US DOT National
University Transportation Center for Safety

Carnegie Mellon University

Penn
University of Pennsylvania

The Ohio State University

CCAC Community College of Allegheny County

Community College of Philadelphia

The University of Texas Rio Grande Valley

Morgan State University

Project Title

Cyber resilience of connected and autonomous transportation systems (Phase I): State-of-the-art and research gaps

Investigators

Mohamadhossein Noruzoliaee (https://orcid.org/0000-0003-3860-8911)
Fatemeh Nazari (https://orcid.org/0000-0003-1587-1848)

Final Report – August 2025

DISCLAIMER

Technical Report Documentation Page

1. Report No. 547	**2. Government Accession No.**	**3. Recipient's Catalog No.**
4. Title and Subtitle Cyber resilience of connected and autonomous transportation systems (Phase I): State-of-the-art and research gaps		**5. Report Date** August 22, 2025 **6. Performing Organization Code**
7. Author(s) Mohamadhossein Noruzoliaee, Ph.D. https://orcid.org/0000-0003-3860-8911 Fatemeh Nazari, Ph.D. https://orcid.org/0000-0003-1587-1848		**8. Performing Organization Report No.**
9. Performing Organization Name and Address The University of Texas Rio Grande Valley (UTRGV) 1201 W University Dr Edinburg, Texas 78539		**10. Work Unit No.** **11. Contract or Grant No.** Federal Grant # 69A3552344811 / 69A3552348316
12. Sponsoring Agency Name and Address Safety21 University Transportation Center Carnegie Mellon University 5000 Forbes Avenue Pittsburgh, PA 15213		**13. Type of Report and Period Covered** Final Report (July 1, 2024 – June 30, 2025) **14. Sponsoring Agency Code** USDOT

15. Supplementary Notes
Conducted in cooperation with the U.S. Department of Transportation, Federal Highway Administration.

16. Abstract
Connected and autonomous transportation systems (CATS) promise major advances in efficiency and safety but also expose cyber-physical infrastructures to evolving cyber attacks that threaten security and safety. This survey provides a unified synthesis of cyber resilience in CATS, organized along three axes: (1) operational scale (micro, meso, and macro), (2) targeted functional domains (connectivity and autonomy) and cyber-physical components (sensing, control, and networking), and (3) attack-defense mapping, where attack surfaces are categorized by the confidentiality-integrity-availability (CIA) triad and defenses are aligned with resilience objectives (robustness, detection, response, recovery, and adaptation). Building on this taxonomy, the survey advances three contributions. First, it integrates attack surfaces, functional domains, cyber-physical components, defense strategies, and resilience objectives into a coherent framework spanning multiple scales of CATS. Second, it synthesizes methodological and assurance frontiers across theoretical approaches (optimization, game theory, and control theory), learning-based techniques (AI and adversarial machine learning), and emerging paradigms (quantum and post-quantum), together with validation infrastructures such as digital twins, testbeds, and benchmarking frameworks. Third, it articulates a forward-looking research agenda that identifies critical gaps, encompassing cross-layer resilience, unified trustworthiness, certified guarantees in safety-critical contexts, dual-use risks, lifecycle-aware resilience, and socio-technical integration. By consolidating fragmented research into a rigorous taxonomy and roadmap, this survey provides both the foundations and the future directions for advancing trustworthy and resilient transportation systems.

17. Key Words Cyber resilience; Connected and autonomous transportation systems; Multi-scale cyber-physical systems; Artificial intelligence security; Quantum and post-quantum resilience.	**18. Distribution Statement** No restrictions.

19. Security Classif. (of this report) Unclassified	**20. Security Classif. (of this page)** Unclassified	**21. No. of Pages** 50	**22. Price**

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized

Table of Contents

1. Introduction

1.1. Background and Motivation

Transportation systems are undergoing a foundational transformation, propelled by the convergence of connectivity, autonomy, and advanced computing. Connected and autonomous transportation systems (CATS) integrate vehicle-to-everything (V2X) communications, high-fidelity sensing, and artificial intelligence (AI) to enable real-time perception, prediction, and decision-making that collectively enhance safety, efficiency, and sustainability [1–3]. However, these same capabilities that underpin their transformative potential simultaneously introduce cyber vulnerabilities that are growing in sophistication, frequency, and scale, with the capacity to compromise operational reliability and public trust [4–7]. Consequently, modern transportation has emerged as a tightly coupled cyber-physical ecosystem in which the confidentiality of critical information, the integrity of operational data, and the availability of essential services are as indispensable to safe and resilient operations as the robustness of the physical infrastructure itself.

Documented incidents demonstrate that cyber attacks on transportation systems can be highly targeted and disruptive. At the vehicle level, researchers have exploited controller area network (CAN) bus vulnerabilities to remotely assume safety-critical functions such as steering, braking, and acceleration [8], while sensor-level adversarial manipulations, such as LiDAR spoofing and camera feed falsification, have triggered false object detection and lane boundary misinterpretation in autonomous driving systems [9, 10]. In positioning, navigation, and timing (PNT) systems, spoofing of global navigation satellite systems (GNSS) has been used to misdirect vehicles and disrupt fleet logistics [11, 12]. On the infrastructure side, attackers have infiltrated traffic signal control networks through unsecured communication channels, maliciously altering signal phase and timing plans to induce localized congestion and degrade throughput [13, 14]. At the network layer, falsified global positioning system (GPS) coordinates and Sybil attacks have fabricated congestion patterns, manipulating routing algorithms in navigation platforms such as Google Maps and Waze to generate adversary-preferred detours [15–17]. The strategic salience of such cyber threats is underscored by the identification of transportation as one of the four most ransomware-targeted U.S. critical infrastructure sectors in 2022, highlighting that cyber-induced disruptions pose direct risks to mobility, public safety, and national resilience [18].

In light of the rapidly growing cyber attack surfaces and the demonstrated cyber disruptions in CATS, cyber resilience has transitioned from a desirable capability to an operational imperative. Defined as the capacity to anticipate, withstand, recover from, and adapt to cyber incidents while preserving essential functions throughout the system lifecycle, even under successful attacks, cyber resilience transcends the preventive focus of conventional cybersecurity to encompass operational continuity and restoration [19–23]. This broader scope is crucial given the unknown,

zero-day, and strategically adaptive nature of smart adversarial threats, whose nonstationary and evolving patterns defy exhaustive enumeration or purely probabilistic, historically grounded risk modeling. It also differentiates cyber resilience from physical or natural hazard resilience [24, 25], where hazard patterns are comparatively stationary and can be addressed using probabilistic, risk-based approaches rooted in historical data. The need for cyber resilience in CATS is further motivated by the transportation sector's dual role as safety-critical and highly interconnected, where even transient disruptions can cascade across vehicles, infrastructure, and networked services. Addressing this challenge requires integrated strategies that combine proactive defense with real-time monitoring, rapid recovery, and adaptive response to sustain operational continuity under evolving cyber threats.

1.2. Objective and Scope

Building on the motivation established in Section 1.1, this survey positions itself as both a conceptual framework and a knowledge synthesis of the cyber resilience of CATS. Its primary objective is to provide a structured foundation for understanding how cyber threats emerge, how they compromise system functions, and how defenses can be designed, evaluated, and advanced. The scope of the survey encompasses three layers of inquiry: foundations, frontiers, and vision. The **foundations** cover conceptual constructs, attack-defense typologies, and resilience principles. The **frontiers** highlight methodological advances across theoretical approaches (optimization, game theory, and control theory), learning-based techniques (AI and adversarial machine learning), and emerging paradigms (quantum and post-quantum), with emphasis on their dual roles as both enablers of resilience and sources of new vulnerabilities. The **vision** extends beyond current practices to outline major research gaps and directions for future research, providing a roadmap for advancing cyber resilience theory, methods, and applications in CATS.

The survey is organized around three axes that together provide systematic coverage of the transportation cyber resilience landscape. The first axis relates to the **functional domain and cyber-physical components compromised**, which distinguishes between attacks on connectivity and autonomy as the two defining pillars of CATS, and on their enabling components of sensing, control, and networking. Connectivity encompasses V2X communication infrastructures that coordinate vehicles, roadside units, and networked services, but are also vulnerable to attacks such as eavesdropping, session hijacking, and denial-of-service. Autonomy encompasses perception, decision-making, and actuation processes within vehicles and infrastructure, which introduce attack surfaces such as sensor spoofing, data poisoning, model poisoning, model extraction, and backdoor attacks. At the cyber-physical component level, sensing systems (e.g., cameras, LiDAR, GNSS) can be compromised through spoofing, jamming, or perception overload, while control systems (e.g., vehicle controllers, roadside units, and traffic signal logic) are exposed to threats such as firmware tampering, command injection, or poisoning of AI models, and networking systems (e.g., in-vehicle buses, and V2X links) face threats such as message tampering and Sybil

attacks. Examining connectivity and autonomy in tandem with their enabling cyber-physical components highlights both their critical role in sustaining CATS operations and their susceptibility to exploitation, thereby grounding cyber resilience analysis in the concrete attack surfaces summarized in Section 2.

The second axis is the **operational scale**, which situates vulnerabilities and defenses across micro-, meso-, and macro-systems. At the micro-scale, vehicle-level functions such as in-vehicle networks, perception sensors, and local decision-making are prime targets for cyber attacks that compromise data integrity, availability, or control logic. At the meso-scale, corridor- and fleet-level systems such as traffic signals, cooperative adaptive cruise control, and vehicle platooning are exposed to both cyber disruptions (e.g., spoofing and denial-of-service) and cyber-physical disruptions that propagate through traffic operations. At the macro-scale, network-wide operations, intermodal coordination, and regional infrastructure management must withstand coordinated, large-scale threats capable of cascading across jurisdictions and transportation modes. Positioning cyber resilience across these nested scales highlights not only cascading risks but also the need for defense architectures that integrate across scales rather than remain siloed within them.

The third axis is the **threat-defense mapping**, which structures cyberattacks and defense approaches in systematic correspondence. Threats are organized along the confidentiality-integrity-availability (CIA) triad, which provides comprehensive coverage of attack surfaces without requiring exhaustive enumeration, an infeasible task given the prevalence of unknown and zero-day attacks. Confidentiality refers to preserving privacy and preventing unauthorized access, with threats such as eavesdropping and data exfiltration. Integrity refers to maintaining correctness and trustworthiness of information, with threats such as spoofing, data tampering, and poisoning of models or signals. Availability refers to ensuring continuous access to system functions, with threats such as denial-of-service. Defenses are aligned with resilience objectives that span robustness, detection, response, recovery, and adaptation, thereby capturing the full resilience lifecycle. At the same time, defenses can be further distinguished by their typologies, which include heuristic approaches that are lightweight but often brittle, certified methods that provide provable guarantees, probabilistic techniques that quantify uncertainty, and architectural measures that exploit system design (e.g., modular redundancy or fallback modes) to contain failures. Methods are explicitly treated as dual-use, with AI, optimization, and quantum or post-quantum techniques relevant both as defensive instruments and as attack enablers. This axis also incorporates evaluation and assurance mechanisms including digital twins, testbeds, cyber ranges, and benchmarking protocols, which are integral to verifying defense efficacy.

This three-axis framing provides a structured lens to capture transportation cyber resilience across scales, domains, and defense objectives, while aligning directly with the study's organization. Section 2 establishes the foundational concepts and taxonomies. Section 3 surveys methodological and assurance frontiers. Section 4 outlines a forward-looking research agenda. The

scope is therefore not merely descriptive but integrative, linking disparate lines of research into a coherent framework that can guide both academic inquiry and practical deployment in CATS.

1.3. Contributions

Existing surveys on cyber resilience and security in transportation have advanced the field but remain fragmented along several dimensions. Some specialize by the **functional domain of attack surface**, considering either connectivity or autonomy. Vehicular communications and V2X surveys focus on confidentiality and authentication in protocol-level security [26, 27], while reviews of autonomous vehicles emphasize attacks on perception, decision-making, and control [4, 28, 29]. Others focus on the **cyber-physical component compromised**. Surveys of in-vehicle intrusion detection focus primarily on networking components such as the CAN bus and related protocols [30], while studies of traffic signal control and traffic management emphasize control components at the intersection and corridor levels [13, 14, 31]. By contrast, comparatively fewer reviews explicitly examine the sensing components of vehicles, despite the growing literature on perception attacks such as sensor spoofing and data poisoning [6, 28]. Moreover, other surveys differentiate by the **operational scale of CATS**. Vehicle-level surveys investigate onboard networks and sensors [28, 30], corridor-level reviews consider cooperative adaptive cruise control, platooning, and traffic signals [13, 14], and network-level reviews address traffic management systems and coordinated threats [31]. Yet these operational scales are treated independently, without integrating micro-, meso-, and macro-systems into a unified resilience architecture. Finally, surveys differ in their treatment of the **threat-defense mapping**. Most surveys concentrate on specific attack surfaces, such as spoofing and tampering [4, 11, 28], data poisoning [6], or denial-of-service [26], while others emphasize narrow sets of defense goals or typologies, such as heuristic intrusion detection [30] or protocol-level cryptography [32], without integrating certified, probabilistic or uncertainty-aware, and architectural strategies.

Beyond transportation, there is a growing body of cyber resilience surveys in other domains. **Domain-tailored reviews** focus on sectors such as smart grids [33, 34] and healthcare cyber-physical systems [35], providing insights into domain-specific vulnerabilities and regulatory constraints but without addressing the connectivity-autonomy interplay or cascading traffic effects unique to CATS. Additionally, **cross-domain methodology surveys** emphasize methodological frameworks and techniques. In this line of research, comprehensive reviews of cyber resilience strategies across cyber-physical systems [21, 36, 37], cyber resilience through reinforcement learning [38], and surveys of resilient coordination or anomaly detection in cyber-physical systems [39] illustrate methods with broad applicability but lack transportation-specific operational contexts.

In view of the above gaps, the present survey makes three contributions. **First**, it develops a taxonomy that systematically integrates attack surfaces, functional domains, cyber-physical

components, defense objectives, and defense typologies across micro-, meso-, and macro-scales. Unlike prior surveys that treat functions, components, or scales in isolation, this taxonomy establishes systematic correspondence across the full CIA triad, resilience objectives (robustness, detection, response, recovery, adaptation), and defense typologies (heuristic, certified, probabilistic, architectural). **Second**, it synthesizes methodological and assurance frontiers by jointly considering theoretical approaches (optimization, game theory, and control theory), learning-based techniques (AI and adversarial machine learning), and emerging paradigms (quantum and post-quantum), together with assurance infrastructures such as digital twins, testbeds, cyber ranges, and benchmarking frameworks. While existing surveys typically emphasize either methods or infrastructures, this integration highlights their complementarity. **Third**, it articulates a forward-looking research agenda that identifies persistent gaps, including cross-layer resilience, unified trustworthiness, certified guarantees in safety-critical contexts, dual-use risks, lifecycle-aware resilience, standardized benchmarking, and socio-technical integration, thereby moving beyond descriptive taxonomies toward a strategic roadmap.

2. Foundations

The foundations of cyber resilience in CATS lie in the systematic characterization of how attacks emerge, how they propagate across transportation system layers, and how defenses can be organized to mitigate their impact. Establishing this foundation requires clear definitions of threat surfaces, resilience objectives, and defense strategies, together with an understanding of the architectures through which these elements interact. To this end, Section 2 introduces the conceptual axes that structure this survey, encompassing (1) the operational scales of transportation systems at the micro, meso, and macro levels, (2) the targeted functional domains of connectivity and autonomy together with their enabling components of sensing, networking, and control, and (3) the threat-defense mapping that aligns attack surfaces under the CIA triad with resilience objectives spanning robustness, detection, response, recovery, and adaptation. Within this framework, this section first details attack surfaces, then examines system functions and components most frequently targeted, and finally discusses how resilience objectives organize defense approaches. These foundational elements provide the taxonomy and concepts upon which methodological and assurance frontiers are assessed in Section 3.

2.1. Cyber Attack Surfaces

The attack surfaces in CATS are continuously expanding as connectivity deepens and autonomy advances. Unlike conventional transportation systems, CATS function as coupled cyber-physical ecosystems in which vulnerabilities emerge across vehicles, infrastructure, data pipelines, and communication networks. Exhaustively enumerating all cyber attacks is infeasible because even known attacks may vary in timing, frequency, and sophistication, while unknown zero-day exploits remain unpredictable. To establish systematic structure on this complexity, we organize

cyber attack surfaces along three complementary perspectives: 1) the **confidentiality, integrity, and availability (CIA) triad** [40, 41], 2) the distinction between **connectivity and autonomy functions** compromised, and 3) the targeted **cyber-physical components** that compose CATS.

CATS are multi-layered infrastructures. The physical layer includes infrastructure, vehicles, sensors, actuators, and controllers. The cyber layer encompasses embedded processors, operating systems, data analytics pipelines, and computational services at the edge or in the cloud. The communication layer enables interaction among on-board units, roadside devices, and traffic management centers. These layers interact through a closed-loop sense-process-decide-act cycle, spanning sensing and localization, perception and fusion, prediction and planning, and control and actuation. The interplay of connectivity and autonomy across these layers creates an expansive attack surface. Confidentiality attacks compromise mobility data, communication records, or user credentials [42]. Integrity attacks manipulate data streams, learning models, or control commands through methods such as sensor spoofing, data poisoning, or controller tampering [6]. Availability attacks disrupt system continuity through denial-of-service (DoS) or distributed denial-of-service (DDoS) strategies that impair vehicle and infrastructure coordination [43]. Situating each threat along the connectivity dimension (communication protocols and data flows) and the autonomy dimension (inference, decision-making, and control logic), as well as identifying the targeted cyber-physical components (sensors, controllers, or networks), provides a comprehensive and streamlined framework for analyzing cyber attack surfaces in CATS.

2.1.1. Confidentiality Attacks

Confidentiality attacks in CATS concern the unauthorized access to or disclosure of sensitive information, such as vehicle trajectories, traffic control logic, and traffic system states (e.g., traffic flow). Breaches of confidentiality compromise privacy by exposing personally identifiable information, undermine security by revealing exploitable system states, and degrade operational performance by enabling informed integrity and availability attack planning. As summarized in Table 1, confidentiality attacks may exploit vulnerabilities originated from the connectivity or autonomy functions of CATS and target three main cyber-physical components, including sensors, controllers, and networks. Each attack surface involves distinct threats with implications at micro (vehicle-level), meso (intersection or corridor), and macro (network-level) scales. The following sub-sections expand on each attack listed in Table 1.

2.1.1.1. Connectivity-Origin Confidentiality Attacks

Sensor-targeted attacks. One prominent confidentiality attack is radio-frequency (RF) *eavesdropping*, in which adversaries passively intercept dedicated short-range communications (DSRC) or cellular-vehicle-to-everything (C-V2X) messages to capture basic safety messages (BSMs). At the micro scale, intercepted messages may reveal a vehicle's precise position and speed, enabling tracking of individual drivers. At the meso scale, repeated interception near

intersections could reveal traffic signal phase and timing (SPaT) data or vehicle platoon behavior. At the macro scale, network-wide interception exposes mobility patterns of entire fleets. Empirical demonstrations confirm that BSMs, even pseudonymized, leak trajectory data [42, 44]. Another notorious sensor-targeted threat is *traffic analysis*, where attackers infer mobility or commuting patterns by exploiting beaconing frequency or pseudonym changes. For instance, attackers stationed along arterial roads can correlate pseudonym change intervals with recurring vehicle appearances, enabling partial reconstruction of origin-destination (OD) flows. Simulation and field studies further demonstrate that such pseudonym-linking attacks can compromise user privacy even in dense urban networks [45]. More recent work shows that large-scale traffic analysis, when combined with machine learning classifiers, can deanonymize travel corridors and reveal commuting patterns despite pseudonym-switching strategies [46].

Table 1. Confidentiality attacks in CATS

Attack surface		**Specific attack examples**	
CATS function	**cyber-physical component**	**Attack name**	**Attack description**
Connectivity	Sensors	RF eavesdropping	Passive interception of DSRC/C-V2X signals to capture basic safety messages
		Traffic analysis	Infers mobility patterns from beacon frequency or pseudonym changes
	Controllers	API misconfiguration	Poorly secured RSUs leak probe data or control logic
		Debug backdoors	Exposed interfaces reveal traffic signal scheduling or sensor feeds
	Networks	Session hijacking	Intruder takes over active V2X sessions
		Downgrade attack	Forces fallback to weaker encryption, enabling sniffing
Autonomy	Sensors	Data leakage	Logs or calibration files reveal LiDAR/video data or passenger patterns
	Controllers	Model inversion	Reconstructs sensitive training data
		Membership inference	Identifies if data were included in training
		Model extraction	Clones trajectory models via queries
	Networks	Multi-tenant isolation failures	Edge/cloud leaks between tenants
		Cloud data leakage	Misconfigurations expose training or routing data

Controller-targeted attacks. Confidentiality risks extend to controllers such as roadside units and traffic signal controllers. One critical vector is application programming interface *(API) misconfiguration*, where poorly secured endpoints expose sensitive operational data [47]. For example, improperly authenticated roadside unit APIs may leak probe vehicle datasets, disclosing trajectories of connected vehicles in real time [48]. Another related confidentiality breach arises

from *debug backdoors*, which are diagnostic interfaces unintentionally left open after system deployment. Debug backdoors allow adversaries to access detector feeds, internal logs, or incident management protocols, creating a persistent leakage channel [49]. At the macro scale, such vulnerabilities in traffic management centers can expose large-scale operational strategies, including regional rerouting policies during emergencies, undermining trust in centralized connected-traffic control.

Network-targeted attacks. At the communication layer, confidentiality is threatened by *session hijacking*, in which adversaries intrude into active V2X sessions between vehicles and RSUs. Once a session is hijacked, attackers can intercept routing instructions, vehicle identifiers, or platoon membership information [50]. At the micro scale, this enables monitoring of individual vehicle trips. At the meso scale, it exposes fleet-level routing preferences. At the macro scale, hijacked sessions aggregate into a revealing picture of regional public transit or ride-hailing demand. Another potent risk is the *downgrade attack*, where adversaries force communication protocols to revert to weaker encryption standards, thereby enabling subsequent interception [51]. These attacks suggest that confidentiality breaches at the network layer not only compromise individual privacy but also leak system-level mobility intelligence, which adversaries or competitors can exploit.

2.1.1.2. Autonomy-Origin Confidentiality Attacks

Sensor-targeted attacks. A major confidentiality risk at the perception layer of autonomous transportation systems is *data leakage*, in which raw or auxiliary sensor outputs inadvertently expose sensitive information. At the micro scale, leaked LiDAR point clouds or camera calibration logs can disclose pedestrian movement patterns or individual vehicle trajectories[52]. At the meso scale, exposed fleet-level video feeds can enable re-identification attacks on drivers or pedestrians through face and gait recognition. At the macro scale, aggregated LiDAR, radar, or camera datasets leaked from autonomous vehicle fleets may reveal regional commuting flows and population-level traffic densities, providing attackers or competitors with sensitive mobility intelligence.

Controller-targeted attacks. At the autonomy control layer, confidentiality threats are driven by machine learning-specific attack vectors. *Model inversion* attacks reconstruct sensitive elements of training data by querying trajectory planning or perception models, exposing rare crash trajectories or proprietary driver reaction traces [53, 54]. *Membership inference* attacks determine whether a particular data record, such as an accident scenario or edge-case trajectory, was included in the model's training set, threatening the privacy of study participants and the integrity of safety datasets [55]. *Model extraction* attacks allow adversaries to clone proprietary control policies (e.g., trajectory planning or platoon stability models) by systematically probing the outputs of deployed application programming interfaces (APIs), effectively stealing intellectual property [56]. At the micro scale, these attacks may expose an individual AV's car-following or lane-change model. At the meso scale, they may compromise fleet-level routing strategies. Whereas, at the macro scale,

they can lead to the leakage of proprietary urban traffic optimization policies.

Network-targeted attacks. The supporting cloud and edge infrastructure for autonomy is subject to confidentiality breaches such as multi-tenant isolation failures and cloud data leakage. In *multi-tenant isolation failures*, improper isolation on edge servers or roadside units allows data from one tenant (e.g., a fleet operator) to be accessed by another, exposing trajectory logs, routing preferences, or passenger demand distributions [57, 58]. As for *cloud data leakage* attacks, misconfigurations or insecure APIs expose sensitive fleet-level datasets, such as dispatch plans, rider histories, or traffic demand matrices [59]. At the micro scale, this could reveal an individual passenger's trip history. At the meso scale, leaked roadside unit logs may disclose fleet allocation strategies. At the macro scale, exposure of mobility-as-a-service (MaaS) or autonomous vehicle dispatch datasets may reveal population-scale passenger flows, which can be exploited by both attackers and competitors.

2.1.2. Integrity Attacks

Integrity attacks aim to corrupt or manipulate data, models, or control logic so that CATS make decisions based on incorrect information. Unlike confidentiality attacks that focus on unauthorized access, integrity attacks seek to directly change system behavior by injecting false information, tampering with models, or manipulating communications). Table 2 summarizes the main classes of integrity attacks, grouped by their origin (connectivity and autonomy) and targeted cyber-physical component (sensing, control, or networks).

Table 2. Integrity attacks in CATS

Attack surface		**Specific attack examples**	
CATS function	**cyber-physical component**	**Attack name**	**Attack description**
Connectivity	Sensors	False data injection	Malicious alteration of sensor data streams (e.g., loop detectors, GPS)
		Replay attack	Legitimate sensor messages are recorded and re-sent later to mislead operations
	Controllers	Command injection	Insertion of malicious commands into traffic controllers
		Firmware tampering	Modification of controller firmware to persistently corrupt operations
	Networks	Message tampering	Alteration of message payloads during transit
		Man-in-the-middle	Intercepting and modifying communications between vehicles and infrastructure
Autonomy	Sensors	Sensor spoofing	Injection of corrupted sensor inputs (e.g., GNSS spoofing)
		Perception overload	Overwhelming perception systems with excessive or conflicting data

Attack surface		Specific attack examples	
CATS function	**cyber-physical component**	**Attack name**	**Attack description**
	Controllers	Model poisoning	Compromising AI model training or updates to bias decisions
		Backdoor attack	Hidden triggers embedded in AI models to cause targeted misbehavior
	Networks	Sybil attack	Fake identities created to distort cooperative systems
		Consensus manipulation	Adversarial biasing of distributed or federated decision-making

2.1.2.1. Connectivity-Origin Integrity Attacks

Sensor-targeted attacks. Integrity threats that originate at the sensing layer of connected systems primarily manifest as false data injection and replay attacks. In *false data injection*, adversaries deliberately alter measurement streams such as loop detector counts, GPS positions, or probe vehicle data with the goal of misleading downstream estimation and control applications. At the micro scale, manipulated detector readings may cause ramp meters or adaptive signals to allocate green times inefficiently, creating localized congestion. At the meso scale, corrupted probe vehicle data can bias arterial travel time estimation, leading to mistimed coordination across signalized corridors. At the macro scale, falsified inputs to origin-destination estimation or dynamic traffic assignment models may cause underestimation or overestimation of regional demand, producing flawed system-wide routing or planning decisions. Studies confirm that even modest falsification rates can trigger substantial performance deterioration in model-based and data-driven control [6, 60]. Closely related are *replay attacks*, where adversaries capture valid sensor data and retransmit them at later times. At the micro level, replaying outdated pedestrian detection messages can trick traffic signals into activating walk phases unnecessarily. At the meso level, replaying prior video or probe data can produce false incident reports or phantom congestion. At the macro level, re-injected floating car data streams can suggest congestion at places where none exists, distorting both real-time traveler information and long-term network management [61, 62]. Both false data injection and replay attacks thus compromise the integrity of the traffic sensing backbone, undermining the reliability of connectivity-based control.

Controller-targeted attacks. Controllers that actuate connected transportation systems are highly susceptible to command injection and firmware tampering. In *command injection* attacks, adversaries compromise control channels to insert malicious instructions. At the micro scale, such attacks could alter adaptive traffic signal logic (e.g., forcing unsafe signal phase sequences), while at the meso scale they can disrupt coordination across signalized arterials and they can corrupt traffic management centers at the macro scale, propagating false signal phase plans or routing recommendations across entire networks [63–65]. *Firmware tampering* represents a more

persistent form of attack, wherein adversaries modify firmware within roadside units, traffic signal controllers, or connected infrastructure to systematically corrupt operations [66–68]. These manipulations can miscommunicate with connected vehicles, generate biased V2X safety alerts, or sustain long-term denial of reliable control, making firmware integrity a cornerstone of secure controller deployment in connected transportation systems.

Network-targeted attacks. At the communication network layer, message tampering and man-in-the-middle (MitM) attacks represent major integrity threats. *Message tampering* occurs when adversaries alter communication payloads during transmission, resulting in false routing guidance, corrupted traffic density estimates, or invalid basic safety messages. At the micro scale, this can generate incorrect collision warnings between nearby vehicles. At the meso scale, tampered cooperative awareness messages (CAMs) can distort corridor traffic state estimation. At the macro scale, corrupted floating car or connected vehicle messages can bias system-wide traveler information platforms [69, 70]. *Man-in-the-middle attacks* pose an even greater systemic risk by enabling adversaries to intercept and selectively modify messages exchanged between vehicles and infrastructure [71, 72]. Such attacks can alter congestion reports provided to traffic management centers, leading to distorted network-wide routing and resource allocation. By compromising the communication integrity of connected networks, message tampering and MitM attacks destabilize both local safety-critical services and large-scale mobility management.

2.1.2.2. Autonomy-Origin Integrity Attacks

Sensor-targeted attacks. Autonomy-origin integrity threats on sensing systems are among the most direct forms of attack on autonomous transportation systems. *Sensor spoofing* involves directly forging false signals to mislead perception modules. GNSS spoofing, for example, manipulates satellite navigation by transmitting counterfeit signals that override authentic ones, thereby causing an autonomous vehicle to mis-localize its position [11, 73, 74]. Such attacks have been demonstrated in both simulation and field experiments [75], with the potential to reroute single vehicles, destabilize platoons [76], or disrupt large-scale network flows [77]. *Perception overload* attacks further undermine sensor integrity by overwhelming perception systems with adversarial inputs. Examples include adversarial stop signs that cause misclassification in deep vision models [78], laser injection that creates phantom obstacles in LiDAR point clouds [79, 80], and flooding attacks that degrade radar/LiDAR detection accuracy under high-noise conditions [81]. At micro scales, these attacks compromise single-vehicle detection. At meso scales, they destabilize platoons or cooperative maneuvers, while they distort network-level routing and safety-critical perception at macro scales.

Controller-targeted attacks. Integrity threats also target the decision-making controllers of autonomous transportation systems. *Model poisoning* attacks compromise learning pipelines by inserting malicious updates into training or federated learning rounds, shifting model parameters to induce unsafe behaviors. Such poisoning can degrade reinforcement learning for car-following,

bias routing policies, or systematically redirect large-scale planning [82–84]. *Backdoor attacks* are a stealthier variant, embedding hidden triggers during training so that models behave normally under standard conditions but produce unsafe actions when exposed to specific inputs. For instance, a trigger pattern on a roadside sign can cause an autonomous vehicle to brake or swerve unexpectedly [85, 86]. In federated settings, poisoning and backdoor attacks can bypass robust aggregation methods and persist across global model updates [87]. These controller-level threats are especially critical because they compromise the autonomy core, directly altering autonomous decision policies.

Network-targeted attacks. Beyond sensors and controllers, integrity attacks extend to collective autonomy mechanisms, where vehicles and infrastructure rely on distributed consensus. *Sybil attacks* involve adversaries creating multiple fake identities, injecting false data to bias cooperative decisions. At the micro scale, a single attacker may appear as a phantom platoon [88]. At the meso scale, cooperative adaptive cruise control synchronization can be disrupted [89]. At the macro scale, distributed routing algorithms may be skewed toward attacker-preferred paths [90]. Another critical integrity threat is *consensus manipulation*, in which adversaries bias distributed protocols such as federated learning aggregation or decentralized traffic state estimation. Recent work shows that even Byzantine-robust consensus protocols can be manipulated by carefully crafted adversarial updates, leading to global deviation from optimal equilibria [91, 92]. Such network-level integrity attacks threaten the scalability and trustworthiness of collaborative autonomy frameworks, particularly in CATS.

2.1.3. Availability Attacks

Availability attacks aim to degrade or completely disrupt the operational continuity of CATS by overwhelming system resources or obstructing communication. Unlike confidentiality and integrity breaches, availability attacks aim to deny, degrade, or delay service, such as disrupting traffic signal operations, blocking basic safety messages, or overloading vehicular computing units. These disruptions are particularly dangerous in transportation as they can create cascading safety-critical failures. A local outage at a single road intersection may ripple into regional traffic congestion, or a delayed decision by one autonomous vehicle may propagate into multi-vehicle accidents. By undermining the timeliness of information flow and the ability to act, availability attacks strike at the real-time decision-making foundation of both connectivity and autonomy in CATS. Availability attacks are primarily realized through *denial-of-service (DoS)* mechanisms and their variants, as outlined below. These attacks can originate either from the connectivity layer (targeting communication networks) or from the autonomy layer (targeting computational resources and control modules).

Table 3. Availability attacks in CATS

Attack surface		Specific attack examples	
CATS function	**cyber-physical component**	**Attack name**	**Attack description**
Connectivity	Sensors	Jamming	GNSS jamming, DSRC or C-V2X interference
	Networks	DoS, DDoS, flooding	Traffic flooding against VANETs and RSUs
Autonomy	Controllers	Resource exhaustion DoS	Overloading autonomous vehicle perception and planning GPU with adversarial inputs

2.1.3.1. Connectivity-Origin Availability Attacks

Sensor-targeted attacks. *Jamming attacks* are the canonical availability threats against sensors. By transmitting strong signals on the same frequencies used by GNSS, DSRC, or C-V2X, an attacker can block vehicles or roadside units from receiving valid data. For GNSS, even small, inexpensive jammers can disturb satellite signals, causing large errors in vehicle positioning and timing that ripple through systems depending on location accuracy [93]. Large-scale monitoring has shown that such interference events occur regularly in practice and can persist in specific areas, making them a serious risk for traffic operations that depend on GPS or other GNSS services [94]. For V2X communications, jamming can reduce the success rate of safety messages. This can be done by simply transmitting noise, or more subtly by targeting the rules used for channel access in C-V2X, which prevents legitimate vehicles from successfully sending their messages [95, 96]. At the micro level, this disrupts situational awareness for individual vehicles. At the meso level, repeated interference near intersections can block SPaT information or disturb vehicle platoons. At the macro level, corridor-wide interference can cause connectivity losses that translate into regional traffic flow disruptions.

Network-targeted attacks. At the network layer, availability attacks appear as *denial-of-service (DoS)* and its distributed variant *(DDoS)*. In these attacks, adversaries overwhelm roadside units, cloud servers, or vehicular backbone networks with excessive traffic, leaving no resources for legitimate messages. *Flooding attacks* are a common case, where attackers inject a high number of unnecessary messages into vehicular networks, consuming bandwidth and RSU processing capacity. This prevents timely delivery of basic safety messages or other control information [97, 98]. Recent work has developed real datasets for vehicular flooding scenarios, making it possible to test detection methods in realistic settings [99]. Countermeasures include simple rate limiting at RSUs, congestion-control policies at the medium access control (MAC) layer, and anomaly detectors that look for abnormal traffic volumes or timing patterns. Modern detection systems show promise for real-time recognition of flooding and DDoS attacks with low false-alarm rates [97, 100].

2.1.3.2. Autonomy-Origin Availability Attacks

Controller-targeted attacks. Within vehicles or traffic management centers, availability failures can also come from *resource exhaustion attacks*, where computational units such as CPUs, GPUs, or controllers are overloaded by abnormal inputs. In the vehicle perception and planning modules, crafted inputs can make algorithms take longer than expected to process, causing delays or system stalls without directly corrupting the data [101]. For example, an attacker can feed inputs that force the object detection system to run very slowly, delaying downstream modules for braking or steering [102]. This type of attack may not produce incorrect decisions, but it disrupts the timing of decision-making, which is critical for safety. At the controller and middleware layers, attackers may also flood vehicles with control-plane or network messages that overload communication queues and delay sensor fusion and actuation [103]. Defensive measures include setting processing limits for each module, using algorithms that can return a "best effort" result quickly under heavy load, and monitoring queues for abnormal traffic patterns. Despite this, a major open problem is how to provide guaranteed timing performance in autonomous driving systems when they are under attack, which is an issue closely tied to certification in safety-critical transportation.

2.2. Cyber Defense Objectives and Strategies

Cyber defense in CATS should be designed for continuity of system function under stress rather than prevention alone. In practice, this means aligning defenses with a multi-stage resilience characterization that spans preparation and robustness before an incident, graceful performance under bounded disruption, fast and reliable detection when the system deviates from nominal behavior, safe online containment when compromises occur, efficient restoration of services to acceptable levels, and adaptive learning that reduces future exposure. This systems view is consistent with cyber resilience engineering that emphasizes anticipating, withstanding, recovering, and adapting across the lifecycle, and doing so in ways that respect the real-time, safety-critical, and networked nature of transportation operations [104–106]. The remainder of this section formalizes the objectives that such defenses should meet and subsequently analyzes defense strategy typologies and deployment architectures that can deliver those objectives at the micro, meso, and macro scales of transportation systems.

2.2.1. Defense and Resilience Objectives

We adopt a multi-stage characterization of cyber resilience that is tailored to transportation cyber-physical operations and grounded in established resilience literature [104–106]. **Robustness** is the pre-incident and during-incident capability to maintain acceptable performance under bounded disturbances, uncertainty, or attack actions. In road transportation, robustness is reflected in platooning or cooperative adaptive cruise control that preserves string stability despite bounded communication delay and packet loss, thereby attenuating, rather than amplifying, disturbances along a vehicle string [107–109]. Robustness is specified and engineered *a priori* and measured

online through safety margins and performance envelopes. It is not a guarantee against every threat but a commitment to degrade slowly and predictably when perturbations remain within design bounds [107, 110].

Detection is the timely and reliable identification of departures from nominal system behavior caused by faults, misuse, or adversary actions. In CATS, detection spans in-vehicle intrusion detection for controller area network (CAN) traffic, anomaly and misuse detection on V2X links, and integrity monitors for PNT. The related literature shows the feasibility and limits of signal-, protocol-, and learning-based detectors for in-vehicle networks, including coverage gaps introduced by stealthy, low-rate attacks and concept drift in real traffic [111–113]. In the PNT domain, spoofing can be detected by signal-quality tests, multi-antenna spatial discrimination, and consistency checks against inertial and map priors, but adversaries that mimic legitimate signals can still pass simplistic monitors, motivating multi-sensor cross-validation and decision-level fusion [114]. Across meso- and macro-scales, detection includes monitoring of traffic controller setpoints and of network-wide traffic flows to flag impossible traffic states or policy-inconsistent traffic signal timing plans [115, 116].

Response is the execution of safe, bounded interventions while the system is compromised, such that hazards remain controlled and mission-critical services continue. Examples include switching a vulnerable controller to a failsafe control law that trades throughput for safety, forcing a vehicle to a minimum-risk condition when localization confidence collapses, or isolating a corridor's traffic signal control to time-of-day plans when central coordination is suspected compromised. Runtime assurance frameworks from safety-critical CATS, such as control-barrier-function safety filters, formalize this notion of online containment and have been extended to autonomy settings where complete pre-deployment proofs are infeasible [117–120].

Recovery is the efficient restoration of nominal or near-nominal service levels once the immediate hazard is contained. In transportation operations, this includes re-synchronizing traffic signals after a controller rollback, re-establishing secure keys and routes on V2X, and restoring degraded perception pipelines once trusted models are reloaded. Recovery metrics combine time-to-restore and residual performance during restoration [121–125]. Lastly, **adaptation** refers to the systematic learning and hardening that reduces future exposure through updating detection thresholds after false-negative analysis, refining fallback policies to improve service under degraded sensing, and redesigning trust and management procedures after incident [126, 127]. Cyber resilience, in this sense, is not a single mechanism but a closed-loop, multi-stage characterization of robustness, detection, response, recovery, and adaptation that composes across micro vehicle behavior, meso corridor control, and macro network management.

2.2.2. Defense strategy typologies and deployment architectures

Cyber defense strategies can be broadly organized along two complementary directions: (1)

methodological guarantees (or lack thereof), encompassing heuristic and empirical methods, statistical and probabilistic methods, and certified and provable methods; and 2) deployment architecture, such as modular and end-to-end pipelines as well as centralized, decentralized, distributed, or federated settings. The choice along each direction has concrete implications for fault isolation, attack containment, latency, scalability, and certifiability at each operational scale in CATS.

Heuristic and empirical defense strategies rely on specification conformance, signatures, rule-based checks, and learned anomaly profiles. At the micro scale in CATS, these include protocol sanity checks and payload plausibility tests on controller area network (CAN) [128], timing-consistency checks on sensor streams [129, 130], and traffic-shaping on V2X interfaces [131, 132]. At meso- and macro-scales, they include policy conformance checks on traffic signal timing plans [133, 134] and integrity monitors on center-to-field messages, i.e., communication between a traffic management center (the "center") and field devices such as traffic signal controllers and roadside units (the "field") [31, 135]. Such methods are lightweight and practical, but they are susceptible to evasion by adaptive adversaries and require continual re-tuning as platforms, protocols, and traffic evolve [136]. Their advantage is speed and coverage for known failure and misuse modes, whereas their limitation is the lack of guarantees outside the envelope captured by rules and training data.

Statistical and probabilistic defense strategies make uncertainty explicit and seek to quantify confidence in system state, detection decisions, and control actions. Examples include residual-based detectors with false-alarm guarantees [137], Bayesian filters that fuse GNSS to test for PNT anomalies [138], and traffic state estimators that flag infeasible traffic flows [139]. At the control layer, stochastic model predictive control [140] and chance-constrained optimization [141] trade performance against tail risk, thereby expressing robustness requirements as probability-of-violation bounds. At the micro scale, this helps quantify when to invoke minimum-risk vehicle maneuvers. At the meso scale, it guides when to cut over to pre-timed corridor signal control plans. At the macro level, it supports admission control and rerouting under suspected data poisoning. Overall, these methods generalize better than pure heuristics, but they still depend on modeling assumptions about noise, dependence, and attack surfaces that adversaries can target.

Certified and provable defense strategies aim for formal guarantees. In autonomy, barrier-certificate synthesis can prove that closed-loop vehicle trajectories remain within safety sets despite bounded faults or disturbances and can be evaluated online for runtime shielding [142, 143]. In networked transportation, design for string stability and bounded delay can be proved for cooperative vehicle control under realistic communication assumptions, thereby ensuring disturbance attenuation across platoons and suppressing amplification that attackers could exploit [108, 144]. For AI components, formal verification tools for neural networks can certify local robustness to input perturbations in perception or decision modules, which complements but does

not replace system-level assurance [145–148]. Certified defenses are attractive for safety-critical functions in CATS, yet they typically incur higher computational cost, require conservative modeling, and may need runtime assurance wrappers to remain effective under model error or distribution shift [149, 150].

The **deployment architecture** shapes how the aforementioned defense methods compose at scale. Modular pipelines (i.e., sensing, perception, prediction, planning, control) facilitate fault isolation and targeted fallback strategies. They are amenable to component-level verification and to runtime guards placed at well-defined interfaces [151–153]. By contrast, end-to-end pipelines reduce computational overhead but complicate certification and containment, and therefore often require external monitors and safety filters (e.g., [154]). With respect to organizational topology, centralized architectures (e.g., corridor or network control from a transportation management center) simplify global situational awareness and coordinated response but create single points of failure. Decentralized or distributed architectures localize autonomy and control, which improves containment and reduces latency at the cost of more complex synchronization and potential performance loss in global objectives. In cooperative driving scenarios, for instance, theoretical and empirical results show how communication topology and delay bounds interact with closed-loop stability, illustrating the containment and scalability advantages of designs that preserve string stability under realistic network constraints [144, 155]. Finally, federated or hierarchical data and model management can reduce privacy and confidentiality risk by keeping raw data local while exchanging aggregates or model updates. However, they introduce their own trust and integrity challenges that must be controlled by robust aggregation and audit mechanisms [156, 157].

Across micro, meso, and macro scales of CATS, it is the alignment of defense objective, method, and architecture (e.g., a certified runtime safety filter wrapped around a learned planner in vehicles, policy-conformance and statistical monitors in the field, and conservative fallback in the transportation management center) that yields transportation cyber resilience.

3. Frontiers

While the foundations (Section 2) establish what is being defended and how cyber resilience can be defined, the frontiers address how cyber resilience is operationalized through methodological advances. Section 3 surveys the principal analytical and computational approaches that underpin state-of-the-art defenses, with emphasis on both their promise and limitations. These include 1) analytical and theoretical methods, such as optimization, control, and game theory, which provide structure and, in some cases, formal guarantees, 2) learning and computational methods such as adversarial machine learning, anomaly detection, and reinforcement learning that offer adaptivity but often lack rigorous assurance, and 3) emerging paradigms such as quantum and post-quantum approaches that are beginning to reshape the cyber resilience landscape. Complementing these methods are assurance infrastructures, including digital twins, cyber ranges,

and benchmarking frameworks, which enable systematic evaluation and validation.

While the foundations in Section 2 define what is at stake and how cyber resilience can be conceptualized, the frontiers turn to how resilience is enacted through methodological innovation. Section 3 surveys the principal analytical and computational approaches that drive state-of-the-art defenses, highlighting both their capabilities and their inherent limitations. These encompass: (1) analytical and theoretical frameworks, including optimization, game theory, uncertainty frameworks, and control theory, which embed structure and, in some cases, provable guarantees; (2) learning-based and computational methods, such as adversarial machine learning and reinforcement learning, that enable adaptivity but often lack rigorous assurance; and (3) emerging paradigms, such as quantum and post-quantum approaches, which are beginning to redefine the landscape of cyber resilience. Importantly, these methodological frontiers are complemented by assurance infrastructures, including digital twins, cyber ranges, and benchmarking frameworks, which provide the experimental settings needed to test, validate, and compare resilience strategies under realistic conditions. However, as will be shown, the same innovations that advance resilience simultaneously open new avenues for adversaries, underscoring the dual-use nature of methodological progress.

3.1. Methodological Frontiers

Methodological innovations form the intellectual backbone of cyber resilient transportation. To tackle the escalating sophistication of cyber-physical threats, researchers have advanced diverse methodological frameworks that integrate rigorous theory, adaptive computation, and next-generation technologies. These frontiers can be organized into three complementary categories. First, theoretical and analytical frameworks, which ground cyber resilience in operations research and control theory. Second, AI-centered frameworks, which span using AI as a defensive tool (i.e., AI for security) as well as guarding learning systems themselves from adversarial exploitation (i.e., security of AI). Finally, emerging paradigms, particularly including quantum information science and engineering, which is set to redefine the boundaries of secure communication, inference, and optimization. Each category addresses different dimensions of the CIA triad that underpins cyber resilience. Despite these methodological innovations to enhance cyber resilience, a paradox persists. The very techniques that offer cyber resilience often create new attack surfaces, as adversaries exploit the same methodological advances to design stealthier, more adaptive, and more scalable attacks.

3.1.1. Theoretical and Analytical Frameworks

Theoretical and analytical frameworks provide the foundational layer for designing cyber resilient transportation systems. Unlike heuristic defenses discussed in Section 2.2.2, these methods can offer provable guarantees and interpretability, enabling systematic reasoning about adversarial behavior in CATS. Their value lies in embedding rigor and structure into resilience

strategies, spanning from optimization formulations to dynamic control. Importantly, these frameworks can address the three types of cyber attack surfaces (i.e., confidentiality, integrity, and availability) by quantifying risks of data breaches, mitigating falsified or manipulated sensor inputs, and ensuring continuity of operations under disruption. Broadly, these methods can be grouped into four categories: 1) optimization approaches, 2) game-theoretic frameworks, 3) probabilistic and uncertainty frameworks, and 4) control-theoretic approaches.

Optimization approaches. Optimization provides a structured means of designing resilient decision rules in transportation systems. *Robust optimization* can protect against worst-case realizations of cyber attacks by bounding uncertainty sets. This is particularly relevant for maintaining availability, such as ensuring routing or scheduling decisions remain feasible under DoS disruptions [158, 159]. *Distributionally robust optimization (DRO)* extends this by hedging against adversarially shifted probability distributions, which is useful for countering integrity attacks such as falsified travel time reports or sensor spoofing [160]. *Chance-constrained optimization* further balances resilience with efficiency, controlling the probability of confidentiality or availability failures under stochastic disruptions [161]. Example applications of optimization approaches in transportation include network design under interdiction [162], traffic signal control under uncertainty [163], and infrastructure hardening for multimodal systems [164]. However, these methods are only as resilient as their assumptions. That is, adversaries with knowledge of the defender's uncertainty sets can engineer stealthy disruptions that bypass optimization safeguards. Thus, while optimization enhances resilience, it simultaneously creates exploitable attack surfaces defined by modeling assumptions.

Game-theoretic approaches. Game theory explicitly models the strategic interplay between defenders and adversaries, providing insight into adversarial intent and adaptive responses. In *Stackelberg security games*, defenders pre-commit to strategies anticipating adversarial responses. This is well-suited for preserving integrity, such as mitigating false data injection attacks where adversaries exploit sensor networks [165, 166]. *Bayesian games* capture incomplete information, where defenders face uncertainty about attacker capabilities, directly addressing confidentiality concerns by incorporating hidden attacker types [167]. *Repeated and stochastic games* can further capture persistence, deception, and adaptation over time, central to maintaining availability in critical infrastructures targeted by long-term adversarial campaigns [168, 169]. Example applications include transportation network interdiction [170], defense of connected vehicle perception [171], and modeling cyber risks in infrastructure systems [172]. Despite these, equilibria themselves can be double-edged in the sense that once equilibrium strategies are public or learned, attackers may adapt to exploit them. This illustrates the paradoxical dual role of game-theoretic methods as both a resilience enabler and a map of exploitable vulnerabilities.

Probabilistic and uncertainty frameworks. Probabilistic frameworks embed uncertainty quantification into cyber resilience planning. *Markov decision processes (MDPs)* and their robust

variants address availability attacks by guaranteeing continuity of control policies under uncertain transitions caused by cyber disruptions [173]. *Bayesian risk analysis* quantifies uncertainty in attacker intentions and outcomes, directly relating to confidentiality (e.g., estimating likelihood of hidden surveillance) and integrity (e.g., bounding the probability of undetected falsified data) [174]. *Stochastic programming* integrates uncertainty into optimization, balancing cost and resilience by preparing against plausible scenarios of cyber disruption [175]. Example applications in transportation systems comprise resilience assessment of critical infrastructure [176], cyber risk quantification in vehicular networks [177], and uncertainty-aware routing under adversarial conditions [178]. Despite their advantages, probabilistic defenses are inherently limited by the accuracy of prior models, i.e., adversaries with superior information may manipulate assumptions, rendering posterior-based defenses blind. This epistemic fragility underscores the need for careful integration of probabilistic methods with real-time data-driven monitoring.

Control-theoretic approaches. Control-theoretic methods engage directly with system dynamics, ensuring stability and observability under cyber interference. *Robust and adaptive control* safeguard availability by stabilizing traffic flow even under packet drops or sensor failures [179]. Resilient *state estimation* and *observer-based anomaly detection* can defend integrity by identifying falsified sensor signals inconsistent with physical dynamics [180]. *Control watermarking* and authentication-based feedback loops protect confidentiality, preventing adversaries from reverse-engineering or predicting system responses [181]. Example applications to transportation systems include secure traffic signal control [182], vehicle platoon stability under adversarial communication [183], and resilient monitoring of networked infrastructures [184]. Analogous to other theoretical and analytical methods discussed above, informed adversaries can align their attacks with system dynamics to create stealthy false data injections that evade detection. Therefore, even control theory, long regarded as a rigorous framework in cyber-physical systems, paradoxically defines the limits of stealth for attackers with structural knowledge.

3.1.2. Learning and Computational Frameworks

AI has emerged as a central methodological frontier in transportation cybersecurity because of its ability to model complex spatiotemporal patterns, adapt to evolving adversaries, and infer hidden attack signatures from large-scale data. Its contributions can be understood along two intertwined dimensions: 1) AI for security, where AI methods and algorithms directly enable detection, response, and resilience, and 2) security of AI, in which the learning systems themselves become attack surfaces susceptible to adversarial exploitation. This dual framing is essential for capturing the paradox of AI in CATS, i.e., the same AI algorithms that enhance cyber resilience can be weaponized against it. Four major AI paradigms, encompassing supervised learning, unsupervised learning, reinforcement learning, and generative AI, define the current landscape of opportunities and risks.

AI for Security. *Supervised learning* methods leverage labeled data to identify attack

patterns or abnormal conditions. In transportation systems, they have been used for intrusion detection systems, anomaly classification in vehicular networks, and malware detection in intelligent infrastructure [185–187]. Against the CIA triad, supervised classifiers primarily strengthen integrity by flagging falsified sensor data, and confidentiality by detecting packet sniffing or unauthorized access attempts. However, their reliance on labeled data makes them vulnerable to concept drift, where adversaries deliberately introduce new attack variants not represented in training sets. This limitation reflects both their defensive utility and susceptibility to exploitation as adversaries can poison labeled datasets, leading to corrupted models that misclassify attacks [188, 189].

Unsupervised learning, such as clustering, autoencoders, and graph-based methods, are essential when labeled attack data is scarce. These approaches are particularly suited for availability threats, where DoS or jamming attacks manifest as structural deviations in traffic or communication flows [190, 191]. Autoencoders, for example, reconstruct expected signals and flag anomalies when reconstruction error exceeds a threshold [192]. Graph neural networks extend this by modeling interdependencies across network nodes, capturing anomalies in distributed cyber-physical dynamics [193, 194]. As with other methods, unsupervised methods can themselves be deceived as adversaries may design perturbations that mimic normal variability, bypassing thresholds while still degrading integrity or availability.

Reinforcement learning (RL) provides a rigorous framework for adaptive cybersecurity defense, where RL agents continuously interact with transportation networks to learn optimal mitigation policies. Example applications include adaptive intrusion response [195, 196], traffic signal control resilience [197, 198], and dynamic spectrum allocation in vehicular networks [199]. RL particularly addresses availability by ensuring continuity of service under DoS or network congestion, while also tackling integrity threats by adjusting policies in the presence of falsified data. However, RL models are acutely vulnerable to model poisoning attacks and adversarial manipulation, since state observation attacks, reward tampering, and action perturbations can all degrade RL policy learning [200].

Generative adversarial networks (GANs) and large-scale generative models hold promise for simulating realistic cyber attack scenarios, augmenting scarce cybersecurity datasets, and stress-testing cyber resilience strategies [201, 202]. For instance, GAN-based traffic injection can simulate cyber attacks on sensor streams, enabling defenders to anticipate adversarial manipulations [203–205]. As for defense, generative models can improve confidentiality through synthetic data privacy preservation, while also enhancing integrity via adversarial training that strengthens robustness [206, 207]. Despite its advantages, generative models are also double-edged as they can be co-opted by attackers to synthesize stealthy perturbations indistinguishable from normal traffic or communication flows, directly undermining CIA protections [208, 209].

Security of AI. As outlined earlier, the flip side of AI deployment is the vulnerability of

learning algorithms themselves. Data poisoning attacks corrupt supervised training pipelines, eroding model integrity [210]. Evasion attacks craft adversarial examples that bypass anomaly detectors, threatening both confidentiality and availability [211, 212]. Model inversion and membership inference attacks exploit learned models to recover sensitive training data, striking at confidentiality [213, 214]. In reinforcement learning, policy manipulation through adversarial perturbations can compromise adaptive defense, reducing availability [215]. Even generative AI is not immune noting that adversaries can exfiltrate sensitive data from foundation models through prompt injection or use them to craft highly realistic cyber attacks [216].

3.1.3. Emerging Paradigms

Quantum information science and engineering (QISE) represents a rapidly evolving frontier for transportation cyber resilience. Unlike classical methods discussed in sections 3.1.1 and 3.1.2, quantum methods harness fundamental principles of quantum mechanics, such as superposition and entanglement, to introduce capabilities in computation, communication, and cryptography that cannot be matched by conventional systems. For cyber resilient CATS, this transformation could redefine how defenders and attackers interact. Within the CIA triad, quantum methods promise stronger protection of sensitive communications, new safeguards against data manipulation, and faster optimization for resilient operations. Similar to classical methods, the dual-use nature of quantum methods creates risks as adversaries may exploit quantum computing to break existing cryptosystems, accelerate cyber attack planning, or design stealthier adversarial AI methods.

Quantum-resistant cryptography (QRC). One of the most immediate implications of QISE lies in protecting confidentiality. Algorithms such as Shor's have demonstrated that once scalable quantum computers are available, today's widely deployed public-key cryptosystems could be broken in polynomial time [217, 218]. To address this, post-quantum cryptography (PQC) is being developed using mathematical problems such as lattices, error-correcting codes, multivariate polynomials, and hash-based constructions [219–222]. These methods can be computationally efficient on classical hardware and can be deployed in V2X communications, roadside-vehicle authentication, and sensor-to-controller data exchanges. Importantly, PQC strengthens confidentiality by preventing eavesdropping and spoofing, while also supporting availability since lattice-based schemes are often suitable for resource-constrained vehicular devices. However, these approaches remain vulnerable to side-channel attacks, premature standardization risks, and interoperability challenges, which adversaries may exploit to degrade confidentiality and availability in large-scale transportation networks [223, 224].

Quantum key distribution (QKD) and quantum networks. While post-quantum cryptography resists quantum attackers using classical resources, quantum key distribution (QKD) directly exploits physical quantum properties to guarantee confidentiality. Any attempt at eavesdropping disturbs the transmitted quantum states, alerting communicating parties to the intrusion [225, 226]. This means QKD enables information-theoretic secure key exchange, even

against an adversary with unlimited computational power. For integrity, QKD strengthens message authentication by ensuring that falsification attempts in control channels, such as fake vehicle trajectory updates or altered traffic signal commands, are detectable [227–229]. Nevertheless, QKD faces deployment barriers for availability. It requires specialized optical infrastructure, is sensitive to noise and distance, and cannot yet scale across heterogeneous vehicular and roadside systems without hybrid integration with classical cryptography [230, 231]. Hybrid infrastructures that combine QKD for backbone communications and PQC for last-hop vehicular links may provide a path toward resilient deployment in transportation networks [232].

Quantum-enhanced optimization and control. Beyond cryptography, quantum computing has potential to transform optimization and control tasks that are critical for transportation cyber resilience. Techniques such as the quantum approximate optimization algorithm [233] and quantum annealing [234] are being tested for solving large-scale combinatorial optimization problems faster than classical solvers [235]. In practice, this could enable real-time vehicle rerouting during network disruptions, dynamic fleet scheduling under cyber constraints, or rapid restoration of traffic flows after DoS attacks. By accelerating convergence and improving exploration of solution spaces, quantum solvers enhance availability by reducing recovery time. With regard to integrity, quantum-enhanced anomaly detection is being explored to analyze massive high-dimensional cyber and traffic datasets, potentially distinguishing subtle manipulations from natural variability [236, 237]. Despite these promising strengths, the same strength could be weaponized as adversaries may use quantum solvers to craft undetectable perturbations in reinforcement learning-based traffic signal controllers or to optimize coordinated false-data injection [238–240].

3.2. Testing and Evaluation

Testing and evaluation form the practical foundation of cyber resilient transportation. While theoretical and computational models discussed in section 3.1 provide insights into vulnerabilities and defense strategies, their credibility rests on robust evaluation pipelines. These pipelines encompass simulation-based studies, digital twins that closely mirror reality, and physical testbeds and cyber ranges that integrate live hardware, communications, and adversarial tooling. Together, they provide a continuum for assessing the resilience to CIA attack surfaces, enabling reproducibility, benchmarking, and meaningful comparison across methods.

3.2.1. Simulation and Digital Twins

High-fidelity simulation environments are widely used to emulate traffic dynamics and cyberattack scenarios without incurring safety risks. Microscopic traffic simulators, such as SUMO and VISSIM, have been integrated with communication and network simulators to evaluate DoS attacks, false data injection, and GPS spoofing in vehicular networks [241, 242]. These co-simulation frameworks capture the coupling between mobility, control, and communication layers,

making them valuable for analyzing availability and integrity threats at scale.

Beyond traditional simulation, digital twin architectures represent a frontier for cyber resilience evaluation. Digital twins synchronize real-time traffic, infrastructure, and cyber data with virtual models, allowing continuous monitoring, predictive assessment, and testing of defense strategies [243–245]. For instance, in connected intersection control, digital twins can replicate sensor feeds and controller states to evaluate the impact of adversarial packet loss or falsified messages, while ensuring confidentiality by controlling access to mirrored data streams [246, 247]. However, the accuracy of digital twins depends critically on data fidelity and synchronization, which themselves may become attack surfaces if adversaries compromise update channels.

3.2.2. Physical Testbeds and Cyber Ranges

Physical testbeds complement simulations by providing hardware realism and exposing unforeseen vulnerabilities. Hardware-in-the-loop (HIL) systems integrate real controllers and roadside units with simulated environments, enabling repeatable testing of availability disruptions such as jamming [248–252]. Fleet pilots and roadway deployments extend realism further, but raise concerns of safety governance and liability, necessitating careful instrumentation and safeguards. Moreover, cyber ranges extend the physical paradigm into controlled adversarial experimentation, in which they integrate networking equipment, programmable logic controllers, and adversarial tools for safe red-team exercises [253, 254]. Cyber ranges provide reproducibility and controlled exposure of confidentiality and integrity attack types, while allowing researchers to validate cyber resilience metrics such as detection delay or recovery latency in environments close to operational networks. However, scaling such platforms to large traffic systems remains resource intensive, and interoperability between cyber ranges and transportation testbeds remains an open challenge [255].

3.2.3. Benchmarks, Datasets, and Metrics

A crucial enabler of credible evaluation is the establishment of standardized benchmarks. Datasets capturing traffic dynamics, communication traces, and cyber attack logs provide the foundation for reproducibility. For example, open datasets on vehicular communications and transportation networks can be used to evaluate intrusion detection systems against confidentiality and integrity attacks [256–259]. However, many studies remain limited by proprietary datasets or synthetic attack traces, raising questions of generalizability.

Cyber resilience metrics are equally important. Performance degradation measures capture the loss of traffic throughput or increased delay under attack. Detection delay and false-alarm rates quantify the responsiveness and precision of anomaly detection systems. Recovery latency measures how quickly a system restores functionality after disruption, while cascading impact analysis tracks how local failures propagate to system-wide disruptions [260–263]. In addition,

benchmarking protocols that systematically vary attack intensity, duration, and location enable fair comparison across competing defenses. Without such shared protocols, resilience claims risk being fragmented or incomparable.

4. Vision and Outlook

The conceptual foundations established in Section 2 and the methodological frontiers outlined in Section 3 together provide a structured perspective for understanding both the current state and future trajectory of cyber resilience in CATS. Section 2 introduced the multi-faceted attack surfaces across the CIA triad, the defense and resilience objectives spanning robustness, detection, response, recovery, and adaptation, and the contrasting architectural approaches such as modular and end-to-end pipelines. Section 3 extended these insights by highlighting frontier methodologies in optimization, game theory, AI, and quantum information science and engineering, while also emphasizing the growing need for rigorous evaluation and benchmarking infrastructures. Yet, the insights from Sections 2 and 3 also underscore persistent fragmentation in the sense that defenses are studied at single scales rather than across them, methodological advances are siloed without accounting for their dual-use nature, and evaluation infrastructures remain immature. Therefore, Section 4 outlines a forward-looking vision that synthesizes these gaps into a coherent research agenda, spanning cross-layer resilience, unified trustworthiness, certified guarantees and trade-offs, dual-use vulnerabilities, emerging paradigms, lifecycle composition of resilience objectives, benchmarking, and socio-technical governance.

4.1. Cross-Layer Resilience Across Scales, Functions, and Components

One of the most critical gaps is the lack of integrated resilience frameworks that operate across transportation systems scales, system functions compromised, and targeted cyber-physical components. Cyber threats against CATS do not remain confined to one level or module. Rather, they propagate across micro, meso, and macro layers, and can simultaneously exploit interdependencies among connectivity, autonomy, sensing, control, and network infrastructure. For example, a falsified perception input may corrupt the sensing stack, destabilize cooperative adaptive cruise control at the corridor level, and bias demand flows for network-level traffic routing algorithms. Similarly, a DoS attack on V2X connectivity can disrupt communication networks, impair autonomy decisions that rely on timely updates, and cascade into degraded regional mobility. Yet existing research tends to address these boundaries in isolation through intrusion detection for in-vehicle networks, cryptographic safeguards for connectivity, anomaly monitors for arterial corridors, or redundancy in control modules. This siloed development leaves systems vulnerable to adversaries capable of coordinating campaigns across scales, functions, and components simultaneously. Addressing this challenge requires new abstractions for hierarchical data fusion, compositional resilience guarantees that account for cross-domain interactions, and architectures that ensure interventions at one level or module reinforce resilience across the

broader system. Developing such cross-layer frameworks remains largely unexplored yet is indispensable for preventing adversaries from exploiting the artificial boundaries that currently fragment defenses.

4.2. Unified Trustworthiness Beyond CIA Silos

Closely related to the challenge of cross-layer resilience is the need to move beyond the narrow framing of trustworthiness as isolated CIA objectives. Transportation systems must also contend with safety, interpretability, accountability, and fairness, all of which interact with resilience and security in complex ways. A single GNSS spoofing attack, for instance, simultaneously violates integrity, undermines resilience, and jeopardizes safety. Similarly, an anomaly detector that maximizes detection accuracy may sacrifice interpretability, eroding operator trust and compliance. The siloed treatment of trustworthiness properties —more specifically, confidentiality safeguarded by encryption, integrity by anomaly detection, availability by redundancy, safety by runtime assurance, privacy by federated learning, and interpretability by explainable AI— leads to brittle systems where gains in one dimension often come at the expense of another. As a consequence, a major research gap is the absence of unified frameworks that jointly model and optimize multiple trustworthiness dimensions. Such frameworks must quantify interdependencies, articulate trade-offs (e.g., between privacy and interpretability, or safety and efficiency), and design architectures that achieve balance rather than isolated protection. Only by treating security, resilience, safety, interpretability, and related properties as an integrated whole can CATS achieve trustworthy operation in adversarial and uncertain environments.

4.3. Guarantees and Trade-offs in Safety-Critical Contexts

A second and closely related gap lies in the limited availability of certified guarantees for cyber resilience strategies across methods. While control-theoretic and optimization-based techniques sometimes provide bounded assurances, AI, probabilistic, and quantum methods are typically deployed with only empirical validation. As transportation applications become increasingly safety-critical and latency-constrained, this reliance on empirical robustness becomes insufficient. Systems that must guarantee safe stopping distances, real-time traffic signal operations, or collision avoidance cannot depend on defenses that degrade unpredictably under unforeseen attacks. Moreover, there exists a fundamental efficiency-resilience trade-off, where stronger guarantees often require conservative assumptions or higher computational overhead, which may reduce system efficiency or responsiveness. Conversely, methods tuned for efficiency and adaptivity often sacrifice provable resilience. Hence, striking the right balance between efficiency and resilience under strict safety and latency requirements is a pressing research challenge, one that demands new frameworks for quantifying and optimizing these trade-offs.

4.4. Security of Methods: The Dual-Use Dilemma

Beyond guarantees, a broader systemic gap arises from the dual-use nature of the very methods deployed for cyber resilience. Optimization, game theory, control, AI, and quantum techniques provide defenders with sophisticated tools for robustness, detection, and recovery, yet adversaries can exploit the same methods to craft stealthier, more adaptive, and more scalable attacks. Robust optimization can be inverted to design adversarial inputs that lie just outside assumed uncertainty sets. Game-theoretic equilibria can be exploited by adversaries who anticipate and adapt to defenders' strategies. Control-theoretic approaches can be subverted by aligning attacks with natural system dynamics, evading detection while destabilizing operations. AI introduces vulnerabilities such as model poisoning, evasion, and concept drift that directly erode its defensive value, while quantum solvers could equally empower adversaries to optimize coordinated false-data injection or break cryptosystems. What is missing is a general theory for bounding adversarial co-option of methods, along with architectures that explicitly account for the possibility of methodological exploitation. Unless addressed, the dual-use dilemma risks undermining cyber resilience at its very foundations.

4.5. Emerging Paradigms: Quantum and Post-Quantum Resilience

The potential of emerging paradigms such as post-quantum cryptography, quantum key distribution, and quantum-enhanced optimization adds both opportunity and complexity to the cyber resilience landscape. Existing work has demonstrated proof-of-concept deployments of PQC in vehicular communication channels and evaluated the feasibility of hybrid PQC-classical protocols, yet practical integration into latency-sensitive and resource-constrained vehicular networks remains elusive. Similarly, quantum key distribution offers theoretically secure communication, but its reliance on specialized infrastructure and sensitivity to noise hinder its applicability in heterogeneous roadside environments. Quantum optimization and machine learning have shown promise in accelerating routing and recovery tasks, but their runtime behavior and stability under adversarial perturbations remain undefined. The dual-use nature of these paradigms further complicates matters, since quantum solvers that accelerate resilience could equally empower adversaries to design undetectable attacks or break cryptosystems. A rigorous research agenda is thus needed to establish models of scalability, interoperability, and adversarial symmetry, ensuring that emerging paradigms are operationalized with verifiable guarantees rather than aspirational claims.

4.6. Lifecycle Composition of Cyber Resilience Objectives

Section 2.2 defined cyber resilience as a lifecycle of robustness, detection, response, recovery, and adaptation. Yet, existing research often treats these stages as independent, developing methods for robustness, anomaly detection, or adaptive recovery in isolation. In practice, however, these stages are deeply interconnected, noting that delayed detection reduces the efficacy of response, overly conservative robustness measures may limit adaptability, and adaptation

strategies, if poorly guided, may reinforce adversarial patterns or degrade long-term stability. Few models exist that systematically capture these lifecycle interactions or quantify resilience as a temporally composed property [38]. A critical gap is therefore the development of lifecycle-aware resilience frameworks that explicitly model dependencies among stages, quantify trade-offs across objectives, and provide verifiable guarantees of end-to-end system behavior under attack. Such frameworks would move cyber resilience research beyond isolated objectives toward holistic, lifecycle-oriented assurance.

4.7. Standardization of Evaluation and Benchmarking

Another enduring limitation lies in the fragmentation of evaluation infrastructures. Although simulation platforms, digital twins, and cyber ranges are increasingly employed, their deployment remains inconsistent, relying on proprietary datasets, heterogeneous attack models, and non-standard metrics. This fragmentation undermines reproducibility and comparability across studies, with resilience claims often resting on narrowly scoped evidence. Without shared evaluation protocols, the field lacks the cumulative knowledge base needed for scientific progress. As a result, a pressing research need exists for standardized benchmarking frameworks that define canonical attack-defense scenarios, open datasets spanning communication, control, and traffic layers, and cyber resilience metrics that capture cascading impacts across scales. Establishing such standards will not only enable fair comparison of competing methods but also accelerate the translation of laboratory demonstrations into operational practice.

4.8. Socio-Technical Integration: Governance, Deployment, & Human Factors

Last but not least, cyber resilience must be understood not only as a technical property but as a socio-technical capability shaped by governance, regulation, and human behavior. Technological defenses may be robust and adaptive, but their effectiveness depends on operator compliance, institutional support, and user trust. Trade-offs between robustness and efficiency, privacy and availability, or safety and throughput cannot be resolved by technical design alone. Rather, they require governance mechanisms and regulatory frameworks that align incentives and enforce compliance. Moreover, human actors introduce their own vulnerabilities, considering that operators may override safety mechanisms to maintain throughput, users may disable security features for convenience, and agencies may under-invest in monitoring and evaluation. Thus, future research must extend beyond technical design to include participatory governance, compliance-aware architectures, and human-centered evaluation frameworks. Only by embedding socio-technical considerations into cyber resilience design can CATS deliver security and trustworthiness in real-world deployments.

4.9. Outlook

The path forward requires bridging fragmentation across layers, trust dimensions, resilience

guarantees, methodological dual-use risks, lifecycle objectives, and socio-technical interfaces. Doing so can transform cyber resilience from a fragmented aspiration into a provable, adaptive, and deployable capability within CATS. By aligning innovations in AI, optimization, control, and quantum with system-level governance and trustworthiness frameworks, researchers can ensure that future transportation systems are not only efficient and autonomous but also secure, safe, interpretable, and trustworthy in adversarial environments.

References

1. Di X, Shi R (2021) A survey on autonomous vehicle control in the era of mixed-autonomy: From physics-based to AI-guided driving policy learning. *Transportation Research Part C: Emerging Technologies*, 125:103008. https://doi.org/10.1016/j.trc.2021.103008

2. Li J, Yu C, Shen Z, Su Z, Ma W (2023) A survey on urban traffic control under mixed traffic environment with connected automated vehicles. *Transportation Research Part C: Emerging Technologies*, 154:104258. https://doi.org/10.1016/j.trc.2023.104258

3. Chen L, Li Y, Huang C, Li B, Xing Y, Tian D, Li L, Hu Z, Na X, Li Z, Teng S, Lv C, Wang J, Cao D, Zheng N, Wang F-Y (2023) Milestones in Autonomous Driving and Intelligent Vehicles: Survey of Surveys. *IEEE Transactions on Intelligent Vehicles*, 8(2):1046–1056. https://doi.org/10.1109/TIV.2022.3223131

4. Petit J, Shladover SE (2015) Potential Cyberattacks on Automated Vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 16(2):546–556. https://doi.org/10.1109/TITS.2014.2342271

5. Pham M, Xiong K (2021) A survey on security attacks and defense techniques for connected and autonomous vehicles. *Computers & Security*, 109:102269. https://doi.org/10.1016/j.cose.2021.102269

6. Wang F, Wang X, Ban X (Jeff) (2024) Data poisoning attacks in intelligent transportation systems: A survey. *Transportation Research Part C: Emerging Technologies*, 165:104750. https://doi.org/10.1016/j.trc.2024.104750

7. Nazari F, Noruzoliaee M, Mohammadian A (Kouros) (2025) Autonomous Vehicle Adoption Behavior and Safety Concern: A Study of Public Perception. *Multimodal Transportation*, :100252. https://doi.org/10.1016/j.multra.2025.100252

8. Koscher K, Czeskis A, Roesner F, Patel S, Kohno T, Checkoway S, McCoy D, Kantor B, Anderson D, Shacham H, Savage S (2010) Experimental Security Analysis of a Modern Automobile. *2010 IEEE Symposium on Security and Privacy*, :447–462. https://doi.org/10.1109/SP.2010.34

9. Eykholt K, Evtimov I, Fernandes E, Li B, Rahmati A, Xiao C, Prakash A, Kohno T, Song D (2018) Robust Physical-World Attacks on Deep Learning Visual Classification. *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*, :1625–1634. https://doi.org/10.1109/CVPR.2018.00175

10. Cao Y, Xiao C, Yang D, Fang J, Yang R, Liu M, Li B (2019) Adversarial Objects Against LiDAR-Based Autonomous Driving Systems. https://doi.org/10.48550/arXiv.1907.05418

11. Psiaki ML, Humphreys TE (2016) GNSS Spoofing and Detection. *Proceedings of the IEEE*, 104(6):1258–1270. https://doi.org/10.1109/JPROC.2016.2526658

12. Dasgupta S, Rahman M, Islam M, Chowdhury M (2022) A Sensor Fusion-Based GNSS Spoofing Attack Detection Framework for Autonomous Vehicles. *IEEE Transactions on Intelligent*

Transportation Systems, 23(12):23559–23572. https://doi.org/10.1109/TITS.2022.3197817

13. Perrine KA, Levin MW, Yahia CN, Duell M, Boyles SD (2019) Implications of traffic signal cybersecurity on potential deliberate traffic disruptions. *Transportation Research Part A: Policy and Practice*, 120:58–70. https://doi.org/10.1016/j.tra.2018.12.009

14. Feng Y, Huang SE, Wong W, Chen QA, Mao ZM, Liu HX (2022) On the Cybersecurity of Traffic Signal Control System With Connected Vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 23(9):16267–16279. https://doi.org/10.1109/TITS.2022.3149449

15. Sinai MB, Partush N, Yadid S, Yahav E (2014) Exploiting Social Navigation. https://doi.org/10.48550/arXiv.1410.0151

16. Waniek M, Raman G, AlShebli B, Peng JC-H, Rahwan T (2021) Traffic networks are vulnerable to disinformation attacks. *Scientific Reports*, 11(1):5329. https://doi.org/10.1038/s41598-021-84291-w

17. Eryonucu C, Papadimitratos P (2022) Sybil-Based Attacks on Google Maps or How to Forge the Image of City Life. *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, :73–84. https://doi.org/10.1145/3507657.3528538

18. GAO (2024) Critical Infrastructure Protection: Agencies Need to Enhance Oversight of Ransomware Practices and Assess Federal Support. Available online at: https://www.gao.gov/products/gao-24-106221. https://www.gao.gov/products/gao-24-106221

19. Zou B, Choobchian P, Rozenberg J (2021) Cyber resilience of autonomous mobility systems: cyber-attacks and resilience-enhancing strategies. *Journal of Transportation Security*, 14(3):137–155. https://doi.org/10.1007/s12198-021-00230-w

20. Ross R, Pillitteri V, Graubart R, Bodeau D, McQuaid R (2021) Developing cyber-resilient systems : a systems security engineering approach. :NIST SP 800-160v2r1. https://doi.org/10.6028/NIST.SP.800-160v2r1

21. Alhidaifi SM, Asghar MR, Ansari IS (2024) A Survey on Cyber Resilience: Key Strategies, Research Challenges, and Future Directions. *ACM Comput. Surv.*, 56(8):196:1-196:48. https://doi.org/10.1145/3649218

22. Araujo MS de, Machado BAS, Passos FU (2024) Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance. *Applied Sciences*, 14(5):2116. https://doi.org/10.3390/app14052116

23. Weisman MJ, Kott A, Ellis JE, Murphy BJ, Parker TW, Smith S, Vandekerckhove J (2025) Quantitative Measurement of Cyber Resilience: Modeling and Experimentation. *ACM Trans. Cyber-Phys. Syst.*, 9(1):1:1-1:25. https://doi.org/10.1145/3703159

24. Wan C, Yang Z, Zhang D, Yan X, Fan S (2018) Resilience in transportation systems: a systematic review and future directions. *Transport Reviews*, 38(4):479–498. https://doi.org/10.1080/01441647.2017.1383532

25. Shen Z, Ji C, Lu S (2024) Transportation network resilience response to the spatial feature of hazards. *Transportation Research Part D: Transport and Environment*, 128:104121. https://doi.org/10.1016/j.trd.2024.104121

26. Bernardini C, Asghar MR, Crispo B (2017) Security and privacy in vehicular communications: Challenges and opportunities. *Vehicular Communications*, 10:13–28. https://doi.org/10.1016/j.vehcom.2017.10.002

27. Yoshizawa T, Singelée D, Muehlberg JT, Delbruel S, Taherkordi A, Hughes D, Preneel B (2023) A Survey of Security and Privacy Issues in V2X Communication Systems. *ACM Comput. Surv.*, 55(9):185:1-185:36. https://doi.org/10.1145/3558052

28. Islam T, Sheakh MdA, Jui AN, Sharif O, Hasan MZ (2023) A review of cyber attacks on sensors and perception systems in autonomous vehicle. *Journal of Economy and Technology*, 1:242–258. https://doi.org/10.1016/j.ject.2024.01.002

29. Pham M, Xiong K (2021) A survey on security attacks and defense techniques for connected and autonomous vehicles. *Computers & Security*, 109:102269. https://doi.org/10.1016/j.cose.2021.102269

30. Lampe B, Meng W (2023) A survey of deep learning-based intrusion detection in automotive applications. *Expert Systems with Applications*, 221:119771. https://doi.org/10.1016/j.eswa.2023.119771

31. Khattak ZH, Park H, Hong S, Boateng RA, Smith BL (2018) Investigating Cybersecurity Issues In Active Traffic Management Systems. https://doi.org/10.48550/arXiv.1804.05901

32. Rana S, Parast FK, Kelly B, Wang Y, Kent KB (2023) A comprehensive survey of cryptography key management systems. *Journal of Information Security and Applications*, 78:103607. https://doi.org/10.1016/j.jisa.2023.103607

33. Chen J, Yan J, Kemmeugne A, Kassouf M, Debbabi M (2025) Cybersecurity of distributed energy resource systems in the smart grid: A survey. *Applied Energy*, 383:125364. https://doi.org/10.1016/j.apenergy.2025.125364

34. Zhang Z, Turnbull B, Kermanshahi SK, Pota H, Damiani E, Yeun CY, Hu J (2025) A survey on resilient microgrid system from cybersecurity perspective. *Applied Soft Computing*, 175:113088. https://doi.org/10.1016/j.asoc.2025.113088

35. Pavão J, Bastardo R, Rocha NP (2024) Cyber Resilience and Healthcare Information Systems, a Systematic Review. *Procedia Computer Science*, 239:149–157. https://doi.org/10.1016/j.procs.2024.06.157

36. Segovia-Ferreira M, Rubio-Hernan J, Cavalli A, Garcia-Alfaro J (2024) A Survey on Cyber-Resilience Approaches for Cyber-Physical Systems. *ACM Comput. Surv.*, 56(8):202:1-202:37. https://doi.org/10.1145/3652953

37. Zhu Q (2024) Foundations of Cyber Resilience: The Confluence of Game, Control, and Learning Theories. https://doi.org/10.48550/arXiv.2404.01205

38. Huang Y, Huang L, Zhu Q (2022) Reinforcement Learning for feedback-enabled cyber resilience. *Annual Reviews in Control*, 53:273–295. https://doi.org/10.1016/j.arcontrol.2022.01.001

39. Liao Z, Shi J, Zhang Y, Wang S, Sun Z (2024) A Survey of Resilient Coordination for Cyber-Physical Systems Against Malicious Attacks. https://doi.org/10.48550/arXiv.2402.10505

40. Sun X, Yu FR, Zhang P (2022) A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs). *IEEE Transactions on Intelligent Transportation Systems*, 23(7):6240–6259. https://doi.org/10.1109/TITS.2021.3085297

41. Engoulou RG, Bellaïche M, Pierre S, Quintero A (2014) VANET security surveys. *Computer Communications*, 44:1–13. https://doi.org/10.1016/j.comcom.2014.02.020

42. Petit J, Schaub F, Feiri M, Kargl F (2015) Pseudonym Schemes in Vehicular Networks: A Survey. *IEEE Communications Surveys & Tutorials*, 17(1):228–255. https://doi.org/10.1109/COMST.2014.2345420

43. Alipour-Fanid A, Dabaghchian M, Zeng K (2020) Impact of Jamming Attacks on Vehicular Cooperative Adaptive Cruise Control Systems. *IEEE Transactions on Vehicular Technology*, 69(11):12679–12693. https://doi.org/10.1109/TVT.2020.3030251

44. Ying B, Makrakis D, Mouftah HT (2013) Dynamic Mix-Zone for Location Privacy in Vehicular Networks. *IEEE Communications Letters*, 17(8):1524–1527. https://doi.org/10.1109/LCOMM.2013.070113.122816

45. Zhang C, Zhu L, Xu C, Du X, Guizani M (2019) A Privacy-Preserving Traffic Monitoring Scheme via Vehicular Crowdsourcing. *Sensors*, 19(6):1274. https://doi.org/10.3390/s19061274

46. Babaghayou M, Labraoui N, Abba Ari AA, Lagraa N, Ferrag MA (2020) Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: A survey. *Journal of Information Security and Applications*, 55:102618. https://doi.org/10.1016/j.jisa.2020.102618

47. Dhanush K, Azeez SA, Vara Prasad KHN, Sai Kiran PM, Kavitha S, Kavitha M (2024) A Comprehensive Study on Misconfiguration-SAAS Security Threat. *2024 Second International Conference on Inventive Computing and Informatics (ICICI)*, :433–438. https://doi.org/10.1109/ICICI62254.2024.00077

48. Vincenzi MD, Pesé MD, Bodei C, Matteucci I, Brooks RR, Hasan M, Saracino A, Hamad M, Steinhorst S (2024) Contextualizing Security and Privacy of Software-Defined Vehicles: State of the Art and Industry Perspectives. https://doi.org/10.48550/arXiv.2411.10612

49. Richter I, Zhou J, Criswell J (2024) DeTRAP: RISC-V Return Address Protection With Debug Triggers. https://doi.org/10.48550/arXiv.2408.17248

50. Farsimadan E, Moradi L, Palmieri F (2025) A Review on Security Challenges in V2X Communications Technology for VANETs. *IEEE Access*, 13:31069–31094. https://doi.org/10.1109/ACCESS.2025.3541035

51. Jover RP (2019) The current state of affairs in 5G security and the main remaining security challenges. https://doi.org/10.48550/arXiv.1904.08394

52. Privacy-preserving Pedestrian Tracking using Distributed 3D LiDARs | IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/10099061

53. Fredrikson M, Jha S, Ristenpart T (2015) Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, :1322–1333. https://doi.org/10.1145/2810103.2813677

54. Zhou Z, Zhu J, Yu F, Li X, Peng X, Liu T, Han B (2024) Model Inversion Attacks: A Survey of Approaches and Countermeasures. https://doi.org/10.48550/arXiv.2411.10023

55. Shokri R, Stronati M, Song C, Shmatikov V (2017) Membership Inference Attacks Against Machine Learning Models. *2017 IEEE Symposium on Security and Privacy (SP)*, :3–18. https://doi.org/10.1109/SP.2017.41

56. A Survey of Model Extraction Attacks and Defenses in Distributed Computing Environments. https://arxiv.org/html/2502.16065v1

57. Guntupalli R (2024) Enhancing Cloud Security with AI: A Deep Learning Approach to Identify and Prevent Cyberattacks in Multi-Tenant Environments. https://doi.org/10.2139/ssrn.5329132

58. Chippagiri S (2025) A Study of Cloud Security Frameworks for Safeguarding Multi-Tenant Cloud Architectures. *International Journal of Computer Applications*, 186(60):50–57. https://doi.org/10.5120/ijca2025924369

59. Analyzing and Preventing Data Privacy Leakage in Connected Vehicle Services. https://www.sae.org/publications/technical-papers/content/2019-01-0478/

60. Huang X, Wang X (2022) Detection and Isolation of False Data Injection Attack in Intelligent Transportation System via Robust State Observer. *Processes*, 10(7):1299. https://doi.org/10.3390/pr10071299

61. Elsaeidy AA, Jagannath N, Sanchis AG, Jamalipour A, Munasinghe KS (2020) Replay Attack Detection in Smart Cities Using Deep Learning. *IEEE Access*, 8:137825–137837. https://doi.org/10.1109/ACCESS.2020.3012411

62. Kumar A, Shahid MA, Jaekel A, Zhang N, Kneppers M (2023) Machine learning based detection of replay attacks in VANET. *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, :1–6. https://doi.org/10.1109/NOMS56928.2023.10154299

63. Alnabulsi H, Islam R (2019) Protecting Code Injection Attacks in Intelligent Transportation System. *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, :799–806. https://doi.org/10.1109/TrustCom/BigDataSE.2019.00116

64. Vuong TP, Loukas G, Gan D, Bezemskij A (2015) Decision tree-based detection of denial of service and command injection attacks on robotic vehicles. *2015 IEEE International Workshop on Information Forensics and Security (WIFS)*, :1–6. https://doi.org/10.1109/WIFS.2015.7368559

65. Kong P-Y (2021) A Survey of Cyberattack Countermeasures for Unmanned Aerial Vehicles. *IEEE Access*, 9:148244–148263. https://doi.org/10.1109/ACCESS.2021.3124996

66. Dafoe J, Singh H, Chen N, Chen B (2024) Enabling Real-Time Restoration of Compromised ECU Firmware in Connected and Autonomous Vehicles. *Security and Privacy in Cyber-Physical Systems and Smart Vehicles*, :15–33. https://doi.org/10.1007/978-3-031-51630-6_2

67. Bielawski R, Gaynier R, Ma D, Lauzon S, Weimerskirch A, University of Michigan. Transportation Research Institute, University of Michigan D, Volkswagen Group of America (Herndon V (2020) Cybersecurity of Firmware Updates. https://doi.org/10.21949/1530213

68. Mbakoyiannis D, Tomoutzoglou O, Kornaros G (2019) Secure over-the-air firmware updating for automotive electronic control units. *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, :174–181. https://doi.org/10.1145/3297280.3297299

69. Duan X, Yan H, Tian D, Zhou J, Su J, Hao W (2023) In-Vehicle CAN Bus Tampering Attacks Detection for Connected and Autonomous Vehicles Using an Improved Isolation Forest Method. *IEEE Transactions on Intelligent Transportation Systems*, 24(2):2122–2134. https://doi.org/10.1109/TITS.2021.3128634

70. Rathore H, Samant A, Jadliwala M (2021) TangleCV: A Distributed Ledger Technique for Secure Message Sharing in Connected Vehicles. *ACM Trans. Cyber-Phys. Syst.*, 5(1):6:1-6:25. https://doi.org/10.1145/3404500

71. Ahmad F, Kurugollu F, Adnane A, Hussain R, Hussain F (2020) MARINE: Man-in-the-Middle Attack Resistant Trust Model in Connected Vehicles. *IEEE Internet of Things Journal*, 7(4):3310–3322. https://doi.org/10.1109/JIOT.2020.2967568

72. Ahmad F, Adnane A, Franqueira VNL, Kurugollu F, Liu L (2018) Man-In-The-Middle Attacks in Vehicular Ad-Hoc Networks: Evaluating the Impact of Attackers' Strategies. *Sensors*, 18(11):4040. https://doi.org/10.3390/s18114040

73. Bhatti J, Humphreys TE (2017) Hostile Control of Ships via False GPS Signals: Demonstration and Detection. *NAVIGATION*, 64(1):51–66. https://doi.org/10.1002/navi.183

74. Mohammadi A, Ahmari R, Hemmati V, Owusu-Ambrose F, Mahmoud MN, Kebria P, Homaifar A (2025) Detection of Multiple Small Biased GPS Spoofing Attacks on Autonomous Vehicles Using Time Series Analysis. *IEEE Open Journal of Vehicular Technology*, 6:1152–1163. https://doi.org/10.1109/OJVT.2025.3559461

75. Dasgupta S, Shakib KH, Rahman M (2024) Experimental Validation of Sensor Fusion-based GNSS Spoofing Attack Detection Framework for Autonomous Vehicles. https://doi.org/10.48550/arXiv.2401.01304

76. Wang J, Guo J, Li K, Zheng H (2024) Distributed Adaptive Event-Triggered Control of Connected Automated Vehicle Platoon Systems With Spoofing Cyber Attacks. *IEEE Transactions on Vehicular Technology*, 73(12):18186–18197. https://doi.org/10.1109/TVT.2024.3436052

77. Chu K-F, Guo W (2024) Multi-Agent Reinforcement Learning-Based Passenger Spoofing Attack on Mobility-as-a-Service. *IEEE Transactions on Dependable and Secure Computing*, 21(6):5565–5581. https://doi.org/10.1109/TDSC.2024.3379283

78. Eykholt K, Evtimov I, Fernandes E, Li B, Rahmati A, Xiao C, Prakash A, Kohno T, Song D (2018) Robust Physical-World Attacks on Deep Learning Models. https://doi.org/10.48550/arXiv.1707.08945

79. Sun J, Cao Y, Chen QA, Mao ZM (2020) Towards Robust LiDAR-based Perception in Autonomous Driving: General Black-box Adversarial Sensor Attack and Countermeasures. :877–894. https://www.usenix.org/conference/usenixsecurity20/presentation/sun

80. PhantomLiDAR: Cross-modality Signal Injection Attacks against LiDAR. https://arxiv.org/html/2409.17907v1

81. Cao Y, Xiao C, Yang D, Fang J, Yang R, Liu M, Li B (2019) Adversarial Objects Against LiDAR-Based Autonomous Driving Systems. https://doi.org/10.48550/arXiv.1907.05418

82. Fang M, Cao X, Jia J, Gong NZ (2021) Local Model Poisoning Attacks to Byzantine-Robust Federated Learning. https://doi.org/10.48550/arXiv.1911.11815

83. Almutairi S, Barnawi A (2024) A comprehensive analysis of model poisoning attacks in federated learning for autonomous vehicles: A benchmark study. *Results in Engineering*, 24:103295. https://doi.org/10.1016/j.rineng.2024.103295

84. Zhang X, Ma Y, Singla A, Zhu X (2020) Adaptive Reward-Poisoning Attacks against Reinforcement Learning. *Proceedings of the 37th International Conference on Machine Learning*, :11225–11234. https://proceedings.mlr.press/v119/zhang20u.html

85. Gu T, Liu K, Dolan-Gavitt B, Garg S (2019) BadNets: Evaluating Backdooring Attacks on Deep Neural Networks. *IEEE Access*, 7:47230–47244. https://doi.org/10.1109/ACCESS.2019.2909068

86. Wang Y, Sarkar E, Li W, Maniatakos M, Jabari SE (2021) Stop-and-Go: Exploring Backdoor Attacks on Deep Reinforcement Learning-based Traffic Congestion Control Systems. *IEEE Transactions on Information Forensics and Security*, 16:4772–4787. https://doi.org/10.1109/TIFS.2021.3114024

87. Wang H, Sreenivasan K, Rajput S, Vishwakarma H, Agarwal S, Sohn J, Lee K, Papailiopoulos D (2020) Attack of the Tails: Yes, You Really Can Backdoor Federated Learning. https://doi.org/10.48550/arXiv.2007.05084

88. Xiao B, Yu B, Gao C (2006) Detection and localization of sybil nodes in VANETs. *Proceedings of*

the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks, :1–8. https://doi.org/10.1145/1160972.1160974

89. Boeira F, Barcellos MP, Freitas EP de, Vinel A, Asplund M (2017) On the impact of sybil attacks in cooperative driving scenarios. *2017 IFIP Networking Conference (IFIP Networking) and Workshops*, :1–2. https://doi.org/10.23919/IFIPNetworking.2017.8264890

90. Yu JJQ (2021) Sybil Attack Identification for Crowdsourced Navigation: A Self-Supervised Deep Learning Approach. *IEEE Transactions on Intelligent Transportation Systems*, 22(7):4622–4634. https://doi.org/10.1109/TITS.2020.3036085

91. Fung C, Yoon CJM, Beschastnikh I (2020) Mitigating Sybils in Federated Learning Poisoning. https://doi.org/10.48550/arXiv.1808.04866

92. Xie C, Koyejo S, Gupta I (2019) Fall of Empires: Breaking Byzantine-tolerant SGD by Inner Product Manipulation. https://doi.org/10.48550/arXiv.1903.03936

93. Dimc F, Pavlovčič-Prešeren P, Bažec M (2021) Robustness against Chirp Signal Interference of On-Board Vehicle Geodetic and Low-Cost GNSS Receivers. *Sensors*, 21(16):5257. https://doi.org/10.3390/s21165257

94. Qiao J, Lu Z, Lin B, Song J, Xiao Z, Wang Z, Li B (2023) A survey of GNSS interference monitoring technologies. *Frontiers in Physics*, 11https://doi.org/10.3389/fphy.2023.1133316

95. Trkulja N, Starobinski D, Berry RA (2020) Denial-of-Service Attacks on C-V2X Networks. *arXiv.org*, https://arxiv.org/abs/2010.13725v1

96. Giang AT, Tran HT, Le HT, Doan NQ, Nguyen MH (2022) Jamming Attack in Vehicular Networks: Adaptively Probabilistic Channel Surfing Scheme. *Wireless Communications and Mobile Computing*, 2022(1):3884761. https://doi.org/10.1155/2022/3884761

97. Karthikeyan H, Usha G (2022) Real-time DDoS flooding attack detection in intelligent transportation systems. *Computers and Electrical Engineering*, 101:107995. https://doi.org/10.1016/j.compeleceng.2022.107995

98. Abdullah M, Raza I, Zia T, Hussain SA (2021) Interest flooding attack mitigation in a vehicular named data network. *IET Intelligent Transport Systems*, 15(4):525–537. https://doi.org/10.1049/itr2.12042

99. Sousa B, Magaia N, Silva S, Thanh Hieu N, Liang Guan Y (2024) Vehicle-to-Vehicle Flooding Datasets using MK5 On-board Unit Devices. *Scientific Data*, 11(1):1363. https://doi.org/10.1038/s41597-024-04173-4

100. Sheikh MS, Liang J, Wang W (2019) A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs). *Sensors*, 19(16):3589. https://doi.org/10.3390/s19163589

101. Wan Z, Shen J, Chuang J, Xia X, Garcia J, Ma J, Chen QA (2022) Too Afraid to Drive: Systematic Discovery of Semantic DoS Vulnerability in Autonomous Driving Planning under Physical-World Attacks. https://doi.org/10.48550/arXiv.2201.04610

102. Chen E-C, Chen P-Y, Chung I-H, Lee C (2024) Overload: Latency Attacks on Object Detection for Edge Devices. https://doi.org/10.48550/arXiv.2304.05370

103. Stübler T, Amodei A, Capriglione D, Tomasso G, Bonnotte N, Mohammed S (2024) An Investigation of Denial of Service Attacks on Autonomous Driving Software and Hardware in Operation. https://doi.org/10.48550/arXiv.2409.01324

104. Ross R, Pillitteri V, Graubart R, Bodeau D, McQuaid R (2021) Developing cyber-resilient systems : a systems security engineering approach. :NIST SP 800-160v2r1. https://doi.org/10.6028/NIST.SP.800-160v2r1

105. Hosseini S, Barker K, Ramirez-Marquez JE (2016) A review of definitions and measures of system resilience. *Reliability Engineering & System Safety*, 145:47–61. https://doi.org/10.1016/j.ress.2015.08.006

106. Linkov I, Kott A (2019) Fundamental Concepts of Cyber Resilience: Introduction and Overview. *Cyber Resilience of Systems and Networks*, :1–25. https://doi.org/10.1007/978-3-319-77492-3_1

107. Althoff M, Dolan JM (2014) Online Verification of Automated Road Vehicles Using Reachability Analysis. *IEEE Transactions on Robotics*, 30(4):903–918. https://doi.org/10.1109/TRO.2014.2312453

108. Öncü S, Ploeg J, Wouw N van de, Nijmeijer H (2014) Cooperative Adaptive Cruise Control: Network-Aware Analysis of String Stability. *IEEE Transactions on Intelligent Transportation Systems*, 15(4):1527–1537. https://doi.org/10.1109/TITS.2014.2302816

109. Feng S, Zhang Y, Li SE, Cao Z, Liu HX, Li L (2019) String stability for vehicular platoon control: Definitions and analysis methods. *Annual Reviews in Control*, 47:81–97. https://doi.org/10.1016/j.arcontrol.2019.03.001

110. Zhu Q, Basar T (2024) Disentangling Resilience from Robustness: Contextual Dualism, Interactionism, and Game-Theoretic Paradigms. https://doi.org/10.48550/arXiv.2403.06299

111. Althunayyan M, Javed A, Rana O (2025) A Survey of Learning-Based Intrusion Detection Systems for In-Vehicle Network. https://doi.org/10.48550/arXiv.2505.11551

112. Jeong S, Lee S, Lee H, Kim HK (2024) X-CANIDS: Signal-Aware Explainable Intrusion Detection System for Controller Area Network-Based In-Vehicle Network. *IEEE Transactions on Vehicular Technology*, 73(3):3230–3246. https://doi.org/10.1109/TVT.2023.3327275

113. Liu Y, Xue L, Wang S, Luo X, Zhao K, Jing P, Ma X, Tang Y, Zhou H (2025) Vehicular Intrusion Detection System for Controller Area Network: A Comprehensive Survey and Evaluation. *IEEE Transactions on Intelligent Transportation Systems*, 26(7):10979–11009. https://doi.org/10.1109/TITS.2025.3567940

114. Psiaki ML, Humphreys TE (2016) GNSS Spoofing and Detection. *Proceedings of the IEEE*, 104(6):1258–1270. https://doi.org/10.1109/JPROC.2016.2526658

115. Sabour S, Rao S, Ghaderi M (2021) DeepFlow: Abnormal Traffic Flow Detection Using Siamese Networks. https://doi.org/10.48550/arXiv.2108.12016

116. Chowdhury A, Karmakar G, Kamruzzaman J, Das R, Newaz SHS (2023) An Evidence Theoretic Approach for Traffic Signal Intrusion Detection. *Sensors*, 23(10):4646. https://doi.org/10.3390/s23104646

117. Online Verification of Automated Road Vehicles Using Reachability Analysis | IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/document/6784493

118. Bernabei F, Secchi C (2025) Smart infrastructure and autonomous vehicles: Ensuring safety and efficiency in urban traffic with Control Barrier Functions. *Mechatronics*, 109:103332. https://doi.org/10.1016/j.mechatronics.2025.103332

119. Molnar TG, Orosz G, Ames AD (2023) On the Safety of Connected Cruise Control: Analysis and Synthesis with Control Barrier Functions. https://doi.org/10.48550/arXiv.2309.00074

120. Abate M, Coogan S (2020) Enforcing Safety at Runtime for Systems with Disturbances. https://doi.org/10.48550/arXiv.2008.07019

121. Pan Y, Li T, Zhu Q (2022) On the Resilience of Traffic Networks under Non-Equilibrium Learning. https://doi.org/10.48550/arXiv.2210.03214

122. Pan Y, Li T, Zhu Q (2023) Is Stochastic Mirror Descent Vulnerable to Adversarial Delay Attacks? A Traffic Assignment Resilience Study. *2023 62nd IEEE Conference on Decision and Control (CDC)*, :8328–8333. https://doi.org/10.1109/CDC49753.2023.10384003

123. Mousavinejad E, Yang F, Han Q-L, Ge X, Vlacic L (2020) Distributed Cyber Attacks Detection and Recovery Mechanism for Vehicle Platooning. *IEEE Transactions on Intelligent Transportation Systems*, 21(9):3821–3834. https://doi.org/10.1109/TITS.2019.2934481

124. Akowuah F, Prasad R, Espinoza CO, Kong F (2021) Recovery-by-Learning: Restoring Autonomous Cyber-physical Systems from Sensor Attacks. *2021 IEEE 27th International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA)*, :61–66. https://doi.org/10.1109/RTCSA52859.2021.00015

125. Shin J, Baek Y, Lee J, Lee S (2019) Cyber-Physical Attack Detection and Recovery Based on RNN in Automotive Brake Systems. *Applied Sciences*, 9(1):82. https://doi.org/10.3390/app9010082

126. Zhang T, Xu C, Zhang B, Shen J, Kuang X, Grieco LA (2022) Toward Attack-Resistant Route Mutation for VANETs: An Online and Adaptive Multiagent Reinforcement Learning Approach. *IEEE Transactions on Intelligent Transportation Systems*, 23(12):23254–23267. https://doi.org/10.1109/TITS.2022.3198507

127. Yang Y-T, Zhu Q (2024) Game-Theoretic Foundations for Cyber Resilience Against Deceptive Information Attacks in Intelligent Transportation Systems. https://doi.org/10.48550/arXiv.2412.04627

128. Bozdal M, Samie M, Aslam S, Jennions I (2020) Evaluation of CAN Bus Security Challenges. *Sensors*, 20(8):2364. https://doi.org/10.3390/s20082364

129. You C, Hau Z, Demetriou S (2021) Temporal Consistency Checks to Detect LiDAR Spoofing Attacks on Autonomous Vehicle Perception. *Proceedings of the 1st Workshop on Security and Privacy for Mobile AI*, :13–18. https://doi.org/10.1145/3469261.3469406

130. Blevins DH, Moriano P, Bridges RA, Verma ME, Iannacone MD, Hollifield SC (2021) Time-Based CAN Intrusion Detection Benchmark. *Proceedings Third International Workshop on Automotive and Autonomous Vehicle Security*, https://doi.org/10.14722/autosec.2021.23013

131. Balador A, Cinque E, Pratesi M, Valentini F, Bai C, Gómez AA, Mohammadi M (2022) Survey on decentralized congestion control methods for vehicular communication. *Vehicular Communications*, 33:100394. https://doi.org/10.1016/j.vehcom.2021.100394

132. Bazzi A (2020) Congestion Control Mechanisms in IEEE 802.11p and Sidelink C-V2X. https://doi.org/10.48550/arXiv.2001.08495

133. Wang B, Schultz GG, Macfarlane GS, Eggett DL, Davis MC (2023) A Methodology to Detect Traffic Data Anomalies in Automated Traffic Signal Performance Measures. *Future Transportation*, 3(4):1175–1194. https://doi.org/10.3390/futuretransp3040064

134. Feng Y, Huang SE, Wong W, Chen QA, Mao ZM, Liu HX (2022) On the Cybersecurity of Traffic Signal Control System With Connected Vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 23(9):16267–16279. https://doi.org/10.1109/TITS.2022.3149449

135. Heijden RW van der, Dietzel S, Leinmüller T, Kargl F (2019) Survey on Misbehavior Detection

in Cooperative Intelligent Transportation Systems. *IEEE Communications Surveys & Tutorials*, 21(1):779–811. https://doi.org/10.1109/COMST.2018.2873088

136. Han D, Wang Z, Zhong Y, Chen W, Yang J, Lu S, Shi X, Yin X (2021) Evaluating and Improving Adversarial Robustness of Machine Learning-Based Network Intrusion Detectors. *IEEE Journal on Selected Areas in Communications*, 39(8):2632–2647. https://doi.org/10.1109/JSAC.2021.3087242

137. Liu J, Guo G, Zhang R (2023) Residual-Based Fault Detection and Exclusion With Enhanced Localization Integrity. *IEEE Transactions on Vehicular Technology*, 72(5):5798–5808. https://doi.org/10.1109/TVT.2022.3222416

138. Shen M, Zhao D, Sun J (2016) Enhancement of Low-cost GNSS Localization in Connected Vehicle Networks Using Rao-Blackwellized Particle Filters. https://doi.org/10.48550/arXiv.1606.03736

139. Wang F, Wang X, Hong Y, Tyrrell Rockafellar R, Ban X (Jeff) (2024) Data poisoning attacks on traffic state estimation and prediction. *Transportation Research Part C: Emerging Technologies*, 168:104577. https://doi.org/10.1016/j.trc.2024.104577

140. Chen J, Shi Y (2021) Stochastic model predictive control framework for resilient cyber-physical systems: review and perspectives. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 379(2207):20200371. https://doi.org/10.1098/rsta.2020.0371

141. Singh B, Watson J-P (2018) Chance-Constrained Optimization for Critical Infrastructure Protection. https://doi.org/10.2172/1474266

142. Safe Reach Set Computation via Neural Barrier Certificates. https://arxiv.org/html/2404.18813v1

143. Yu Y, Shan D, Benderius O, Berger C, Kang Y (2022) Formally Robust and Safe Trajectory Planning and Tracking for Autonomous Vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 23(12):22971–22987. https://doi.org/10.1109/TITS.2022.3196623

144. Liu J, Zhou Y, Liu L (2025) Communication delay-aware cooperative adaptive cruise control with dynamic network topologies—A convergence of communication and control. *Digital Communications and Networks*, 11(1):191–199. https://doi.org/10.1016/j.dcan.2023.07.004

145. Validation, Robustness, and Accuracy of Perturbation-Based Sensitivity Analysis Methods for Time-Series Deep Learning Models. https://arxiv.org/html/2401.16521v1

146. Bernardeschi C, Lami G, Merola F, Rossi F (2025) Verifying Robustness of Neural Networks in Vision-Based End-to-End Autonomous Driving. *IEEE Access*, 13:71688–71704. https://doi.org/10.1109/ACCESS.2025.3563120

147. Zheng S, Song Y, Leung T, Goodfellow I (2016) Improving the Robustness of Deep Neural Networks via Stability Training. *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, :4480–4488. https://doi.org/10.1109/CVPR.2016.485

148. Wu B, Wei S, Zhu M, Zheng M, Zhu Z, Zhang M, Chen H, Yuan D, Liu L, Liu Q (2023) Defenses in Adversarial Machine Learning: A Survey. https://doi.org/10.48550/arXiv.2312.08890

149. Raghunathan A, Steinhardt J, Liang P (2020) Certified Defenses against Adversarial Examples. https://doi.org/10.48550/arXiv.1801.09344

150. Liu S, Cullen AC, Montague P, Erfani S, Rubinstein BIP (2025) Multi-level Certified Defense Against Poisoning Attacks in Offline Reinforcement Learning. https://doi.org/10.48550/arXiv.2505.20621

151. Coutinho AC, Araújo LV de (2025) MICRA: A Modular Intelligent Cybersecurity Response Architecture with Machine Learning Integration. *Journal of Cybersecurity and Privacy*, 5(3):60. https://doi.org/10.3390/jcp5030060

152. Adu-Kyere A, Nigussie E, Isoaho J (2023) Self-Aware Cybersecurity Architecture for Autonomous Vehicles: Security through System-Level Accountability. *Sensors*, 23(21):8817. https://doi.org/10.3390/s23218817

153. Gautham S, Rajagopala A, Jayakumar AV, Deloglos C, Karincic E, Elks C (2020) Heterogeneous Runtime Verification of Safety Critical Cyber Physical Systems. https://doi.org/10.48550/arXiv.2009.09533

154. Wu H, Yunas S, Rowlands S, Ruan W, Wahlstrom J (2023) Adversarial Driving: Attacking End-to-End Autonomous Driving. *2023 IEEE Intelligent Vehicles Symposium (IV)*, :1–7. https://doi.org/10.1109/IV55152.2023.10186386

155. Öncü S, Ploeg J, Wouw N van de, Nijmeijer H (2014) Cooperative Adaptive Cruise Control: Network-Aware Analysis of String Stability. *IEEE Transactions on Intelligent Transportation Systems*, 15(4):1527–1537. https://doi.org/10.1109/TITS.2014.2302816

156. Lin G, Qian S, Khattak ZH (2025) FedAV: Federated learning for cyberattack vulnerability and resilience of cooperative driving automation. *Communications in Transportation Research*, 5:100175. https://doi.org/10.1016/j.commtr.2025.100175

157. Pillutla K, Kakade SM, Harchaoui Z (2022) Robust Aggregation for Federated Learning. *IEEE Transactions on Signal Processing*, 70:1142–1154. https://doi.org/10.1109/TSP.2022.3153135

158. Bertsimas D, Sim M (2004) The Price of Robustness. *Operations Research*, 52(1):35–53. https://doi.org/10.1287/opre.1030.0065

159. (2009) Robust Optimization | Princeton University Press. https://press.princeton.edu/books/hardcover/9780691143682/robust-optimization

160. Rahimian H, Mehrotra S (2022) Distributionally Robust Optimization: A Review. *Open Journal of Mathematical Optimization*, 3:1–85. https://doi.org/10.5802/ojmo.15

161. Shapiro A, Dentcheva D, Ruszczynski A (2021) Lectures on Stochastic Programming: Modeling and Theory, Third Edition. https://doi.org/10.1137/1.9781611976595

162. Kosanoglu F, Bier VM (2020) Target-oriented utility for interdiction of transportation networks. *Reliability Engineering & System Safety*, 197:106793. https://doi.org/10.1016/j.ress.2020.106793

163. Bao J, Zheng L, Ban X (Jeff) (2023) Biobjective robust Network-wide traffic signal optimization against Cyber-attacks. *Transportation Research Part C: Emerging Technologies*, 151:104124. https://doi.org/10.1016/j.trc.2023.104124

164. Ouyang M (2014) Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety*, 121:43–60. https://doi.org/10.1016/j.ress.2013.06.040

165. Tambe M (2011) Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned. https://doi.org/10.1017/CBO9780511973031

166. Manshaei MH, Zhu Q, Alpcan T, Bacşar T, Hubaux J-P (2013) Game theory meets network security and privacy. *ACM Comput. Surv.*, 45(3):25:1-25:39. https://doi.org/10.1145/2480741.2480742

167. Zhuang J, Bier VM, Alagoz O (2010) Modeling secrecy and deception in a multiple-period

attacker–defender signaling game. *European Journal of Operational Research*, 203(2):409–418. https://doi.org/10.1016/j.ejor.2009.07.028

168. Ba?ar T, Olsder GJ (1998) Dynamic Noncooperative Game Theory, 2nd Edition. https://doi.org/10.1137/1.9781611971132

169. Zhu Q, Basar T (2015) Game-Theoretic Methods for Robustness, Security, and Resilience of Cyberphysical Control Systems: Games-in-Games Principle for Optimal Cross-Layer Resilient Control Systems. *IEEE Control Systems Magazine*, 35(1):46–65. https://doi.org/10.1109/MCS.2014.2364710

170. Hunt K, Zhuang J (2024) A review of attacker-defender games: Current state and paths forward. *European Journal of Operational Research*, 313(2):401–417. https://doi.org/10.1016/j.ejor.2023.04.009

171. Gu Z, An Y, Tan F, Li Y, Zheng S (2019) A Game Theory Approach to Attack-Defense Strategy for Perception of Connected Vehicles. *2019 IEEE Symposium Series on Computational Intelligence (SSCI)*, :2587–2594. https://doi.org/10.1109/SSCI44817.2019.9002791

172. Hausken K, Welburn JW, Zhuang J (2025) A Review of Game Theory and Risk and Reliability Analysis in Infrastructures and Networks. *Reliability Engineering & System Safety*, 261:111123. https://doi.org/10.1016/j.ress.2025.111123

173. Nilim A, El Ghaoui L (2005) Robust Control of Markov Decision Processes with Uncertain Transition Matrices. *Operations Research*, 53(5):780–798. https://doi.org/10.1287/opre.1050.0216

174. Rios Insua D, Rios J, Banks D (2009) Adversarial Risk Analysis. *Journal of the American Statistical Association*, 104(486):841–854. https://doi.org/10.1198/jasa.2009.0155

175. Birge JR, Louveaux F (2011) Introduction to Stochastic Programming. https://doi.org/10.1007/978-1-4614-0237-4

176. Shafieezadeh A, Ivey Burden L (2014) Scenario-based resilience assessment framework for critical infrastructure systems: Case study for seismic resilience of seaports. *Reliability Engineering & System Safety*, 132:207–219. https://doi.org/10.1016/j.ress.2014.07.021

177. Sheehan B, Murphy F, Mullins M, Ryan C (2019) Connected and autonomous vehicles: A cyber-risk classification framework. *Transportation Research Part A: Policy and Practice*, 124:523–536. https://doi.org/10.1016/j.tra.2018.06.033

178. RESFL: An Uncertainty-Aware Framework for Responsible Federated Learning by Balancing Privacy, Fairness and Utility in Autonomous Vehicles. https://arxiv.org/html/2503.16251v1

179. Doakhan M, Kabganian M, Azimi A (2023) Robust adaptive control for formation-based cooperative transportation of a payload by multi quadrotors. *European Journal of Control*, 69:100763. https://doi.org/10.1016/j.ejcon.2022.100763

180. Pasqualetti F, Dörfler F, Bullo F (2013) Attack Detection and Identification in Cyber-Physical Systems. *IEEE Transactions on Automatic Control*, 58(11):2715–2729. https://doi.org/10.1109/TAC.2013.2266831

181. Naha A, Teixeira A, Ahlén A, Dey S (2023) Quickest physical watermarking-based detection of measurement replacement attacks in networked control systems. *European Journal of Control*, 71:100804. https://doi.org/10.1016/j.ejcon.2023.100804

182. Xie N, Wang H (2025) Distributed adaptive traffic signal control based on shockwave theory. *Transportation Research Part C: Emerging Technologies*, 173:105052.

https://doi.org/10.1016/j.trc.2025.105052

183. Li Z, Zhou Y, Zhang Y, Li X (2024) Enhancing vehicular platoon stability in the presence of communication Cyberattacks: A reliable longitudinal cooperative control strategy. *Transportation Research Part C: Emerging Technologies*, 163:104660. https://doi.org/10.1016/j.trc.2024.104660

184. Haddad J, Mirkin B (2020) Resilient perimeter control of macroscopic fundamental diagram networks under cyberattacks. *Transportation Research Part B: Methodological*, 132:44–59. https://doi.org/10.1016/j.trb.2019.01.020

185. Hodo E, Bellekens X, Hamilton A, Dubouilh P-L, Iorkyase E, Tachtatzis C, Atkinson R (2016) Threat analysis of IoT networks using artificial neural network intrusion detection system. *2016 International Symposium on Networks, Computers and Communications (ISNCC)*, :1–6. https://doi.org/10.1109/ISNCC.2016.7746067

186. Kang M-J, Kang J-W (2016) Intrusion Detection System Using Deep Neural Network for In-Vehicle Network Security. *PLOS ONE*, 11(6):e0155781. https://doi.org/10.1371/journal.pone.0155781

187. Wazid M, Singh J, Pandey C, Sherratt RS, Das AK, Giri D, Park Y (2025) Explainable Deep Learning-Enabled Malware Attack Detection for IoT-Enabled Intelligent Transportation Systems. *IEEE Transactions on Intelligent Transportation Systems*, 26(5):7231–7244. https://doi.org/10.1109/TITS.2025.3525505

188. Barreno M, Nelson B, Joseph AD, Tygar JD (2010) The security of machine learning. *Machine Learning*, 81(2):121–148. https://doi.org/10.1007/s10994-010-5188-5

189. Guldemir NH, Olukoya O, Martínez-del-Rincón J (2025) Addressing malware family concept drift with triplet autoencoder. https://doi.org/10.48550/arXiv.2507.00348

190. Ahmed M, Naser Mahmood A, Hu J (2016) A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, 60:19–31. https://doi.org/10.1016/j.jnca.2015.11.016

191. Erfani SM, Rajasegarar S, Karunasekera S, Leckie C (2016) High-dimensional and large-scale anomaly detection using a linear one-class SVM with deep learning. *Pattern Recognition*, 58:121–134. https://doi.org/10.1016/j.patcog.2016.03.028

192. Fuentes J, Ortega-Fernandez I, Villanueva NM, Sestelo M (2025) Cybersecurity threat detection based on a UEBA framework using Deep Autoencoders. https://doi.org/10.48550/arXiv.2505.11542

193. Bilot T, Madhoun NE, Agha KA, Zouaoui A (2024) Few Edges Are Enough: Few-Shot Network Attack Detection with Graph Neural Networks. 14977:257–276. https://doi.org/10.1007/978-981-97-7737-2_15

194. Sathishkumar P, Nikitha S, Sruthi R, Vishwa RR (2025) Anomaly Detection in Network Security Using Unsupervised Graph Neural Network. *2025 International Conference on Advanced Computing Technologies (ICoACT)*, :1–7. https://doi.org/10.1109/ICoACT63339.2025.11004728

195. Phan TV, Bauschert T (2022) DeepAir: Deep Reinforcement Learning for Adaptive Intrusion Response in Software-Defined Networks. *IEEE Transactions on Network and Service Management*, 19(3):2207–2218. https://doi.org/10.1109/TNSM.2022.3158468

196. Yang W, Acuto A, Zhou Y, Wojtczak D (2024) A Survey for Deep Reinforcement Learning Based Network Intrusion Detection. https://doi.org/10.48550/arXiv.2410.07612

197. Qiao Z, Xiang Y, Baker T, Li G, Wu Y, Tong E, Peng S, Zhu Y, Xu D, Niu W (2024) Reinforcement Learning-Based Security Enhancement for Controlled Optimization of Phases in Intelligent Traffic Signal System. *IEEE Transactions on Industrial Cyber-Physical Systems*, 2:575–587.

https://doi.org/10.1109/TICPS.2024.3476455

198. Haydari A, Zhang M, Chuah C-N (2021) Adversarial Attacks and Defense in Deep Reinforcement Learning (DRL)-Based Traffic Signal Controllers. *IEEE Open Journal of Intelligent Transportation Systems*, 2:402–416. https://doi.org/10.1109/OJITS.2021.3118972

199. Deshpande RD, Khan FA, Ahmed QZ (2024) Spectrum Sharing using Deep Reinforcement Learning in Vehicular Networks. https://doi.org/10.48550/arXiv.2410.12521

200. Huang S, Papernot N, Goodfellow I, Duan Y, Abbeel P (2017) Adversarial Attacks on Neural Network Policies. https://doi.org/10.48550/arXiv.1702.02284

201. Creswell A, White T, Dumoulin V, Arulkumaran K, Sengupta B, Bharath AA (2018) Generative Adversarial Networks: An Overview. *IEEE Signal Processing Magazine*, 35(1):53–65. https://doi.org/10.1109/MSP.2017.2765202

202. Lim W, Yong KSC, Lau BT, Tan CCL (2024) Future of generative adversarial networks (GAN) for anomaly detection in network security: A review. *Computers & Security*, 139:103733. https://doi.org/10.1016/j.cose.2024.103733

203. Li Y, Xiang Y, Tong E, Niu W, Jia B, Li L, Liu J, Han Z (2020) An Empirical Study on GAN-Based Traffic Congestion Attack Analysis: A Visualized Method. *Wireless Communications and Mobile Computing*, 2020(1):8823300. https://doi.org/10.1155/2020/8823300

204. Liu Z, Wang Q, Ye Y, Tang Y (2022) A GAN-Based Data Injection Attack Method on Data-Driven Strategies in Power Systems. *IEEE Transactions on Smart Grid*, 13(4):3203–3213. https://doi.org/10.1109/TSG.2022.3159842

205. Ankalaki S, Atmakuri AR, Pallavi M, Hukkeri GS, Jan T, Naik GR (2025) Cyber Attack Prediction: From Traditional Machine Learning to Generative Artificial Intelligence. *IEEE Access*, 13:44662–44706. https://doi.org/10.1109/ACCESS.2025.3547433

206. Sen MA (2024) Attention-GAN for Anomaly Detection: A Cutting-Edge Approach to Cybersecurity Threat Management. https://doi.org/10.48550/arXiv.2402.15945

207. Yang Y, Zhang B, Guo D, Du H, Xiong Z, Niyato D, Han Z (2024) Generative AI for Secure and Privacy-Preserving Mobile Crowdsensing. *IEEE Wireless Communications*, 31(6):29–38. https://doi.org/10.1109/MWC.004.2400017

208. Metta S, Chang I, Parker J, Roman MP, Ehuan AF (2024) Generative AI in Cybersecurity. https://doi.org/10.48550/arXiv.2405.01674

209. Usman Y, Upadhyay A, Gyawali P, Chataut R (2024) Is Generative AI the Next Tactical Cyber Weapon For Threat Actors? Unforeseen Implications of AI Generated Cyber Attacks. https://doi.org/10.48550/arXiv.2408.12806

210. Zhao P, Zhu W, Jiao P, Gao D, Wu O (2025) Data Poisoning in Deep Learning: A Survey. https://doi.org/10.48550/arXiv.2503.22759

211. Ayub MdA, Johnson WA, Talbert DA, Siraj A (2020) Model Evasion Attack on Intrusion Detection Systems using Adversarial Machine Learning. *2020 54th Annual Conference on Information Sciences and Systems (CISS)*, :1–6. https://doi.org/10.1109/CISS48834.2020.1570617116

212. Muthalagu R, Malik J, Pawar PM (2025) Detection and prevention of evasion attacks on machine learning models. *Expert Systems with Applications*, 266:126044. https://doi.org/10.1016/j.eswa.2024.126044

213. Fredrikson M, Jha S, Ristenpart T (2015) Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, :1322–1333. https://doi.org/10.1145/2810103.2813677

214. Shokri R, Stronati M, Song C, Shmatikov V (2017) Membership Inference Attacks Against Machine Learning Models. *2017 IEEE Symposium on Security and Privacy (SP)*, :3–18. https://doi.org/10.1109/SP.2017.41

215. Tekgul BGA, Wang S, Marchal S, Asokan N (2022) Real-time Adversarial Perturbations against Deep Reinforcement Learning Policies: Attacks and Defenses. https://doi.org/10.48550/arXiv.2106.08746

216. Carlini N, Tramer F, Wallace E, Jagielski M, Herbert-Voss A, Lee K, Roberts A, Brown T, Song D, Erlingsson U, Oprea A, Raffel C (2021) Extracting Training Data from Large Language Models. https://doi.org/10.48550/arXiv.2012.07805

217. Shor PW (1997) Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 26(5):1484–1509. https://doi.org/10.1137/S0097539795293172

218. Mosca M (2018) Cybersecurity in an Era with Quantum Computers: Will We Be Ready? *IEEE Security & Privacy*, 16(5):38–41. https://doi.org/10.1109/MSP.2018.3761723

219. Chen L, Jordan S, Liu Y-K, Moody D, Peralta R, Perlner R, Smith-Tone D (2016) Report on Post-Quantum Cryptography. :NIST IR 8105. https://doi.org/10.6028/NIST.IR.8105

220. Alkim E, Ducas L, Pöppelmann T, Schwabe P (2015) Post-quantum key exchange - a new hope. https://eprint.iacr.org/2015/1092

221. Nejatollahi H, Dutt N, Ray S, Regazzoni F, Banerjee I, Cammarota R (2019) Post-Quantum Lattice-Based Cryptography Implementations: A Survey. *ACM Comput. Surv.*, 51(6):129:1-129:41. https://doi.org/10.1145/3292548

222. (2009) Post-Quantum Cryptography. https://doi.org/10.1007/978-3-540-88702-7

223. Chen Z, Ma Y, Jing J (2023) Low-Cost Shuffling Countermeasures Against Side-Channel Attacks for NTT-Based Post-Quantum Cryptography. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 42(1):322–326. https://doi.org/10.1109/TCAD.2022.3174142

224. Ravi P, Chattopadhyay A, D'Anvers JP, Baksi A (2024) Side-channel and Fault-injection attacks over Lattice-based Post-quantum Schemes (Kyber, Dilithium): Survey and New Results. *ACM Trans. Embed. Comput. Syst.*, 23(2):35:1-35:54. https://doi.org/10.1145/3603170

225. Bennett CH, Brassard G (2014) Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11. https://doi.org/10.1016/j.tcs.2014.05.025

226. Lee C, Sohn I, Lee W (2022) Eavesdropping Detection in BB84 Quantum Key Distribution Protocols. *IEEE Transactions on Network and Service Management*, 19(3):2689–2701. https://doi.org/10.1109/TNSM.2022.3165202

227. Xu F, Ma X, Zhang Q, Lo H-K, Pan J-W (2020) Secure quantum key distribution with realistic devices. *Reviews of Modern Physics*, 92(2):025002. https://doi.org/10.1103/RevModPhys.92.025002

228. Shi Q, Yang Z, Cheng T, Wang C, Wu Z, Zhang X, Xu P (2024) QKBAKA: A Quantum-Key-Based Authentication and Key Agreement Scheme for Internet of Vehicles. *IEEE Internet of Things Journal*, 11(7):12292–12306. https://doi.org/10.1109/JIOT.2023.3332947

229. Cheng T, Liu Q, Shi Q, Yang Z, Wang C, Zhang X, Xu P (2024) Efficient Anonymous Authentication and Group Key Distribution Scheme Based on Quantum Random Numbers for VANETs. *IEEE Internet of Things Journal*, 11(13):23544–23560. https://doi.org/10.1109/JIOT.2024.3384993

230. Ahilan A, Jeyam A (2023) Breaking Barriers in Conventional Cryptography by Integrating with Quantum Key Distribution. *Wireless Personal Communications*, 129(1):549–567. https://doi.org/10.1007/s11277-022-10110-8

231. Diamanti E, Lo H-K, Qi B, Yuan Z (2016) Practical challenges in quantum key distribution. *npj Quantum Information*, 2(1):16025. https://doi.org/10.1038/npjqi.2016.25

232. Zeng P, Bandyopadhyay D, Méndez JAM, Bitner N, Kolar A, Solomon MT, Ye Z, Rozpędek F, Zhong T, Heremans FJ, Awschalom DD, Jiang L, Liu J (2024) Practical hybrid PQC-QKD protocols with enhanced security and performance. https://doi.org/10.48550/arXiv.2411.01086

233. Blekos K, Brand D, Ceschini A, Chou C-H, Li R-H, Pandya K, Summer A (2024) A review on Quantum Approximate Optimization Algorithm and its variants. *Physics Reports*, 1068:1–66. https://doi.org/10.1016/j.physrep.2024.03.002

234. Rajak A, Suzuki S, Dutta A, Chakrabarti BK (2023) Quantum Annealing: An Overview. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 381(2241):20210417. https://doi.org/10.1098/rsta.2021.0417

235. Chicano F, Luque G, Dahi ZA, Gil-Merino R (2025) Combinatorial Optimization with Quantum Computers. *Engineering Optimization*, 57(1):208–233. https://doi.org/10.1080/0305215X.2024.2435538

236. Corli S, Moro L, Dragoni D, Dispenza M, Prati E (2025) Quantum machine learning algorithms for anomaly detection: A review. *Future Generation Computer Systems*, 166:107632. https://doi.org/10.1016/j.future.2024.107632

237. Hdaib M, Rajasegarar S, Pan L (2024) Quantum deep learning-based anomaly detection for enhanced network security. *Quantum Machine Intelligence*, 6(1):26. https://doi.org/10.1007/s42484-024-00163-2

238. Shakib KH, Rahman M, Islam M, Chowdhury M (2025) Impersonation Attack Using Quantum Shor's Algorithm Against Blockchain-Based Vehicular Ad-Hoc Network. *IEEE Transactions on Intelligent Transportation Systems*, 26(5):6530–6544. https://doi.org/10.1109/TITS.2025.3534656

239. Yocam E, Rizi A, Kamepalli M, Vaidyan V, Wang Y, Comert G (2024) Quantum Adversarial Machine Learning and Defense Strategies: Challenges and Opportunities. https://doi.org/10.48550/arXiv.2412.12373

240. Edwards D, Rawat DB (2020) Quantum Adversarial Machine Learning: Status, Challenges and Perspectives. *2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, :128–133. https://doi.org/10.1109/TPS-ISA50397.2020.00026

241. Wellens-Miles C, Guo R, Liu N, Parkinson S, Vallati M (2025) A Systematic Literature Review of Simulated Cyber Attacks on Vehicles and Urban Traffic Control. *IEEE Transactions on Intelligent Transportation Systems*, :1–0. https://doi.org/10.1109/TITS.2025.3576922

242. Herman Muraro Gularte K, Paulo Javidi da Costa J, Vargas JAR, Santos da Silva A, Almeida Santos G, Wang Y, Alfons Müller C, Lipps C, Timóteo de Sousa R, Britto Vidal Filho W de, Slusallek P, Dieter Schotten H (2024) Integrating Cybersecurity in V2X: A Review of Simulation Environments. *IEEE Access*, 12:177946–177985. https://doi.org/10.1109/ACCESS.2024.3504404

243. Fuller A, Fan Z, Day C, Barlow C (2020) Digital Twin: Enabling Technologies, Challenges and Open Research. *IEEE Access*, 8:108952–108971. https://doi.org/10.1109/ACCESS.2020.2998358

244. Qureshi AR, Asensio A, Imran M, Garcia J, Masip-Bruin X (2025) A survey on security enhancing Digital Twins: Models, applications and tools. *Computer Communications*, 238:108158. https://doi.org/10.1016/j.comcom.2025.108158

245. Yigit Y, Panitsas I, Maglaras L, Tassiulas L, Canberk B (2024) Cyber-Twin: Digital Twin-Boosted Autonomous Attack Detection for Vehicular Ad-Hoc Networks. *ICC 2024 - IEEE International Conference on Communications*, :2167–2172. https://doi.org/10.1109/ICC51166.2024.10622784

246. Dasgupta S, Rahman M, Jon S (2024) Harnessing Digital Twin Technology for Adaptive Traffic Signal Control: Improving Signalized Intersection Performance and User Satisfaction. *IEEE Internet of Things Journal*, 11(22):36596–36618. https://doi.org/10.1109/JIOT.2024.3420439

247. Wang Z, Han K, Tiwari P (2022) Digital Twin-Assisted Cooperative Driving at Non-Signalized Intersections. *IEEE Transactions on Intelligent Vehicles*, 7(2):198–209. https://doi.org/10.1109/TIV.2021.3100465

248. Kloock M, Scheffe P, Gress O, Alrifaee B (2023) An Architecture for Experiments in Connected and Automated Vehicles. *IEEE Open Journal of Intelligent Transportation Systems*, 4:175–186. https://doi.org/10.1109/OJITS.2023.3250951

249. Yang B, Guo L, Ye J (2020) Real-time Simulation of Electric Vehicle Powertrain: Hardware-in-the-Loop (HIL) Testbed for Cyber-Physical Security. *2020 IEEE Transportation Electrification Conference & Expo (ITEC)*, :63–68. https://doi.org/10.1109/ITEC48692.2020.9161525

250. Goppert J, Shull A, Sathyamoorthy N, Liu W, Hwang I, Aldridge H (2014) Software/Hardware-in-the-Loop Analysis of Cyberattacks on Unmanned Aerial Systems. *Journal of Aerospace Information Systems*, 11(5):337–343. https://doi.org/10.2514/1.I010114

251. Potteiger B, Emfinger W, Neema H, Koutosukos X, Tang C, Stouffer K (2017) Evaluating the effects of cyber-attacks on cyber physical systems using a hardware-in-the-loop simulation testbed. *2017 Resilience Week (RWS)*, :177–183. https://doi.org/10.1109/RWEEK.2017.8088669

252. Behrens T, Heinrich L, Pannek J (2025) Model-Based Development of a Hardware-in-the-Loop Setup for Assessing Cybersecurity of Vehicle-to-Robot Communication. *2025 IEEE Intelligent Vehicles Symposium (IV)*, :801–806. https://doi.org/10.1109/IV64158.2025.11097423

253. Ukwandu E, Farah MAB, Hindy H, Brosset D, Kavallieros D, Atkinson R, Tachtatzis C, Bures M, Andonovic I, Bellekens X (2020) A Review of Cyber-Ranges and Test-Beds: Current and Future Trends. *Sensors*, 20(24):7148. https://doi.org/10.3390/s20247148

254. Shin Y, Kwon H, Jeong J, Shin D (2024) A Study on Designing Cyber Training and Cyber Range to Effectively Respond to Cyber Threats. *Electronics*, 13(19):3867. https://doi.org/10.3390/electronics13193867

255. Urias VE, Stout WMS, Van Leeuwen B, Lin H (2018) Cyber Range Infrastructure Limitations and Needs of Tomorrow: A Position Paper. *2018 International Carnahan Conference on Security Technology (ICCST)*, :1–5. https://doi.org/10.1109/CCST.2018.8585460

256. V2X-Real: a Large-Scale Dataset for Vehicle-to-Everything Cooperative Perception. https://arxiv.org/html/2403.16034v2

257. Bari BS, Puthal D, Yelamarthi K (2025) Datasets in Vehicular Communication Systems: A Review of Current Trends and Future Prospects. *SN Computer Science*, 6(3):210.

https://doi.org/10.1007/s42979-025-03736-5

258. Zhang Q, Wang Y, Zhang X, Liu L, Wu X, Shi W, Zhong H (2018) OpenVDAP: An Open Vehicular Data Analytics Platform for CAVs. *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, :1310–1320. https://doi.org/10.1109/ICDCS.2018.00131

259. Kujala R, Weckström C, Darst RK, Mladenović MN, Saramäki J (2018) A collection of public transport network data sets for 25 cities. *Scientific Data*, 5(1):180089. https://doi.org/10.1038/sdata.2018.89

260. Kott A, Linkov I (2021) To Improve Cyber Resilience, Measure It. https://doi.org/10.48550/arXiv.2102.09455

261. Linkov I, Eisenberg DA, Plourde K, Seager TP, Allen J, Kott A (2013) Resilience metrics for cyber systems. *Environment Systems and Decisions*, 33(4):471–476. https://doi.org/10.1007/s10669-013-9485-y

262. Lezzi M, Corallo A, Lazoi M, Nimis A (2025) Measuring cyber resilience in industrial IoT: a systematic literature review. *Management Review Quarterly*, https://doi.org/10.1007/s11301-025-00495-8

263. Clark A, Zonouz S (2019) Cyber-Physical Resilience: Definition and Assessment Metric. *IEEE Transactions on Smart Grid*, 10(2):1671–1684. https://doi.org/10.1109/TSG.2017.2776279