, IEEE) received the Ph.D. degree in electrical, electronics, and computer engineering from the University of Michigan, MI, USA. His research interests include smart grid security, autonomous vehicles, anomaly detection, energy management systems, SCADA, transportation electrification, renewable energy resources, and load forecasting. He was a recipient of the Rackham Predoctoral Fellowship from the University of Michigan-Rackham Graduate School, from 2024 to 2025. He has served as a reviewer for more than 250 papers in prestigious journals and conferences, particularly IEEE TRANSACTIONS ON SMART GRIDS, IEEE Transactions on Transportation Electrification, IEEE ACCESS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, contributing to the advancement of research in smart grids and transportation electrification.

JUNHO HONG (Senior Member, IEEE) received the Ph.D. degree in cyber-security of substation automation systems in electrical engineering from Washington State University, Pullman, in 2014. From 2014 to 2019, he worked with ABB, where he provided technical project leadership and supported strategic corporate technology development/productization in areas related to cyber-physical security for substations, power grid control and protection, renewable integration, and utility communications. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, University of Michigan–Dearborn. He has been working on the cybersecurity of energy delivery systems with the Department of Energy (DOE) as the Principal Investigator (PI) and the Co-PI in the areas of substations, microgrids, HVDC, FACTS, and high-power EV chargers. He serves in Cigre WG D2.50, "Electric Power Utilities Cyber-Security for Contingency Operations."

SUBHADIP GHOSH (Senior Member, IEEE) received the Bachelor of Technology degree in computer science and engineering from West Bengal University of Technology, India, in 2006, the M.S. degree in electric-drive vehicle engineering from Wayne State University, MI, USA, in 2014, and the Doctor of Engineering degree in automotive systems and mobility from the University of Michigan-Dearborn, USA, in 2024. Since 2006, he has been working on systems and software development for automotive ECUs in the body, EV, and ADAS domains. His research interests include cybersecurity and cyber-physical security of automated and connected vehicles.

JAEROCK KWON (Senior Member, IEEE) received the B.S. and M.S. degrees from Hanyang University, Seoul, South Korea, in 1992 and 1994, respectively, and the Ph.D. degree in computer engineering from Texas A&M University, College Station, USA, in 2009. From 1994 to 2004, he worked at LG Electronics, SK Teletech, and Qualcomm Internet Services. From 2009 to 2010, he was a Professor at the Department of Electrical and Computer Engineering, Kettering University, Flint, MI, USA. Since 2010, he has been a Professor at the Department of Electrical and Computer Engineering, University of Michigan–Dearborn, MI, USA. His research interests include mobile robotics, autonomous vehicles, and artificial intelligence. His awards and honors include the Outstanding Researcher Award, the Faculty Research Fellowship (Kettering University), and the SK Excellent Employee (SK Teletech). He served as the President for Korean Computer Scientists and Engineers Association in America (KOCSEA), in 2020 and 2021.

• • •