Secure Systems Design and Technology Development. Veliko Tarnovo, Bulgaria
Proceedings of the International Scientific Conference, 2026. Volume III, 73-81

Cybersecurity Threats in Intelligent Transport Systems: Challenges and Solution Pathways

Dimitar Dimitrov
Faculty of Transport Management
University of Transport
Sofia, Bulgaria
ddimitrov@vtu.bg

Krassimir Lalov
Faculty of Transport Management
University of Transport
Sofia, Bulgaria
klalov@vtu.bg

Ivan Manchev
Faculty of Transport Management
University of Transport
Sofia, Bulgaria
imanchev@vtu.bg

Irena Petrova
Faculty of Transport Management
University of Transport
Sofia, Bulgaria
ipetrova@vtu.bg

***Abstract* — The rapid integration of Intelligent Transport Systems (ITS) into urban and interurban mobility has significantly improved efficiency, safety, and automation in transport operations. Nevertheless, the extensive connectivity enabled by vehicle-to-everything (V2X) communications, Internet of Things (IoT) devices, and cloud services has also increased exposure to cyber threats. The primary scientific challenge is that compromising Cooperative ITS (C-ITS) can enable manipulation of critical transport functions, such as automated control, braking, and signaling, through falsified or maliciously injected communication messages. The increasing frequency of distributed denial-of-service (DDoS) attacks exacerbates this vulnerability, as these attacks account for most publicly recorded incidents worldwide and directly affect the transportation sector. Furthermore, ransomware and supply-chain attacks have led to a marked increase in system breaches and significant financial losses.**

IoT devices widely deployed within ITS often use inadequately secured communication protocols, creating opportunities for remote intrusion and infrastructure compromise. Simultaneously, Artificial Intelligence (AI) functions as a dual-use technology, facilitating both cyber-attacks, such as automated phishing, adaptive threat generation, and vulnerability analysis, and defense through the deployment of anomaly detection models. Additional risk arises from adversarial attacks that can mislead AI models in autonomous vehicles, thereby undermining real-time decision-making processes.

Proposed solutions include integrating international standards, such as ISO/SAE 21434 and the NIST Cybersecurity Framework; applying cryptographic protection to V2X communications; implementing hybrid intrusion detection systems; and adopting lifecycle-oriented risk management across ITS infrastructures. AI-based predictive analytics and anomaly detection are identified as critical approaches to enhancing cyber resilience. Ongoing coordination among operators, vendors, and public institutions is essential to mitigate systemic risks and protect the integrity of ITS environments.

Keywords—Intelligent Transport Systems, Cybersecurity Threats, Internet of Things (IoT), vehicle-to-everything (V2X), Artificial Intelligence.

I. INTRODUCTION

Intelligent Transport Systems (ITS) integrate digital, communication, and control technologies to enhance the safety, efficiency, and sustainability of transportation. Modern ITS operates as a complex cyber-physical system, combining the Internet of Things (IoT), vehicle-to-everything (V2X) communications, and Artificial Intelligence (AI) to collect and process large volumes of real-time data. While this digitalization improves transportation infrastructure, it also introduces unpredictable cybersecurity threats that may seriously impact public safety and critical infrastructure [1], [2].

The rapid growth of IoT devices in intelligent transport systems, including smart sensors, road infrastructure, on-board computers, and edge network elements, significantly expands the attack surface. Heterogeneous devices, limited computing resources, and the lack of standardized defense mechanisms make these systems particularly vulnerable to threats that compromise data integrity, privacy, and

Online ISSN 3044-7771
https://doi.org/10.68302/std2026.vol3.138

availability. Studies indicate that traditional cryptographic methods often fail to address modern threats such as distributed denial-of-service (DDoS) attacks, data tampering, malicious device management, and zero-day attacks in large-scale IoT environments [3], [4].

Vehicle-to-everything (V2X) communications are critical to cybersecurity. V2X enables vehicles, infrastructure, pedestrians, and network services to exchange information, supporting automated traffic management, incident prevention, and autonomous transport. However, V2X remains vulnerable to attacks such as spoofing, Sybil, replay, and route manipulation, which can disrupt real-time decision-making and lead to physical incidents. Literature reviews highlight the lack of unified security architecture and effective trust management as major challenges for V2X systems [5], [6].

Artificial intelligence is becoming a key tool for strengthening the cyber resilience of ITS. Techniques such as machine learning, deep neural networks, and federated learning support anomaly detection, trust management, attack prediction, and automated incident response. Studies indicate that AI significantly improves detection of complex, adaptive attacks in dynamic transport networks, where static defenses are often insufficient [7], [8].

Although significant progress has been made, integrating artificial intelligence into Intelligent Transport Systems (ITS) cybersecurity poses challenges related to model interpretability, data quality, and resilience to adversarial attacks. Addressing these issues requires a comprehensive, interdisciplinary strategy that incorporates technological, architectural, and managerial solutions. Consequently, systematic research into cybersecurity threats within Intelligent Transport Systems is crucial for developing reliable, safe, and sustainable transport services amid ongoing digital transformation [1], [9].

II. ITS Working Model

ITS is vital for efficient transportation infrastructure, improving road safety, and reducing environmental impact. By integrating IoT, big data, and artificial intelligence, ITS processes large volumes of data in real time to optimize traffic, monitor road conditions, and support vehicle-to-infrastructure communication. However, increased reliance on digital technologies also raises the risk of cyberattacks, technical failures, and network anomalies. To better understand ITS operations and protection strategies, it is helpful to review the Intelligent Transport System model, which includes three main components: the ITS architecture level, the integrated management level, and the ITS security levels [2]. Formula 1 and Figure 1 present this model.

$$ITS\ Working\ Model = f(Integrated\ Management\ Level,\ ITS\ Architecture\ Level,\ ITS\ Security\ Level) \rightarrow max \quad (1)$$

A. Integrated Management Level

This component comprises two modules: the Analytical Level and the Management and Integration Level. The Analytical Level processes large volumes of data from sensors and communication systems using advanced machine learning algorithms. It analyzes both structured and unstructured data, including video streams, sensor signals, and event logs, to detect anomalies and support transport optimization decisions.

Key functions include analyzing historical and real-time data to predict scenarios such as traffic congestion, adapting system behavior, optimizing resource allocation, detecting abnormal activity, and modeling risks related to weather, accidents, or cyberattacks. The Analytical Level works closely with the Computing Layer, which supplies processed data, and the Management Layer, which uses analytical results to inform decisions. For example, traffic forecasts can be sent to traffic light control systems for dynamic adjustments or provided to drivers through user interfaces.

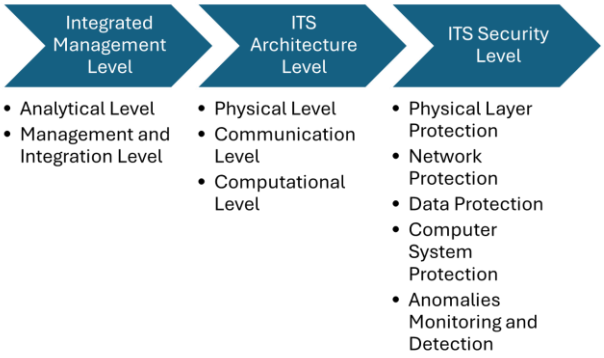

Fig. 1. ITS Working Model

The Management and Integration Level coordinates interactions among users, control systems, and infrastructure components, enabling real-time strategic management of the transport network. Its primary role is to synchronize all system components to optimize efficiency, safety, and convenience. This layer aggregates data from the physical, communication, computing, and analytical layers to formulate and implement optimization decisions. For example, if traffic increases in a specific area, the system can reroute vehicles to alternative routes.

The Management Layer also integrates with other infrastructure elements: it manages charging stations and electric-vehicle energy consumption, transmits data to emergency services during incidents, and monitors vehicle emissions to minimize environmental impact. Effective governance and integration are essential to building reliable, adaptable transport systems that operate efficiently in complex urban environments.

B. Architecture Level

The physical layer forms the foundation of the ITS architecture, encompassing infrastructure such as roads, bridges, tunnels, traffic lights, parking meters, sensors, and IoT devices [10]. This layer collects data on traffic flows, road conditions, and weather. IoT devices are essential for continuous monitoring and data transmission. For example, traffic sensors measure flow and speed, weather sensors monitor environmental conditions, GPS trackers provide real-time vehicle positioning, and video cameras assess traffic conditions and detect violations or emergencies.

The physical layer also interacts with other system layers. Traffic sensors and signals can adjust in real time based on traffic volume, while V2I technologies provide vehicles with traffic, accident, and speed-limit information. Key challenges at this level include ensuring the reliability of IoT devices under adverse conditions [11], maintaining comprehensive real-time monitoring, and protecting against physical attacks or unauthorized access.

Data collected at this layer is transmitted to the communication layer for processing, and video streams are analyzed at the analytical layer to detect violations. This information supports management decisions on traffic optimization and emergency response. The communication layer enables data transfer among all ITS components. Its goal is to provide efficient, reliable, and secure information exchange among physical devices, computing centers, and users, using wireless protocols (Wi-Fi, 5G, V2X), fiber-optic lines, and satellite systems [12].

This layer enables low-latency, real-time data exchange, transmitting information from traffic lights, sensors, and vehicles for processing and analysis. It integrates technologies via protocols such as V2X for data exchange among vehicles, infrastructure, pedestrians, and cloud platforms; 5G for high bandwidth and minimal latency; and fiber-optic networks for high-speed transmission between data centers.

Challenges include minimizing transmission delays, securing data against interception or tampering, and supporting diverse devices and protocols with varying technical standards. Reliable communication is essential for system coordination and underpins the analytics and control layers. Fast, accurate data exchange enables machine learning algorithms to detect anomalies or predict congestion and provides users with current traffic information.

The computational layer provides the system's processing power, including servers, cloud platforms, and data centers where collected data is analyzed. It runs artificial intelligence algorithms for traffic prediction and resource management. Sensor data, such as vehicle speed and road conditions, is sent to computing platforms for rapid analysis, and results are delivered to the analytical layer or directly to control devices. Machine learning and AI algorithms at this level support traffic flow analysis, congestion prediction, and emergency detection. The computational layer links the physical, communication, and analytical layers by receiving, processing, and transmitting data for further analysis.

C. Security Level

Intelligent transport systems are vulnerable to cyberattacks and technical failures, making multi-layered protection essential. Key protection levels include: Physical Layer Protection, which secures equipment and sensors and restricts access to authorized personnel through surveillance and other measures; Network Protection, which employs firewalls, VPNs, traffic encryption, and secure communication protocols such as V2X to prevent unauthorized access and mitigate DDoS risks; Data Protection, which uses encryption, user authentication, and access controls to reduce data leakage and privacy breaches; Protection of Computer Systems, which involves regular software updates, server monitoring, intrusion detection systems, and cloud security through access controls and backup policies; and Anomaly Detection, which uses real-time algorithms to identify and respond to suspicious network activity. To assess risks and maintain ITS stability, probabilistic mathematical models estimate the likelihood of threats and anomalies. These models incorporate historical and current data, supporting accurate prediction of potential issues. Estimating the probability of cyberattacks relies on threat probability functions that account for time-dependent risks. Exponential and Weibull distributions help model both constant and changing risks, reflecting factors such as vulnerability accumulation or the impact of security measures. Anomaly detection in network traffic is also critical, using machine learning algorithms and Bayes' theorem to estimate the probability of anomalies based on current traffic patterns. This approach considers both normal and abnormal system behavior. Integrating these methods into the monitoring process enables a comprehensive security system that addresses both global risks, such as cyberattacks, and local network anomalies. This is increasingly important as the complexity of ITS and the number of connected devices continue to grow.

D. Challenges to the development of ITS

As intelligent transport systems grow more complex, real-time data processing becomes essential. Effective threat-response automation requires coordination among ITS components, including traffic control centers, self-driving vehicles, and infrastructure sensors. Machine learning algorithms detect deviations from normal behavior, which is vital for preventing cyberattacks. Reliable data and robust cybersecurity protocols are crucial for system reliability. Current ITS cybersecurity relies on hybrid models that integrate statistical methods, machine learning, and predictive analysis. Ongoing research should further develop these models and algorithms to strengthen risk management and cybersecurity in ITS.

III. ITS CYBERSECURITY THREATS AND REQUIREMENTS

Intelligent Transport Systems integrate IoT devices, V2X communications, and AI-based controls, introducing a range of cybersecurity threats. Recent literature typically classifies these threats using a functional–architectural approach:

TABLE I. CLASSIFICATION OF CYBERSECURITY THREATS IN ITS

Layer / Component	Threat Type	Description and Impact	Ref
IoT layer	Device compromise	Insufficiently secured sensors and edge devices enable unauthorized access, data tampering, and malware injection	[3], [4]

	Botnet / DDoS attacks	Large-scale compromise of IoT nodes used to launch denial-of-service attacks against transport services	[2]
V2X communications	Spoofing and Sybil attacks	Injection of falsified messages and identities, leading to incorrect safety and traffic management decisions	[5], [6]
	Replay attacks	Re-transmission of legitimate V2X messages to manipulate vehicle and infrastructure behavior	[5]
Network layer	Man-in-the-Middle (MitM)	Eavesdropping and manipulation of data exchanged between vehicles and infrastructure	[5]
Application layer	Data injection attacks	Manipulation of input data used by traffic control systems and AI-driven decision mechanisms	[7]
AI components	Adversarial attacks against models	Malicious inputs designed to mislead AI models and cause incorrect predictions or control actions	[8]
	Data poisoning	Intentional contamination of training datasets degrades the performance and reliability of AI systems	[7]
System level	Privacy breaches	Leakage of sensitive location and personal data of transport system users	[1], [3]

Table 1 shows that cybersecurity threats in ITS can cause physical and safety-related impacts, not just digital consequences. This distinguishes Intelligent Transport Systems from traditional IT infrastructure.

A. Emerging V2X Applications and Challenges

V2X systems exhibit certain peculiarities in deployment options and data traffic characteristics compared with traditional network applications.

TABLE II. V2X APPLICATION CATEGORIES AND ASSOCIATED QOS REQUIREMENTS.

Application	Use cases	Connectivity mode(s)
Road safety	•Collision warning Road safety •Vehicle status warning •Vehicle type warning	V2V, V2I
Traffic management	•Speed limit notification •Vehicle tracking •Traffic flow control	V2I, V2N
Comfort and infotainment	•In-vehicle Internet access •Point of interest alerts •Parking booking	V2I, V2N
Autonomous driving	•Advanced driving •Remote driving •Vehicle platooning	V2V, V2I V2N V2V, V2I

V2X systems span a wide range of network scenarios and support vehicular services with diverse QoS requirements. Specifically, four prevalent classes of emerging V2X applications can be identified within the ITS domain: road safety, traffic management, comfort and infotainment, and autonomous driving, as defined in [13].

Table II outlines the main V2X application categories and example use cases for each. Latency, data rate, and message transmission reliability are key performance indicators (KPIs) for road safety and mobility applications.

B. Security and Privacy Requirements

The primary goal of V2X communication systems is to improve road safety and traffic flow by facilitating targeted information exchange between vehicles and road infrastructure. In safety-critical situations, event-driven warning notifications (such as DENMs or BSMs) are activated to alert drivers, and authorized users must reliably access these notifications. The receiving vehicle must confirm that the message originates from an authentic source. These mechanisms emphasize three fundamental security elements: availability, message integrity, and authenticity [14]. Security risks, such as compromised vehicles transmitting fabricated alerts or adversaries generating counterfeit messages, can seriously impair system operation. These risks are particularly significant in V2X scenarios within C-ITS, including vehicle platooning, cooperative collision avoidance, dynamic map dissemination, and remote driving. Attacks against V2X communication protocols like IEEE 802.11p and C-V2X are increasingly sophisticated [15], [16], [17]. Therefore, it is essential to fulfill critical security and privacy requirements to sustain a secure ITS environment and reduce cybersecurity vulnerabilities. These requirements may differ depending on the sensitivity of the ITS application [18] and the tactics employed to counter specific threats. The subsequent sections deliver a concise summary of V2X security and privacy requirements.

Authentication: This process distinguishes legitimate entities from malicious ones in V2X communication and verifies the sender's identity. This enables unique participant identification and verification [19]. The process comprises user authentication, which confirms device legitimacy, and message authentication, which ensures messages originate from valid sources and remain unaltered.

Authorization: This function manages access to V2X services, ensuring that only verified entities receive the appropriate privileges. Authorization is governed by explicit rules and policies that control access to designated services.

Availability: This guarantees authorized users have continuous access to V2X messages and services. Availability safeguards system operation during disruptions, such as denial-of-service attacks, so authorized entities can access the network without interruption.

Confidentiality: This restricts access to V2X message content to designated recipients, preventing unauthorized interception. Confidentiality is commonly delivered through encryption with shared keys. Although most V2X data is public and does not demand strict confidentiality [20], it is vital to prevent data correlation that might expose user identity or location.

Integrity and Data Trust: This upholds the exchange of accurate, consistent, and promptly verifiable information among V2X entities. V2X systems must deploy

mechanisms that uncover and block data manipulation by malicious actors.

Privacy: Safeguarding V2X user identities prevents vehicle tracking and protects sensitive information. Exposing private data can enable systemic attacks and jeopardize user assets. Privacy can be preserved through anonymization or data obfuscation [21], such as assigning vehicles pseudonyms to conceal their identities. Additional privacy requirements, including anonymity, unlinkability, and unobservability, must be maintained through rigorous security practices and policies [20].

IV. Security Threats and Attacks Other

This section presents a comprehensive analysis of threats and attacks that can compromise V2X networks, along with a classification of malicious attacks documented in the literature.

A. Attack Surface Overview

The attack surface comprises all potential vulnerable entry points that may compromise the security of a V2X system and serve as sources for adversarial attacks or malicious incidents. Examples include in-vehicle user devices such as USB, Wi-Fi, and Bluetooth within infotainment systems, as well as vehicle sensors. As vehicle automation advances, the number of electronic components in in-vehicle networks increases, expanding the attack surface for elements such as electronic control units (ECUs) and the control area network [22]. The study in [23] systematically analyzes various threat vectors within vehicles, including Bluetooth, cellular, WiFi, and RFIDs, and experimentally demonstrates that in-vehicle ECUs are susceptible to remote attacks. The deployment of cooperative intelligent transport systems (C-ITS) further increases interconnection with the external environment, including other vehicles, roadside units (RSUs), and pedestrians, through V2X technologies. As a result, in-vehicle network components are increasingly exposed to external threats. In Internet of Vehicles (IoV) environments, attack surfaces can be categorized into three domains [24]: in-vehicle, V2X access, and infrastructure. Certain attack types, such as denial-of-service (DoS) and flooding, may affect all three domains, while others, such as tampering or physical damage, are specific to a single domain. V2X communication is a primary target for IoV security attacks, including eavesdropping, communication hijacking, spoofing, data injection, and impersonation. Therefore, this paper focuses on the V2X access domain, which encompasses all V2X connectivity modes, including vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-network (V2N).

B. Attacker Model Overview

Attack detection systems are typically designed to identify specific attack types and assess detection performance. Therefore, a comprehensive understanding of attacker behavior and associated attack types is essential for implementing resilient defense mechanisms.

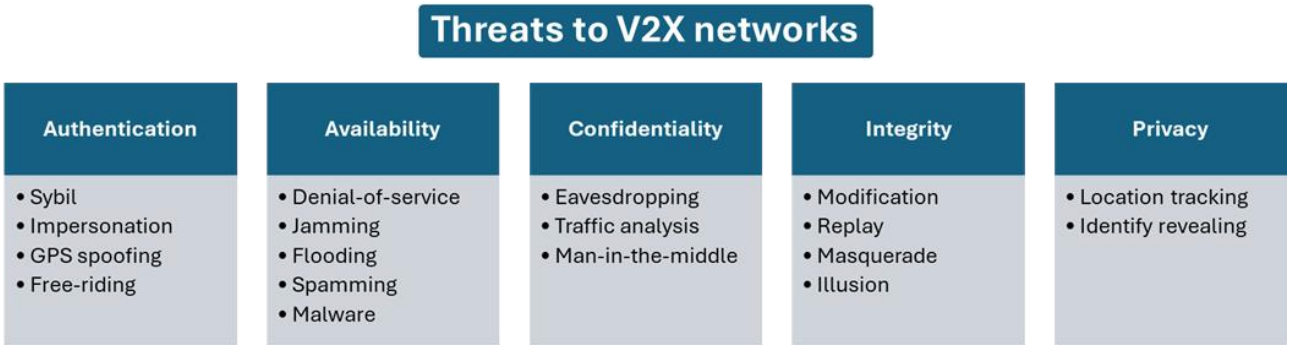

Fig. 2. Classification of V2X cybersecurity threats according to compromised security and privacy requirements.

Currently, there is no universally accepted model for classifying V2X attack variants. This analysis adopts the attacker model proposed in [25], which systematically defines the capabilities and methods available to attackers targeting assets such as vehicles, roadside units (RSUs), and communication channels. According to [25], an attacker is classified as an insider when they possess valid credentials that allow communication with legitimate system members or provide system-wide access. These authenticated insiders generally adhere to system protocols but may transmit false or fabricated information. In contrast, attackers without valid credentials or system access are considered outsiders. Outsiders, also known as intruders, have limited capabilities to launch attacks but can eavesdrop on communication links and infer sensitive information, such as security keys or user data. Attackers may also be categorized as malicious or rational based on their intent. Malicious attackers seek to disrupt or harm legitimate users and destabilize system functionality, often disregarding costs or consequences (e.g., causing accidents, denial-of-service (DoS) attacks, or traffic congestion). Rational attackers, by contrast, are motivated by personal gain, such as financial incentives or insurance fraud, and their methods and targets are often more predictable. V2X attacks can be further distinguished by execution mode: active or passive. Active attackers engage directly with the system, transmitting malicious packets or signals through V2X channels. Representative active attacks include DoS, message replay, false data injection, man-in-the-middle (MitM), and Sybil attacks. These are generally considered the most frequent threats to vehicular networks [6]. Passive attackers, on the other hand, primarily eavesdrop on communications to infer critical information, such as certificates, private keys, or user data, without direct interaction.

C. Classification of Attacks

A variety of existing studies have investigated security threats in the context of V2X communication [16], [26]. These works categorize attacks based on factors such as the wireless interface, communication scope, and behavioral characteristics, thereby aiding the development of robust security solutions for vehicular services. This section elaborates on security threats and attacks that are both common and effective against V2X networks. The classification, summarized in Figure 2, is based on key security requirements: authentication, availability, confidentiality, data integrity, and privacy. While each attack is classified under a primary security requirement, certain attacks, such as malware, may compromise multiple requirements simultaneously. Table 5 summarizes the key characteristics of various attacks in V2X networks, including the feasibility of launching each attack and the associated severity, particularly in safety-critical scenarios. Attacks that significantly impact operational performance or result in privacy breaches are categorized as high severity [27]. Relevant references indicate which communication technologies are susceptible to specific attacks or threats.

These examples demonstrate that many attacks effective against conventional communication systems remain highly effective in V2X environments.

V. PROACTIVE SECURITY MECHANISMS IN VEHICLE-TO-EVERYTHING (V2X) COMMUNICATION

Proactive security mechanisms serve as the primary defense in Vehicle-to-Everything (V2X) communication systems, aiming to prevent cyberattacks before they affect system operations. Unlike reactive approaches that detect and mitigate malicious behavior after the fact, proactive security emphasizes protecting the authenticity, integrity, confidentiality, and privacy of communication through preventive cryptographic and architectural measures. This approach is particularly vital in V2X environments, which are characterized by highly dynamic topologies, stringent real-time requirements, and safety-critical functions.

The deployment of Public Key Infrastructure (PKI)-based solutions is fundamental to proactive V2X security. PKI facilitates message authentication, integrity verification, and non-repudiation using digital signatures and certificates. Standardization bodies such as IEEE and ETSI have established PKI-based security architectures, including IEEE 1609.2 and ETSI TS 103 097, which define secure message formats and certificate management protocols for vehicular communications. These mechanisms restrict V2X communication to legitimate entities, thereby mitigating impersonation and basic spoofing attacks.

To address privacy concerns, proactive security frameworks employ pseudonymous certificates, enabling vehicles to periodically update their identifiers while preserving authentication. This strategy reduces risks associated with location tracking and profiling by preventing the persistent linking of transmitted messages to actual vehicle identities. The survey highlights that pseudonym management is both essential and challenging, as frequent certificate changes elevate signaling overhead and complicate revocation processes.

Another critical category of proactive mechanisms addresses secure key management and certificate revocation. Compromised or misbehaving vehicles pose significant threats to V2X ecosystems, necessitating efficient revocation strategies to promptly exclude them. The literature discusses Certificate Revocation Lists (CRLs) and alternative methods, such as compressed CRLs and regional revocation schemes, that aim to balance security effectiveness with communication efficiency. Nevertheless, scalability remains a major challenge, particularly in high-density traffic environments.

Secure hardware components, such as Hardware Security Modules (HSMs), are also identified as integral to proactive security. HSMs offer tamper-resistant environments for cryptographic operations and secure key storage, thereby substantially reducing the risk of key extraction and physical attacks. These components are commonly incorporated in both academic proposals and standard frameworks for V2X security architecture.

Despite their effectiveness, proactive security mechanisms have inherent limitations. Cryptographic operations incur computational and communication overhead that can conflict with the low-latency requirements of safety-critical V2X applications. Furthermore, proactive approaches are generally ineffective against insider attacks and compromised yet authenticated nodes, as they rely on the presumed trustworthiness of entities with valid credentials. The authors contend that while proactive security is essential, it must be supplemented by reactive and trust-based mechanisms.

Proactive security mechanisms form the foundational layer of V2X cybersecurity, establishing trust, authenticity, and privacy through standardized cryptographic solutions. [5] Nonetheless, persistent challenges in scalability, latency, revocation efficiency, and insider threats necessitate integrating proactive measures with adaptive, intelligence-driven security solutions, as explored in subsequent sections of the survey.

VI. REACTIVE SECURITY MECHANISMS IN V2X COMMUNICATION

Reactive security mechanisms in Vehicle-to-Everything (V2X) communication are intended to detect, identify, and mitigate malicious behavior after an attack has commenced. [5] In contrast to proactive approaches that prevent unauthorized participation through cryptographic safeguards, reactive security targets originate from authenticated or compromised entities, such as insider nodes and misbehaving vehicles. This function is essential in V2X environments, where high mobility, openness, and decentralized operation render preventive security alone inadequate.

Misbehavior detection is a primary category of reactive security solutions that focuses on identifying abnormal or malicious actions by analyzing transmitted messages and

vehicle behavior. The survey examines various mechanisms for detecting misbehavior, including plausibility checks, consistency verification, and context-aware analysis. For instance, these methods detect physically impossible positions, unrealistic speeds, or inconsistent trajectories among neighboring vehicles. Such approaches assume that legitimate vehicle behavior adheres to predictable physical and spatiotemporal constraints.

Reactive security mechanisms are generally categorized into local and cooperative detection strategies. Local mechanisms operate independently within individual vehicles, providing rapid response and minimal communication overhead, though they may suffer limited visibility and higher false-positive rates. In contrast, cooperative mechanisms utilize information sharing among multiple vehicles or infrastructure nodes to enhance detection accuracy and robustness. However, cooperative schemes present challenges related to trust management, scalability, and increased communication overhead.

Trust and reputation management is a significant aspect of reactive security discussed in the survey. Trust-based frameworks dynamically assign trust scores to vehicles according to their observed behavior over time. Vehicles that consistently transmit valid and plausible information are deemed trustworthy, whereas misbehaving entities experience a degradation of trust and eventual isolation. These mechanisms facilitate adaptive responses to evolving attacks but must be carefully designed to prevent manipulation, collusion, and Sybil attacks.

The survey highlights the growing importance of machine learning and data-driven techniques in reactive V2X security. Supervised, unsupervised, and semi-supervised learning models are utilized to classify normal and malicious communication patterns, detect anomalies, and identify emerging threats. These approaches show considerable potential for addressing complex and previously unknown attacks. However, the survey also notes that learning-based solutions introduce new vulnerabilities, including adversarial machine learning and data poisoning, which must be addressed in system design.

Despite their effectiveness, reactive security mechanisms exhibit significant limitations. Detection latency can permit short-lived attacks to affect safety-critical services before mitigation is possible. Furthermore, the absence of standardized datasets and evaluation methodologies complicates objective performance comparisons across detection schemes. Excessive false alarms may also undermine system trust and usability, particularly in dense traffic environments.

In summary, reactive security mechanisms are essential complements to proactive defenses in V2X communication. By facilitating the detection and mitigation of insider attacks, compromised nodes, and unforeseen threats, these mechanisms strengthen the resilience of V2X ecosystems. However, the survey emphasizes that integrating reactive mechanisms with proactive security and trust frameworks is necessary to achieve comprehensive, robust cybersecurity in intelligent transportation systems.

VII. The Role of Artificial Intelligence in V2X Security

Artificial Intelligence (AI) has become a key enabler of improved cybersecurity in Vehicle-to-Everything (V2X) communication systems, especially for addressing complex, dynamic, and previously unknown attack scenarios. While traditional rule-based and cryptographic security mechanisms remain essential, they are often inadequate for managing the scale, mobility, and heterogeneity of V2X environments. [5] Consequently, recent literature increasingly investigates machine learning (ML) and data-driven approaches to supplement both proactive and reactive security mechanisms.

A central application of AI in V2X security is the detection of anomalies and misbehavior. Machine learning models are trained to recognize normal communication and mobility patterns using historical or real-time data, enabling the identification of deviations that may signal malicious activity. Supervised learning techniques, such as support vector machines, decision trees, and neural networks, are effective when labeled datasets are available. Conversely, unsupervised and semi-supervised methods, including clustering and autoencoders, are used to detect novel or previously unknown attacks that require labeled data. These methods are particularly valuable in V2X environments, where attack patterns can change rapidly.

AI-based security mechanisms are also implemented in trust and reputation management systems. Learning-based trust models analyze vehicle behavior over time to dynamically update trust scores and identify persistently malicious or unreliable nodes. Compared to static rule-based frameworks, AI-driven approaches provide greater adaptability and scalability in dynamic traffic conditions. However, the survey notes that these systems are sensitive to data quality and susceptible to manipulation through coordinated or collusion attacks.

Another significant research direction focuses on intelligent intrusion detection systems (IDS) designed for V2X communication. These systems combine data from various sources, such as onboard sensors, network traffic, and contextual information, to achieve more accurate and timely detection. Deep learning models, including convolutional and recurrent neural networks, show considerable promise in capturing the complex spatiotemporal dependencies present in vehicular environments. However, their computational and training demands pose challenges for deployment on resource-constrained vehicular nodes.

Despite their benefits, AI-driven security solutions introduce new threat vectors. The survey identifies vulnerabilities unique to machine learning, such as adversarial examples, data poisoning, and model manipulation. Attackers can inject malicious data during training or operation to reduce detection accuracy or bias trust assessments. These risks raise significant concerns about the reliability and robustness of AI-based V2X

security mechanisms, particularly in safety-critical applications.

Furthermore, the absence of standardized datasets, benchmarks, and evaluation frameworks remains a major barrier to the adoption of AI solutions in V2X security. Many studies rely on simulation-based datasets or simplified assumptions, complicating cross-comparison and limiting real-world validation. The authors emphasize the need for realistic, large-scale datasets and reproducible evaluation methodologies to advance research in this field.

In summary, artificial intelligence offers significant potential for enhancing cybersecurity in V2X communication by enabling adaptive, data-driven detection and decision-making. However, effective integration requires careful attention to robustness, explainability, computational efficiency, and protection against AI-specific attacks. The survey concludes that future V2X security architectures should integrate AI-based mechanisms with traditional proactive and reactive defenses to achieve resilient and trustworthy intelligent transportation systems.

VIII. Outstanding Challenges and Directions for Future Research

Although significant advancements have been made in securing Vehicle-to-Everything (V2X) communications, several unresolved challenges hinder the deployment of fully resilient intelligent transportation systems. A primary concern is the pronounced interdependence between cybersecurity and functional safety. In contrast to traditional networks, successful cyberattacks on V2X systems can directly threaten human safety. However, most current security solutions are not adequately integrated with safety certification and system-level assurance frameworks. Consequently, future research should prioritize integrated security and safety co-design methodologies.

Scalability and latency constraints constitute another significant challenge. Cryptographic authentication, certificate management, and revocation mechanisms introduce processing and communication overhead, which can conflict with stringent real-time requirements, especially in dense traffic environments. As V2X deployments increase, the development of lightweight and latency-aware security mechanisms is essential.

Trust and reputation management in highly dynamic and decentralized environments remains an unresolved issue. While trust-based schemes offer adaptability, they are susceptible to collusion, Sybil attacks, and manipulation of trust metrics. Developing robust, context-aware trust models that function reliably under partial observability and adversarial conditions represents a critical research direction.

The growing integration of artificial intelligence amplifies both opportunities and risks within V2X systems. Although AI-based mechanisms enhance adaptability and detection accuracy, they also introduce vulnerabilities, including adversarial machine learning and data poisoning. Ensuring the robustness, transparency, and verifiability of AI models is therefore essential for safety-critical V2X applications.

The absence of standardized datasets, benchmarks, and evaluation methodologies, combined with interoperability and regulatory challenges, significantly impedes real-world adoption. Future research should advance holistic, scalable, and adaptive security architectures that integrate proactive, reactive, and AI-driven solutions to enable trustworthy and resilient V2X-enabled intelligent transportation systems.

IX. Conclusion

Intelligent Transportation Systems (ITS) increasingly depend on Vehicle-to-Everything (V2X) communication and distributed cyber-physical architectures to improve safety, efficiency, and automation. [28] However, this increased connectivity substantially enlarges the attack surface, underscoring the need for cybersecurity to ensure the reliable operation of modern transportation systems. This paper examines cybersecurity threats in ITS using a structured, multi-dimensional perspective, emphasizing their complexity and potential cyber-physical consequences.

A comprehensive classification of threats is presented, considering threat actors, attack vectors, targeted assets, violated security properties, and resulting impacts. The analysis demonstrates that cybersecurity incidents in ITS frequently extend beyond the digital domain, directly impacting system availability, operational reliability, and road safety. This characteristic distinguishes ITS from traditional information systems and underscores the need for integrated, safety-aware security strategies.

The paper further reviews proactive and reactive security mechanisms for V2X communication. Proactive approaches, such as PKI-based authentication and privacy-preserving mechanisms, establish a necessary baseline of trust but encounter limitations in scalability, latency, and the threat of insider attacks. Reactive mechanisms, including misbehavior detection and trust-based frameworks, complement these defenses by enabling the identification of compromised or malicious nodes during operation, although challenges remain in detection accuracy and timely response.

Artificial intelligence is identified as a powerful enabler of adaptive, data-driven security, capable of addressing complex, evolving attack scenarios. However, AI-based solutions also introduce new vulnerabilities, reinforcing the need for robust, explainable, and verifiable models in safety-critical environments.

In conclusion, achieving resilient and trustworthy intelligent transportation systems requires a holistic cybersecurity approach that integrates proactive, reactive, and AI-driven mechanisms within a unified framework. The solution pathways discussed in this work are intended to support scalable, adaptive, and safety-aware security architectures, thereby contributing to the secure evolution of next-generation ITS.

ACKNOWLEDGMENT

The authors thank their affiliated institutions for their support of this research. They also appreciate the helpful discussions and technical insights that shaped this work.

REFERENCES

[1] S. Joshi, A. Baviskar and S. Rajmane, "A review of cybersecurity in smart cities and intelligent transport systems," *Discover Internet of Things,* vol. 6, p. 41, 2026.

[2] Mashkina I., Rzaieva S., Kostiuk Y., Mazur N., Brzhevska Z., "Cybersecurity in Intelligent Transport Systems: Current Challenges and Solutions," in *Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2025)*, Kyiv, Ukraine, February 28, 2025 (online).

[3] E. Dritsas and M. Trigka, "A Survey on Cybersecurity in IoT," *Future Internet,* vol. 17, 2025.

[4] U. Tariq, I. Ahmed, A. K. Bashir and K. Shaukat, "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review.," *Sensors (Basel, Switzerland),* vol. 23, no. 8, April 2023.

[5] R. Sedar, C. Kalalas, F. Vázquez-Gallego, L. Alonso and J. Alonso-Zarate, "A Comprehensive Survey of V2X Cybersecurity Mechanisms and Future Research Paths," *IEEE Open Journal of the Communications Society,* vol. 4, pp. 325-391, 2023.

[6] K. Herman Muraro Gularte, J. Paulo Javidi da Costa, J. A. R. Vargas, A. Santos da Silva, G. Almeida Santos, Y. Wang, C. Alfons Müller, C. Lipps, R. Timóteo de Sousa, W. de Britto Vidal Filho, P. Slusallek and H. Dieter Schotten, "Integrating Cybersecurity in V2X: A Review of Simulation Environments," *IEEE Access,* vol. 12, pp. 177946-177985, 2024.

[7] R. K. Agrawal, *AI-Driven Secure Vehicular Networks: Intelligent Threat Detection and Trust-Aware Defense for V2X Systems,* IEEE Dataport, 2026.

[8] F. C. Ogenyi, C. N. Ugwu and O. P.-C. Ugwu, "Securing the future: AI-driven cybersecurity in the age of autonomous IoT," *Frontiers in the Internet of Things,* Vols. Volume 4 - 2025, 2025.

[9] O. Grant, "Smart ITS: AI, V2X, Sensors, Security," *Global Journal of Technology and Optimization,* vol. 16, no. 4, 2025.

[10] V. Sokolov, F. Kipchuk, P. Skladannyi, O. Zhyltsov and D. Ageyev, "Method for Increasing the Various Sources Data Consistency for IoT Sensors," in *2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*, 2022.

[11] Dudykevych, V. and Mykytyn, G. and Stosyk, T. and Skladannyi, Pavlo, "Platform for the Security of Cyber-Physical Systems and the IoT in the Intellectualization of Society," *Cybersecurity Providing in Information and Telecommunication Systems 2024,* vol. 3654, pp. pp. 449-457, 2024.

[12] V. Sokolov, P. Skladannyi and N. Mazur, "Wi-Fi Repeater Influence on Wireless Access," in *2023 IEEE 5th International Conference on Advanced Information and Communication Technologies (AICT)*, 2023.

[13] *3GPP, "Service requirements for enhanced V2X scenarios (Release 17)," Tech. Rep. TS 22.186 v17.0.0,* 2022.

[14] B. Brecht, D. Therriault, A. Weimerskirch, W. Whyte, V. Kumar, T. Hehn and R. Goudy, "A Security Credential Management System for V2X Communications," *IEEE Transactions on Intelligent Transportation Systems,* vol. 19, pp. 3850-3871, December 2018.

[15] A. Alnasser, H. Sun and J. Jiang, "Cyber security challenges and solutions for V2X communications: A survey," *Computer Networks,* vol. 151, pp. 52-67, 2019.

[16] M. Hasan, S. Mohan, T. Shimizu and H. Lu, "Securing Vehicle-to-Everything (V2X) Communication Platforms," *IEEE Transactions on Intelligent Vehicles,* vol. 5, pp. 693-713, December 2020.

[17] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV," *Ad Hoc Networks,* vol. 61, pp. 33-50, 2017.

[18] M. Villarreal-Vasquez, B. K. Bhargava and P. Angin, "Adaptable Safety and Security in V2X Systems," *2017 IEEE International Congress on Internet of Things (ICIOT),* pp. 17-24, 2017.

[19] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," *Journal of Network and Computer Applications,* vol. 101, pp. 55-82, 2018.

[20] *ETSI, "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management; Release 2," Tech. Rep. TS 102 940 V2.1.1,* 2021.

[21] D. Manivannan, S. S. Moni and S. Zeadally, "Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs)," *Veh. Commun.,* vol. 25, p. 100247, 2020.

[22] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Vehicular Communications,* vol. 23, p. 100214, 2020.

[23] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner and T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces," in *Proceedings of the 20th USENIX Conference on Security*, USA, 2011.

[24] I. Ivanov, C. Maple, T. Watson and S. Lee, "Cyber Security Standards and Issues in V2X Communications for Internet of Vehicles," in *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, p. 46.

[25] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.,* vol. 15, p. 39–68, January 2007.

[26] R. Lu, L. Zhang, J. Ni and Y. Fang, "5G Vehicle-to-Everything Services: Gearing Up for Security and Privacy," *Proceedings of the IEEE,* vol. 108, pp. 373-389, February 2020.

[27] S. Sharma, A. Kaul, S. Ahmed and S. Sharma, "A detailed tutorial survey on VANETs: Emerging architectures, applications, security issues, and solutions," *International Journal of Communication Systems,* vol. 34, p. e4905, 2021.

[28] D., Dimitrov, Intelligent Transportation Management: Current Issues and Solutions, LAP LAMBERT Academic Publishing, pp. 284, 2026.