AI/ML-Driven Intrusion and Misbehavior Detection in Networked Autonomous Systems: A Survey of Common Practices

Opeyemi Ajibuwa*, Bechir Hamdaoui*, and Attila A. Yavuz†
* Oregon State University, Corvallis, OR, USA, ajibuwao,hamdaoui@oregonstate.edu
† University of South Florida, Tampa, Fl, USA, attilaayavuz@usf.edu

***Abstract*—AI/ML-based intrusion detection systems (IDSs) and misbehavior detection systems (MDSs) have shown great potential in identifying anomalies in network traffic of networked autonomous systems. Despite the vast research efforts, practical deployments of such systems in the real world have been quite limited. Although the safety-critical nature of autonomous systems and the vulnerability of learning-based techniques to adversarial attacks are among the potential reasons, the lack of objective evaluation and feasibility assessment metrics is one key reason behind the limited adoption of these systems in practical settings. Researchers are more focused on presenting theoretical proposals than evaluating the feasibility of their solutions in real-world scenarios. This survey addresses this limitation by presenting an in-depth analysis of AI/ML-based IDSs/MDSs and establishing baseline metrics relevant to networked autonomous systems. Furthermore, this work presents a thorough survey of recent works in this domain, highlighting the evaluation metrics and gaps that exist in the current literature. This work also presents key findings derived from our analysis of the surveyed papers and proposes guidelines for providing AI/ML-based IDS/MDS solution approaches suitable for vehicular network applications. Our work provides researchers and practitioners with the needed tools to evaluate the feasibility of AI/ML-based IDS/MDS techniques in real-world settings, with the aim of facilitating the practical adoption of such techniques in emerging autonomous vehicular systems.**

***Index Terms* — Autonomous Vehicle (AV) networks, Unmanned Aerial Vehicle (UAV) networks, AI/ML-based Intrusion Detection System (IDS) and Misbehavior Detection System (MDS).**

I. Introduction

The recent breakthroughs in sensing, computing, and communication technologies have transformed the realm of cyber-physical systems [1], [2], [3]. Autonomous Vehicles (AVs) and Unmanned Aerial Vehicles (UAVs) [4] are two subdomains of the cyber-physical systems that have seen tremendous growth and innovation due to reasonable computing/sensing costs and 5G wireless service support. The number of devices embedded in these systems and the use of these vehicles are continuously expanding. Because these systems are designed to function without any human input, their various components must share critical data to be able to function properly and safely. Furthermore, there has been a growing demand for these vehicles to interact with one another and other infrastructures, mostly for safety reasons [5]. As a result, concepts such as Vehicle-to-Everything (V2X) communications and Flying Ad-Hoc Networks (FANETs) and their variants have emerged [6], [7], [8].

The increased connectivity provided by these networks is beneficial to the many applications built on top of them, but also creates a host of new attack surfaces. Intrusion detection systems (IDS) [9], [10], [11], [12] and misbehavior detection systems (MDS) [13], [14], [15] have been developed, with a recent focus on the use of artificial intelligence/machine learning (AI/ML)-based tools, to identify and prevent attacks on these safety-critical systems. The number of proposals for AI/ML-based IDS and MDS has increased in the literature over the last decade, owing to the high accuracy of these techniques in finding complex patterns in large datasets. Even though these AI/ML-based IDS/MDS have mostly performed admirably when researched, they have yet to be deployed to their full potential in real-world systems and scenarios [16].

A. Motivation

The use of AI/ML approaches has demonstrated success in various domains, yet the adoption of AI/ML-based IDS/MDS in networked autonomous systems has not been extensive. This may be due to the lack of demonstrated viability of these solutions in the real world, and the absence of evaluation frameworks for assessing their feasibility. The mobility and dynamic nature of AV and UAV networks necessitate the development of efficient security solutions, as well as comprehensive feasibility evaluation frameworks.

To address this gap, we establish a baseline for computation, memory, and latency requirements for AV/UAV networks. By reviewing the literature, we identify key metrics for validating IDS/MDS proposals for real-world AV/UAV networks. Our survey goes beyond highlighting issues with AI/ML-based IDS/MDS and identifies challenges that limit their feasibility. We also propose potential solutions to address these challenges and facilitate the adoption of AI/ML-based detection in networked autonomous systems. Our goal is to provide a comprehensive examination of previously proposed IDS/MDS solutions for AV/UAV networks, enabling researchers and industry practitioners to make informed assessments of their feasibility for real-world applications.

B. State-of-the Art Surveys

Previous surveys have attempted to review prior IDS/MDS techniques, but without evaluating their feasibility in real-world settings (see Table I). Additionally, most of IDS/MDS research has focused on improving detection accuracy rather

This work was supported in part by US National Science Foundation (NSF) under awards No. 1923884 and No. 2003273.

TABLE I
Summary of Techniques, Scope, and Comparison of Related Surveys.

RELATED SURVEYS	FOCUS AREA	PUB. YEAR	TECHNIQUE	SYSTEMS STUDIED	DIFFERENCE WITH OUR WORK
Deep AI/ML-based Anomaly Detection in Cyber-physical Systems: Progress and Opportunities [17]	Anomaly detection	2021	DL	CPS	Focuses on DL-based CPS security; ours broadens the scope to encompass other types of learning and present some new directions and novel work in those domains.
Recent Advances in Machine-Learning Driven Intrusion Detection in Transportation: Survey [18]	IDS	2021	ML/DL	VANETs and UAVs	Scarcely mentions the IDS applications in UAV networks: ours went into greater detail surveying AI/ML-based IDS/MDS approaches in AV/UAV networks.
A Survey on Machine Learning-based Misbehavior Detection Systems for 5G and Beyond Vehicular Networks [19]	MDS	2022	ML/DL	5G and vehicular networks	Focuses on IDS techniques only: ours covers both IDS and MDS approaches, as well as highlights some of the new challenges that these systems face.
Machine Learning for Security in Vehicular Networks: A Comprehensive Survey [20]	Security, Trust/Privacy	2021	AI/ML	Vehicular Networks	Ours focuses on AI/ML-based IDS/MDS techniques for AV and UAV networks.
Our survey	IDS/MDS	2022	AI/ML	AV/UAV networks	—

than optimizing these systems for practical deployments. This survey focuses only on works published in the last few years to provide readers with the latest research developments. Luo et al. [17] presented a survey on deep AI/ML-based anomaly detection for cyber-physical systems. Their work categorized various works based on the threat model, detection strategies, implementation, and evaluation metrics. They also briefly discussed the characteristics and techniques of each neural network model used for building a deep anomaly detection method. However, the authors did not evaluate the feasibility of the anomaly detection methods for real-time applications. Moreover, their work did not include a review of AI/ML-based techniques.

Bangui et al. [18] presented a survey on ML-based techniques for IDS in Vehicular Ad Hoc Networks (VANETs) and UAV networks. While they highlighted some of the main challenges in the literature, a discussion of novel challenges such as concept drift and adversarial attacks was missing in their work. Additionally, they did not provide a real-time evaluation of the surveyed works.

Boualouache et al. [19] presented a comprehensive survey on ML-based MDS for V2X communications. They discussed misbehavior detectors from both security and ML perspectives and provided recommendations for developing, validating, and deploying these ML-based MDS approaches. Furthermore, they highlighted open research and standardization issues surrounding existing systems. However, the authors did not evaluate the feasibility of the proposed MDS in a real-world context.

In Talpur et al. [20], the authors presented a systematic review of ML-based techniques for addressing different security issues in vehicular networks. They provided a taxonomy of attacks in vehicular networks and discussed the security challenges and requirements associated with each. Moreover, they discussed the approaches and working principles of the ML techniques employed in the literature. However, their work did not evaluate the feasibility of the existing works.

Given the gaps in previous surveys, current AI/ML-based IDS/MDS coverage may be inadequate, especially regarding the proposed techniques' practical feasibility in safety-critical networked systems (e.g., AV/UAV networks). Currently, there are no established baselines against which proposed solutions could be compared. Our work aims to address this gap by reviewing recent works and highlighting their current limitations based on our findings. Lastly, we provide new directions from other domains to facilitate the adoption of AI/ML-based IDS/MDS solutions in real-world scenarios. Our goal is to establish baseline assessment metrics that encourage future research innovations in this field.

C. Our Contributions

To the best of our knowledge, our survey is the first to examine the feasibility of the proposed IDS and MDS solutions via objective assessment metrics. Also, there is limited research on developing solutions addressing some of the lingering problems preventing AI/ML-based detection systems from being fully adopted in practice, and our survey aims to fill this research gap. Our survey also describes and presents feasibility criteria that should be used when designing IDS/MDS for AV/UAV networks. Furthermore, as more autonomous cars and UAVs are being developed and embraced by users, this survey serves as a timely reminder of how to best evaluate IDS and MDS techniques for real-world deployment. The following summaries of our contributions:

- We taxonomize AI/ML-based IDS/MDS in AV/UAV networks. We also review the architectures, threat scenarios, and other considerations to establish baseline metrics for a realistic feasibility assessment of the proposed systems. We establish benchmarks in this domain to serve future research developments.
- To establish their viability for real-world applications, we critically analyze and contextualize several recently proposed IDS/MDS approaches in the literature. We only review research papers published in the last couple of years since we feel they are more up-to-date in ad-

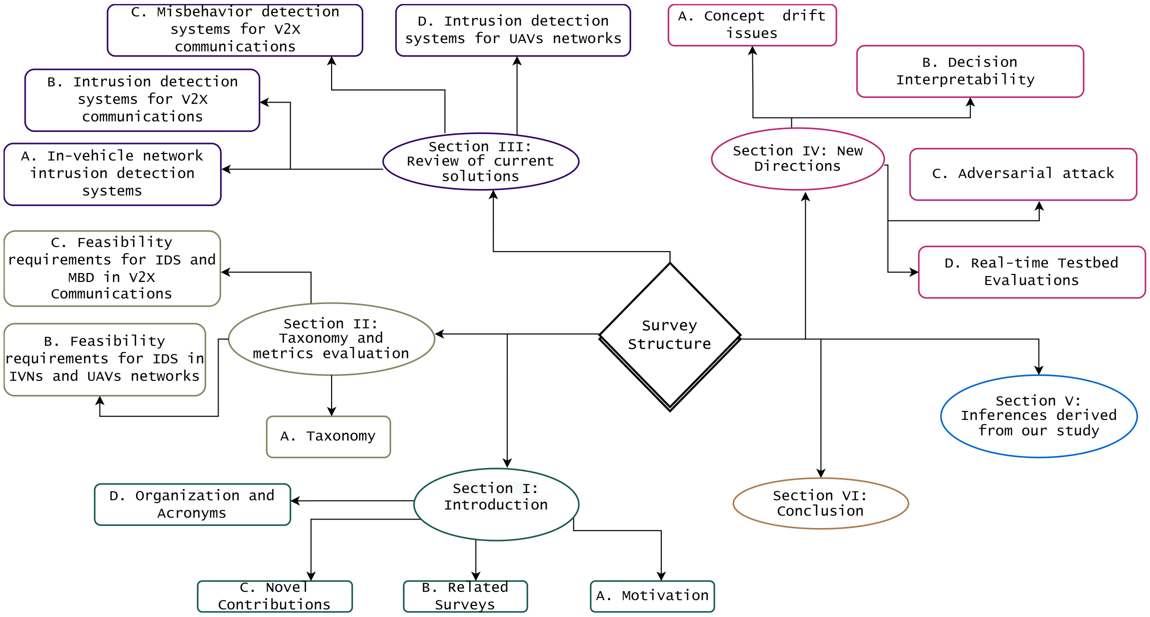
C. Misbehavior detection systems for V2X communications
D. Intrusion detection systems for UAVs networks
A. Concept drift issues
B. Decision Interpretability
B. Intrusion detection systems for V2X communications
Section III: Review of current solutions
Section IV: New Directions
C. Adversarial attack
A. In-vehicle network intrusion detection systems
D. Real-time Testbed Evaluations
C. Feasibility requirements for IDS and MBD in V2X Communications
Survey Structure
Section II: Taxonomy and metrics evaluation
B. Feasibility requirements for IDS in IVNs and UAVs networks
Section V: Inferences derived from our study
A. Taxonomy
Section I: Introduction
D. Organization and Acronyms
Section VI: Conclusion
C. Novel Contributions
B. Related Surveys
A. Motivation

Fig. 1: Organization and Structure of the Survey

dressing some of the current difficulties with IDS/MDS.

- We investigate some of the persistent issues and some new ones that are preventing AI/ML-based IDS/MDS solutions from being deployed in real-world scenarios. We analyze the limitations of machine learning and deep learning approaches and propose new ideas on how to go about overcoming these limitations.
- We also identify and describe several exciting research in the general domain of AI/ML-based intrusion detection proposed to solve some of the issues these autonomous systems currently face.

D. Organization and Acronyms

Figure 1 shows the overall organization of this survey paper. The taxonomy, architecture, and baseline requirements are presented in Section II. Section III analyzes each of the surveyed literature in terms of the requirements defined in the previous section for real-world applications of the proposed IDS/MDS solutions. A detailed review of the challenges with the current solutions are also discussed in Section IV. Section V presents new proposed ideas and directions that aim to address some of the challenges with current AI/ML-based IDS/MDS solutions. We conclude the paper in Section VI. A summary of the acronyms used is provided in Table II.

II. Taxonomy and Evaluation Metrics of IDS/MDS Solution Approaches

We first explain our taxonomy for AI/ML-based IDS/MDS techniques in AV/UAV networks. We then present an overview of the architectures and requirements for assessing the feasibility of the proposed solutions in each of the studied domains: in-vehicle networks (IVN), V2X communications, and UAV networks. Finally, we establish the metrics for evaluating the viability of existing IDS and MDS techniques based on these requirements.

TABLE II
Acronyms

ML	Machine Learning
DL	Deep Learning
VANETs	Vehicular Ad Hoc Networks
FANETs	Flying Ad Hoc Networks
CAN	Controller Area Networks
V2V	Vehicle-to-Vehicle
V2I	Vehicle-to-Infrastructure
V2R	Vehicle-to-Road
V2G	Vehicle-to-Grid
V2C	Vehicle-to-Cloud
BSM	Basic Safety Messages
CAMs	Cooperative Awareness Messages
ECUs	Electronic Control Units
MiTM	Man-in-the-Middle
MBD	Misbehavior Detection
MDS	Misbehavior Detection System
OBD	Onboard Diagnostics Units
DLC	Diagnostics Link Connector
FNR	False Negative Rate
FPR	False Positive Rate
LOS	Line-of-Sight
IoT	Internet of Things
RSU	Roadside Units
MEC	Multi-Access Edge Cloud
OBUs	On-board Units
SDNs	Software Defined Networks
OEMs	Original Equipment Manufacturers
IDS	Intrusion Detection System

A. Taxonomy

We depict our taxonomy in Figure 2, which consists of (1) detection strategies, (2) systems architectures, (3) application scenarios, (4) attack and input types, (5) machine learning models, and (6) implementation and evaluation methods.

1) Detection Strategies

In this section, we delve into the two detection systems reviewed in our study: IDS and MDS. While IDSs are employed in both AV and UAV networks, MDSs are mainly used in vehicles. The reason for this could be that launching insider attacks in UAV swarms is more challenging than in AV networks. Let's take a closer look at each system:

IDS for In-vehicle Networks (IVNs): Modern cars' complexity and connectivity make in-vehicle networks particularly vulnerable to security threats [21]. Some IVN applications lack broadcast authentication and messaging, making it necessary for IDSs to monitor and identify abnormalities in the Controller Area Network Bus (CAN-BUS) network [22].

IDS for V2X Communications: Exposure to multiple connection points makes vehicles vulnerable to various attacks that could threaten lives and other essential infrastructures. To prevent these attacks, IDSs integrate cryptographic security techniques into various V2X communications (e.g., V2V, V2I, V2R, etc.) [23].

IDS for UAVs and Hybrid Networks: Connected UAVs are also vulnerable to attacks, some of which can be detected via IDSs integrated into UAVs' communication networks [24]. Hybrid IDSs are designed to protect vehicular networks from both internal and external attacks.

MDS for V2X Basic Safety Messages: Misbehavior detection for V2X communications involves monitoring the data semantics [25] of transmitted Basic Safety Messages (BSMs) to detect attempts that aim to sabotage the network by sending bogus messages that could mislead other vehicles.

MDS for In-vehicle Sensory Data: Detecting anomalies in vehicles caused by incorrect sensor data readings is critical for the overall system safety. Although faulty sensor data may not be planned as an attack, detecting these anomalies early on is essential to prevent them from being communicated to other vehicles and misinterpreted as an act of attack.

MDS for V2X Basic Perception Messages: Validating semantic validity of Collective Perception Messages (CPMs) is essential to prevent attacks on V2X systems [26]. Trusting CPMs is risky, and as such, IDSs have been proposed to verify the semantic validity of these messages.

2) System Architectures

IDSs have three deployment architectures: centralized, decentralized, and hybrid. In a centralized architecture, data is aggregated at a central node for model training and attack detection. In a decentralized architecture, training and detection are distributed over each local node in the network. In a hybrid architecture, models are trained locally on each node, and the trained models are aggregated centrally to enable a network-wide attack detection capability. At the protocol layer, MDSs operate as an application in VANETs because misbehavior happens at the application layer of the communication protocol stack. On the other hand, IDSs deal with traffic intrusion at the network layer.

3) Application Scenarios

IDSs are used in both AV and UAV networks, whereas MDSs are only applied in AVs in the following scenarios:

VANETs and Internet of Vehicles (IoV): VANETs consist of only vehicle-to-vehicle communications. That is, it is an ad-hoc network of vehicles connected and exchanging data with each other [27]. In contrast, IoV spans a bigger network involving entities such as humans, things, and other heterogeneous networks. It is formally defined in [28] as the real-time exchange of information on roads between vehicles and sensors, vehicles and vehicles, vehicles and roads, and also vehicles and personal devices using different wireless communication access technologies. These information exchanges should ideally be authenticated by respecting the real-time (i.e., delay-aware) requirements of IoVs [29].

Autonomous Vehicles (AV): AVs are vulnerable to both internal and external threats. Compared to conventional vehicles, AVs have to communicate with other vehicles and infrastructure which are external networks and may become a channel for attack and an opportunity for hackers [30].

FANETs and Internet of Drones (IoD): FANETs are networks comprised of multiple UAVs connected in an ad-hoc manner and integrated into a group to achieve high-level goals [31]. On the other hand, IoDs [32] are networks of UAVs that allow users to communicate and control UAVs through the Internet.

4) Attack and Input Types

Attackers can target many aspects of AV and UAV networks and such attacks can take many forms. An attack could be a network-layer MiTM (Man-in-the-middle) or a DDoS (distributed DoS) attack on the network traffic. It could also be launched on the application layer, such as on the network's safety messages, or adversarial attacks launched on the network's models trained for detecting intrusion or misbehavior. Sensory data is commonly utilized for training MDS, while network traffic data (in time-series format or traffic logs) is also be used for training IDS.

5) Machine Learning Models

For IDS/MDS in AV/UAV networks, the most commonly used machine learning models are: deep neural networks (DNN) [33], [34], [35], reinforcement learning (RL) [36], [37], [38] and federated learning (FL) [39].

6) Implementation and Evaluation Methods

Time-series network traffic data is used to train and test ML-based IDS models, whereas sensory data obtained using simulation tools, like VEINS and CARLA, is often used to train and evaluate MDS models. Accuracy, precision, recall, and Receiver Operating Characteristics (ROC) are some of the most commonly used metrics for evaluating such systems.

B. Feasibility Requirements for Intrusion Detection Systems in IVNs and UAV Networks

To derive the metrics for characterizing the feasibility of IDS in IVN and UAVs, we raise and answer some key questions:

1) What Are the Realistic Threats to IVNs?

Several solutions have been proposed and evaluated in the literature based on different attacker models. However, many of these attacks cannot be verified to be possible in real-world

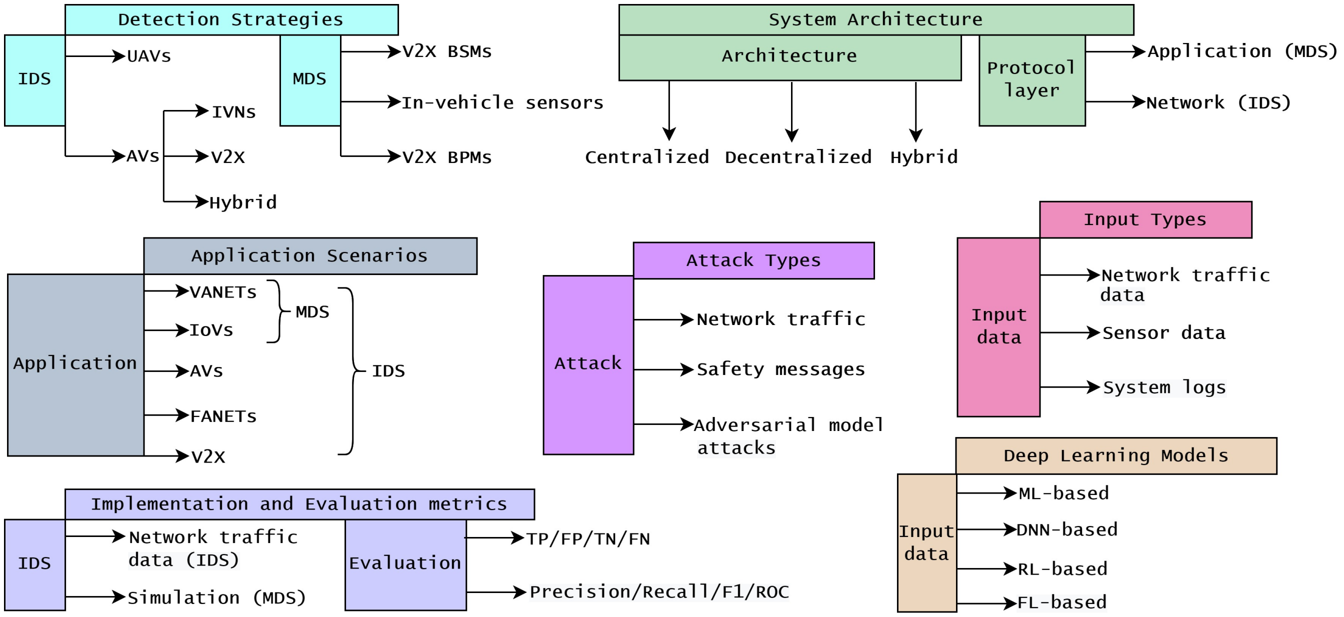

Fig. 2: Taxonomy of AI/ML-based Intrusion and Misbehavior Detection in AVs and UAVs

settings, either because no evidence exists or because their assumptions are unrealistic [40]. As a result, it is essential to consider the types of attacks that pose a serious threat to IVN and for which IDS solutions are fit. Misbehavior in IVNs is due mainly to faulty sensor readings. Since faults are outside the scope of our study, we do not discuss them. As demonstrated by [41], attacks can be launched on the IVNs by either plugging into the OBD-II port or compromising an ECU remotely through WiFi, Bluetooth, or telematics services. The attacks that have been proven to pose a real threat to IVNs are described briefly next.

Denial-of-Service (DoS) Attacks: The attacker spams the IVN by sending messages with a high priority and at a fast rate, delaying or completely denying access to other legitimate nodes that need to send messages on the network. Researchers [33], [42], [43], [44] have demonstrated the efficacy of this attack in the past.

Spoofing Attacks: In this attack scenario, an attacker can create and inject spoofed messages into the IVN to impersonate a victim's ECU. This attack is easily realized by checking the DBC file for a particular car or by performing reverse engineering on the network bus [45], [42].

Replay Attacks: The replay attack injects previously captured traffic into the network and masks it as regular data, slowing real network traffic. Although the replayed traffic represents a previously legitimate traffic sequence, the delay associated with its later insertion disrupts the network's real-time sequence of events. Previous tests showed that it is simple to carry out in most automobiles [45], [46], [44], [47].

Fuzzing Attacks: A fuzzy attack randomly injects compromised CAN ID, DLC, and data fields, resembling legitimate traffic, to manipulate the IVN. The disruptions caused by this attack have been reported to result in abnormalities such as abnormal engine noise [48], abnormal increase in power [48], gear switching [47], erratic change of signal lights [49], etc.

Drop Attacks: The drop attack manifests itself by a compromised ECU pausing or terminating packet transmissions. This implies that messages from the compromised ID do not appear in network traffic for some time after it has been hijacked. This attack has been demonstrated in tests like in [50], [51], [43].

Other variants: Some other forms of attacks reported on the IVN include Ulterior fuzzy attacks [47], Plateau attack [43], Continuous change attack [43], Malfunction attack [52] and Unknown attack [52].

2) What Are the Realistic Threats to UAV Networks?

UAVs are subject to attacks due to the open nature of their wireless communication medium. An attacker can use various strategies to hijack a UAV network and extract important mission information. We focus on the threats that were shown to be the most realistic in the literature.

DoS and DDoS Attacks: In a DoS attack, an attacker sends multiple requests to the UAV network channel, disrupting regular transmission and causing a network outage [53]. DDoS attacks are launched from multiple actors sometimes using distributed entry points into the network [54].

Jamming Attacks: Jamming is a type of DoS attacks that poses a severe danger to UAV networks by impairing network availability [55], [56]. A malicious user floods the UAV network channels with high-power radio signals to disrupt ongoing conversations. Control signals or fake GPS signals can occasionally be used as jamming signals [57].

GPS spoofing Attacks: An adversary creates fake GPS signals and transmits them to the target as legitimate ones. The attacker can alter the content of intercepted signals or use a GPS signal generator to produce spoofing signals [53].

Message Forgery and Replay Attacks: The attacker injects forged data into UAV networks to make UAVs unstable. The spoofed message can be sensor data or control signals meant to coordinate the UAV network operations. Replay attacks are carried out in UAV networks by replacing genuine data from sensors with previously sniffed data to degrade network performance and create instability [58].

3) What Metrics Really Measure the Effectiveness of Attack Detection in IVNs and UAV Networks?

Researchers mostly use the base metrics of accuracy, recall, precision, and F1-score to evaluate the performance of learning-based IDS solutions. Naturally, detecting attacks with high accuracy is important when developing an IDS for vehicular networks; however, it is more beneficial if such a performance is replicated in practice. Since this is not always the case, additional design criteria must be considered when developing realistic IDS solutions for IVNs and UAV networks. The requirements listed below are developed as a baseline reference for assessing IVN and UAV IDS solutions.

Detection Accuracy: It is a useful performance measure for determining the ratio of correctly classified instances to the total number of instances. For a balanced dataset, accuracy is sufficient as a metric of effectiveness of an IDS solution. In contrast, F1-score is considered the correct measure of accuracy for an imbalanced dataset.

False Positive Rates (FPRs) and False Negative Rates (FNRs): False Positives and False Negatives are particularly undesirable for IVNs and UAVs. This is because of their safety-critical nature since false positives and false negatives can have catastrophic effects on the network. Even if network activity is modest, false alarms can have far-reaching consequences for passengers in the vehicle and the UAV's mission, if safety-critical data is wrongly classified as an attack [59]. On the other hand, false negatives occur when intrusion detection systems fail to identify an intrusion during or after it has happened. The outcome might be a slow response to the intrusion, leading to an accident or a failure of the UAV's mission. As a result, to assure complete trust in the performance and use of an IDS, FPRs and FNRs must be kept as low as possible.

Response Time: This may be classified into two groups. The training time, the time it takes to fully train a learning-based IDS, and prediction time, the time it takes an IDS to successfully classify traffic. While having a high accuracy is desirable, if detecting an attack takes an hour, the attacker may have already done damage to the network [22]. Similarly, if the training takes too long, the IDS model may not be updated in time to identify new types of attacks. Furthermore, researchers must consider time complexity and placement strategies when designing an IDS due to resource limitations on the Vehicle ECUs and UAVs.

Throughput: An IDS should be efficient and should not be a network bottleneck [22]. This implies that the data throughput of IVNs and UAV networks must be considered to ensure that there is enough bandwidth to accommodate IDS overheads. This is critical since some applications are time-sensitive (e.g vehicular safety applications which require delays of less than 300ms [60]

Model Update: It is not enough to develop a functional IDS; it is also necessary to ensure that it can be easily updated to detect new attack types without compromising security or introducing delays during the update process. In addition, updates must be done based on the feedback received from real network samples.

Privacy: Because of the various connections interfaces of IVNs and UAVs, an IDS must not leak the private data of the vehicle without permission to other systems. This is especially important if the IDS connects back to a cloud back-end for incident analysis and transfer of sensitive data [59].

4) How is the Current Vehicle Architecture Fit to Meet the Requirements of an IVN IDS?

One of the challenges that hindered the widespread deployment of IVN IDSs is a lack of specification on the requirements of IDS for modern vehicle designs. Although the ISO 21434 standard provides some general specifications for designing IVN cybersecurity solutions, it lacks the finer details required to develop an IDS. Currently, no industry standards exist that describe the onboard infrastructure requirements for deploying an IDS in an IVN. Another issue is that contemporary IDS proposals do not consider modern vehicle designs, making many of the IVN IDS solutions presented in the literature problematic to integrate with existing vehicle designs. Moreover, network resources and performance needs differ from one ECU to another within an IVN. Thus when developing an IDS for the network, it is important to consider the placement of the ECUs as well as their real-time requirements.

ECUs Architecture and Latency Demands: ECUs are classified into different domains based on their functionality and latency requirements. In high-end vehicles, there are at least 70 working ECUs, which are spread throughout the vehicle.

Different recommendations for IDS deployment to protect the ECUs have been suggested. Some have proposed employing an IDS for each of the vehicle's ECUs, while others have pushed for IDS deployment on the bus's gateway. While the latter notion looks to be more realistic, it is difficult to decide which architecture is best without taking into account the real-time requirements of the different domains that make up an IVN. The characteristics of the traffic messages in the domains vary. Some of them are information intensive, while others are safety-critical [21]. Those in the safety-critical category are powertrain and chassis. Powertrain consists of the ECUs that oversee critical processes, including engine management and transmission control. The braking system which prevents tire sliding and maintains vehicle stability belongs to the powertrain category. In the chassis domain, components include the anti-lock braking, suspension, steering, airbag and collision avoidance system. Since all these components are safety-critical and require real-time communication, they have stricter security requirements compared to other ECUS.

5) How is the Current UAV Architecture Fit to Meet the Requirements for an IDS?

The internal architecture of UAVs and the characteristics of their network when interconnected are important considerations in the design of practical IDS. In this section, we briefly review UAVs' general architectures so that we can understand how they dictate the requirements that an IDS must satisfy to be deemed feasible for deployment.

- Flight Controller: It is the UAV's central processing unit, which interacts between software and the drone's onboard electronics. Depending on the application, the memory and CPU capacity of this microcontroller unit may vary. However, UAVs are resource constrained, with high-end microcontroller boards having CPU speeds of only a few Gigahertz and storage space of only a few Gigabytes.
- Ground control Station (GCS): This is an On-Land Facility where human operators provide control signals for the UAV network's launch, command, and monitoring throughout an operation [61]. This control is normally done from afar, and maintaining contact with the UAV swarm requires low-latency communication. Intrusion into the GCS has the potential to sabotage the UAVs by allowing the attacker to take control of the network. As a result, securing the GCS-UAV link is critical to the network's security and safety.
- Wireless communication module: The data link module includes a transmitter and receiver connected to the flight controller board to control information flow between UAVs and the GCS. The type of wireless link deployed depends on the operational range of the UAVs: cellular radio waves for visual LOS and satellite communications for below-visual LOS [61].
- Sensors and Actuation: Sensors on UAVs provide measurement, visibility, and ranging functions, allowing the UAV to estimate its location, speed, and height in relation to its surroundings. The sensor readings are then converted into data, which the Flying Controller processes and sends to the actuator, which produces the necessary actuation for the UAV throughout its flight mission [62]. An attack on the sensor of a UAV can disrupt the entire network if, for example, the UAV is the relay cluster head of its unit.

6) What are the Metrics that are Based on IVN Hardware Constraints?

The ECUs and networks embedded in cars are not comparable to traditional IT systems that are interconnected with high-speed Ethernet connections [63]. Hence, it is essential to consider the resource requirements of ECUs, as IDS solutions that work well in simulations or non-contextual tests may be too resource-intensive to deploy on today's ECU hardware. However, most ECUs are proprietary software devices with limited documentation on their architecture and implementation. As a result, examining their internal configuration is a difficult task that can only be achieved by backdoor reverse engineering. We will not delve into the intricacies of ECU resource needs because we could not find the information needed to do so. Instead, we will try to present relevant evaluation guidelines from a broad view of what is reasonable in IVNs with limited resources:

CPU and Memory Consumption: Most of the ECUs in a vehicle possesses limited computational and memory resources. For instance, low-end ECUs might only need 8bit microcontrollers running at 20Mhz with 32kB memory and 1kB of RAM [64]. This strongly limits their ability for real-time functions in resource-intensive IVN IDS. In this regard, computationally intensive AI/ML-based IDS methods may not be able to meet the real-time demands of current cars.

Network Bandwidth Consumption: The multiple distributed ECUs in an IVN use up a considerable portion of the IVN's capacity. As a result, analyzing network bandwidth usage with IDS is critical to ensuring that real-time message delivery across the network is not jeopardized.

Power Consumption: Automobiles rely on a finite amount of energy to run, thus defining a key metric to assess how much power an IDS solution consumes in IVNs is critical.

7) What are the Metrics that are Based on UAV Hardware Constraints?

Based on the hardware architecture outlined in the previous section, we summarize the key considerations for implementing practical IDS for UAV networks below.

Computational and Memory Costs: Because most UAVs have limited compute and memory resources, any additional components must make minimal resource demands to fit the hardware capability of the UAV without compromising system security. This requires striking a reasonable balance between detection accuracy and the processing and storage overheads associated with such an IDS.

Network Bandwidth Costs: The wireless communication channel's capacity, the UAVs' velocity, the error-prone nature of the wireless connections, and the lack of security with broadcast communications all limit the size of the available bandwidth in UAV networks [65]. Hence, an IDS's efficient bandwidth use is essential, as there are already several applications competing for the limited bandwidth available in the network.

Energy Costs: As rechargeable batteries typically power UAVs, their energy resources are limited. When deployed in a network, the UAV network power is determined by the energy resources of the individual units [65], which can be quickly drained if an inefficient IDS is used in the UAVs. Thus, it is critical to design IDSs that are power aware.

8) What Other Considerations Should Influence IDS Development for IVN and UAVs?

Price: The cost of integrating an IDS solution should also be considered. A system that necessitates substantial redesigns of current hardware or software, for example, incurs additional costs and is thus less desirable to manufacturers (or the owners in case the IDS solution is implemented as an aftermarket product) [63].

System Complexity and Ease of Deployment: This is closely related to the last point as prices tend to increase with system complexity and simplicity makes a security system easier to deploy, audit, maintain and evaluate.

Flexibility and Scalability: This indicates how adaptable an IDS solution is to the different situations that may arise in IVN and UAV networks. For example, how flexible is it to account for a variety of electronic platforms, each of which has hundreds of little variations, and how successfully will the solution manage ECU/sensor software upgrades, replacements, and other tasks, are things to consider when designing such IDSs[66]. In terms of scalability, key factors to consider when designing these systems are [66]: (1) Is the solution future-proof in that it can be readily updated? (2) Is it possible to extend it to detect threats launched from outside the vehicle? (3) Does it allow for independent upgrades to the IDS software and its configuration?

Forensic Capabilities: What features does the IDS solution offer for detecting anomalies, and how effective is it at detecting zero-day attacks? Are cloud-based services available, and if so, what features do they have [66]? All these form important questions that should be answered for designing an effective IDS for IVN and UAV networks.

Recovery from Attacks: In the literature, recovery after attacks is often overlooked. Nonetheless, determining the extent of an intrusion and evaluating its potential impact on the network to effectively recover the IDS from attacks through effective damage assessment and remediation is key.

Relevancy of Datasets: As the costs of real-world experiments are quite prohibitive, IDS evaluated with synthetic datasets obtained either from other network domains or through simulation and/or testbed evaluation should seriously consider the real-world relevancy of the dataset features to avoid models that overfit to simulated environments, but are inefficient in practice.

Table III provides a summary of the different feasibility requirements we surveyed. Our attempt here is to define the most critical factors necessary to evaluate the feasibility of the latest IVN and UAV IDS proposals.

C. Feasibility Requirements for IDS and MBD in V2X Communications

We now provide answers to the same questions as we posed in the preceding section to establish the metrics for evaluating the feasibility of IDS and MBS proposals in V2X.

1) What Are the Realistic Threats to V2X Communication?

Due to the multiple external entities that a vehicle interact with in V2X communication, some of the attacks we have already discussed for IVNs also impact V2X communications, as well as a few others that we will go over briefly below:

Denial-of-Service (DoS) and Distributed DoS attacks: DoS attacks are mostly aimed at denying access to a system resource. In the context of V2X, an attacker initiating DoS can try to shut down the network between vehicles and roadside infrastructures, denying the vehicle access to critical road safety information. Multiple nodes in V2X can launch a distributed DoS attack to deny vehicular access and make critical network infrastructure unavailable for legitimate access. Various forms of DoS and DDoS attacks have been reported in the literature, including JellyFish, intelligent cheater, and flooding [67].

Replay Attacks: In replay attacks, an attacker can resend messages previously transmitted by other vehicles, infrastructure and pedestrians in an attempt to disrupt traffic flow and cause receiving vehicles to improperly react to non-existing road conditions[68], [69].

False Information Attacks: A vehicle might generate false information, such as BSMs or sensor data, and broadcast it to the network. The attacker does this with the aim of causing traffic jams or accidents in the network. This attack can take the form of fake position coordinates, fake speed, false acceleration or false deceleration messages broadcast to other vehicles nearby [69].

Sybil and Blackhole Attacks: Sybil attacks involve a user creating multiple fake identities. The attacker then uses those identities to send different messages to other vehicles, pedestrians, and infrastructure to cause disruption in the network. An attacker performing black-hole attacks manipulates other nodes into routing packets through them and then drops the packets instead of forwarding them, preventing the message from reaching its intended recipient. While a number of researchers have proposed MDS solutions to sybil attacks, the most effective mitigation methods are identification and authentication based methods [70], [69].

2) What Other Considerations Should Influence IDS/MBS Development for V2X Communications?

System Resources: As noted earlier, vehicles have limited processing, memory, and network resources [71]. When added to the strict time requirements of vehicular applications, an IDS/MDS might experience resource constraints filtering out network traffic/messages for attacks or misbehavior under a highly dynamic network topology.

Real-time Constraints: There are strict latency constraints that must be addressed when designing IDS systems as outdated information due to processing delays is of no use in V2X communications [72]. IDS/MDS based on complex learning-based algorithms with high computational demands might become unusable for real-time applications with maximum permissible latency of 300ms in V2X.

Threats Robustness: IDS/MDS designs need to be able to identify and detect zero-day attacks, rather than relying solely on prior signatures of known attacks or misbehavior. Vehicles in V2X can be infiltrated through various entry points and attackers are constantly exploiting new vulnerabilities, making it hard to anticipate all potential risks.

Flexibility: IDSs/MDSs are required to be flexible and dependable due to the myriad of devices and protocols used in the V2X environment. Similarly, given that network connections exist only for a limited period of time due to the dynamic nature of V2X network environments, it is important that the detection solution can adapt to filter traffic even when implemented in previously untested settings.

Privacy: Another concern for V2X communications is privacy because vehicles generate sensitive data and send it to other network participants. Identity and location information theft may occur if IDSs/MDSs cannot ensure that unauthorized users' data are not exposed when in operation and during updates.

III. Review of Current IDS/MDS Solutions

In this section, we analyze and summarize the evaluation of recently proposed IDS and MDS solutions for vehicular networks, including IVN, V2X, and UAV networks. We focus on the aspects that each paper concentrated on and identify any missing feasibility metrics discussed in the preceding section. Our approach is to be specific on some metrics if they are highly relevant to the paper, but otherwise, we discuss any missing metrics. Tables IV-X summarize our evaluation of each reviewed work.

TABLE III
Feasibility Metrics Summary

Metrics Category		Metric	Rationale
Attack Detection	1	Detection Accuracy	How often the IDS classifies network traffic correctly?
	2	False Positives Rate	How often an attack is misclassified as normal traffic?
	3	False negatives Rate	How often normal traffic is misclassified as an attack?
	4	Training Time	How long it takes to train the ML-based IDS?
	5	Prediction Time	How long it takes the IDS to output a detection result?
	6	Throughput	How does the IDS affect the vehicle network traffic data rates?
	7	Model update	How does the IDS update and how long does it take?
	8	Privacy	How does the IDS protect the private data of the vehicle?
	9	Relevancy of evaluation dataset	How relevant is the evaluation dataset for developing the IDS?
Hardware Constraints	10	Processing costs	How does the computational needs of the IDS impact the real-time needs of the vehicle?
	11	Memory costs	What effect does the IDS memory usage have on the vehicle real-time requirements?
	12	Network bandwidth costs	How does the IDS impact the latency requirement of the vehicle?
	13	Energy costs	How does the IDS add to the vehicle‘s energy demands?
	14	Ease of Deployment	What effort and time is required to configure and use the IDS on the vehicle?
Secondary Factors	15	Price constraint	Does the IDS add to the production costs of the vehicle?
	16	System complexity	Does the IDS complexity add any substantial costs to the vehicle?
	17	Flexibility	How adaptable is the IDS to different environments?
	18	Scalability	Is the IDS future-proof?
	19	Forensics capabilities	How does the IDS account for undetected attacks?
	20	Recovery	How does the IDS recover after failure?

A. IVN Intrusion Detection Systems

Zhang et al. [45]: The authors proposed a hybrid IDS that combines rule-based and ML-based techniques to achieve efficient and accurate intrusion detection in IVNs. In the first stage, the rule-based technique acts by the rules defined by the author. The attacks evading this stage are forwarded to the DNN-based classifier in the second stage. The proposed model was trained and evaluated with real data collected from four distinct makes of automobiles. Although the proposed system achieved high detection accuracy on the evaluated dataset, the authors did not clarify the rationale for the rules selection in the first stage. Moreover, important feasibility metrics such as false-negative rate, communication cost, computing overhead, and privacy preservation capabilities were not considered in their evaluation.

Hossain et al. [33]: This paper proposed a CNN-based IDS for the CAN bus system and generated an evaluation dataset of CAN messages obtained from three different vehicle models. The proposed IDS is shown to achieve high accuracy for detecting three studied attack types. However, the proposed dataset is likely too simplistic to capture various practical attack scenarios. Furthermore, the metrics needed to determine the feasibility of the proposed method were not studied, but instead more emphasis was placed on discussing the methodologies of IDS development.

Lin et al. [42]: Authors in [42] proposed a DL-based denoising autoencoder for extracting and learning features based on packet transmission periodicity for the detection of CAN bus traffic anomalies. Although the proposed IDS was tested using real CAN/vehicle data and showed good detection accuracy, only three attacks were modeled.

Hanselmann et al. [43]: To capture the temporal dynamics of the CAN bus, the authors introduced CANet, an LSTM (long-short-term memory)-based architecture. By using an unsupervised learning approach, the proposed system was designed to detect both known and unknown attacks. Real and synthetic CAN data containing five different attack types were used to evaluate the proposed method. However, the memory costs were analyzed only analytically (the number of neural network parameters) without experimental insights.

Tariq et al. [44]: This paper proposed CANtransfer, a convolutional LSTM-based model that utilizes transfer learning to detect unknown attacks in IVNs. The CAN traffic data from two vehicles were used to capture three types of attacks. Although the detection accuracy appears promising for both known and unknown attacks, the authors did not evaluate key practical metrics such as the processing delays, false alarm rates, and false-negative rates, making it difficult to assess the practicality of their proposed approach.

Song et al. [73]: Using real traces obtained from injecting normal and attack traffic into the CAN bus, the authors proposed and tested the performance of a deep CNN-based IDS. Their experimental findings based on five different attack types demonstrated that the proposed model shows high detection accuracy, and low false positives and false negatives rates. They also estimated that it takes 5ms on a 2.3GHz Intel Xeon CPU and 6.7ms on an Nvidia Tesla K80 GPU to predict a traffic sample using their proposed approach. However, the simplicity of the message injection attacks evaluated in their datasets casts doubt on their proposal's practicality in real-world settings. Furthermore, the proposed system cannot detect attacks that have never been seen before, and details on updating the detection model were not provided.

Minawi et al. [74]: The authors proposed a ML-based IDS for the CAN bus that consists of three different inputs, threat detection, and alerting layers. They considered and tested different ML algorithms using the car hacking dataset containing real CAN bus messages and various injection attacks. Although they obtained good results in the detection accuracy and false alarm rates, they did not provide details on the false negatives rates, a metric that is as critical as the others presented. Moreover, the proposed IDS placement as an external hardware attached to the OBD II port might incur additional costs that the vehicle manufacturers or owners may be unwilling to bear. Similarly, the execution time metric evaluated for the proposed system is not a true measure of the computational performance of the proposed IDS.

Zhu et al. [75]: A distributed long-short-term memory (LSTM) framework for IVN anomaly detection is proposed in this paper. To detect anomalous messages on the CAN bus, the proposed method utilizes multi-dimensional temporal and data properties. They also proposed deploying the proposed IDS on a mobile edge to make use of the additional computational resources available there. However, offloading IDS operations to the edge could result in considerable delays, making real-time attack detection impossible. Furthermore, given that the proposed IDS only achieved 90% accuracy on a single test instance, it is hard to predict if it can perform well when applied to other vehicles.

Agrawal et al. [76]: The authors proposed a DL-based IDS incorporating thresholding and error reconstruction for detecting attack traffic on the IVN. They used the car hacking dataset, which contains three attack types, to train and test multiple LSTM architectures and compare their performance. They achieved high attack detection accuracy but mostly at the cost of large computational overheads and a 128ms detection latency. In addition, the authors did not consider other important metrics highlighted in Table III to assess the real-world feasibility of the proposed anomaly detector.

Desta et al. [77]: The authors proposed a convolutional neural network (CNN)-based IDS that detects attacks on the CAN bus by using images created from the temporal relations of CAN messages. The proposed IDS predicts attacks both online and offline. The online prediction analyzes real-time CAN traffic and provides real-time predictions, while offline prediction makes inferences for datasets that have been preprocessed. By using a dataset containing four attack types collected from a real car, the proposed model was trained and basic metrics were evaluated. Additionally, the authors used Nvidia's Jetson TX2 vehicle-class device and an external CAN transceiver connected to a vehicle's CAN bus to demonstrate a proof-of-concept of the proposed IDS. However, the proposed IDS is still limited by the following considerations, despite performing an experimental proof of their solution. First, implementing the IDS using an external device to mitigate the proposed IDS' high detection latency might introduce additional costs that may not meet automakers' and buyers' economic needs. Secondly, the proposed IDS is vehicle-specific and cannot be used on other makes. Finally, when deployed, the proposed IDS cannot be updated online since the learning model must be retrained when it begins to deviate considerably from its training datasets.

Cheng et al. [78]: The proposed TCAN-IDS trains a CNN-based ML model with global attention to detect attacks on the CAN bus using the temporal characteristics of CAN messages. On multi-featured temporal data, the authors demonstrated that the proposed model outperforms time-series neural networks, extracting better temporal and spatial features of the CAN messages. When they tested the proposed IDS on a dataset containing attacks of four distinct types on an Intel computer and the Jetson AGX Xavier Nvidia vehicle-class device, they obtained good detection accuracy and latency. However, since the CNN model's hyperparameters are set during training, updating it to detect new attacks without complete retraining is difficult. Furthermore, without considering the impact of other vehicle components, it is hard to assess the efficiency of inference time.

Xie et al. [34]: The authors proposed an enhanced deep learning GAN-based model for intrusion detection on the CAN bus. The proposed model uses elaborate CAN message blocks in the training samples to mimic the real generated CAN message blocks in the detection phase. The GAN discriminator can then determine whether each message has been tampered with via the CAN communication matrix. The experimental approach to validate the proposed IDS' performance was divided into three sections. First, the GAN model was trained offline on an Intel Xeon CPU with an Nvidia GP102 GPU. Subsequently, the GAN model was tested online on a CAN network prototype with three ECUs. The GAN model-based IDS was then deployed in a real-world setting using a Xilinx Spartan 6 FPGA connected to the CAN system via a vehicle's OBD II connector. The proposed IDS identified all four attacks with high detection accuracy after injecting them into the CAN bus. However, other important metrics like false positive and false negative rates were not considered.

Xun et al. [79]: The authors proposed an IDS that monitors message transmission on the CAN bus using vehicle voltage signals. The proposed IDS is based on the fact that ECUs employ somewhat different materials in their hardware, causing them to generate different voltage signals during transmission. These signal features were retrieved using statistical principles and a deep neural network model was implemented to learn and identify anomalous voltage signals on the CAN bus. The authors validated the proposed IDS on two real vehicles to show that it could be applied to various types of cars. The proposed IDS is designed to be used in the CAN bus automotive gateway and as an independent external device for CAN bus monitoring. However, while the proposed IDS is robust and has a high detection accuracy, it cannot detect attacks originating from the vehicle's ECUs. It can only detect attacks coming from outside sources.

Javed et al. [80]: The authors proposed CANintelliIDS for vehicle intrusion detection on the CAN bus. For detecting single and mixed intrusion attacks on a CAN bus, the proposed IDS uses a combination of CNN and attention-based gated recurrent unit (GRU). They assessed the proposed IDS' performance using a real dataset containing four different attacks; however, they ignored critical metrics like FPR, FNR, and detection latency needed to evaluate the proposed solution's feasibility in the real world.

B. V2X Intrusion Detection Systems

Alladi et al. [81]: This paper presented an IDS for detecting cyberattacks in IoV networks using a deep neural network model deployed on a MEC server connected to the RSU. The proposed system employs two classification techniques, one of which generates time sequences from network broadcast messages. The second method is based on classifying network traffic using image representations of these time sequences. The authors showed the feasibility of the proposed IDS on a Raspberry Pi 3B by simulating four distinct Deep Learning Engines (DLEs) using the Veremi Extension dataset, which contains traces collected from simulated vehicular network instances. They also proposed that the DLEs be trained on resource-rich cloud servers, with the time-critical prediction jobs being performed on locally deployed MEC servers connected to the RSUs. While they excelled in terms of detection accuracy and prediction time, they neglected to assess the communication overheads associated with the proposed MEC deployment plan.

Shu et al. [82]: A multi-discriminator GAN is proposed to enable multiple distributed SDN controllers to jointly train an IDS model for an entire VANET without directly exchanging their sub-network flows. The proposed IDS framework solves the biased flow problem with individual detection and avoids the high system overheads of centralized detection techniques. After training the collaborative IDS model across multiple distributed SDN controllers, the proposed detection model will be utilized over the entire VANET to detect flows among vehicles and RSUs. The proposed framework was validated using KDD99 and NSL-KDD experimental datasets and an emulated cloud server with three distributed SDN controllers. They evaluated some critical metrics based on the complexity of their proposed framework. They demonstrated novelty in their work by demonstrating the proposed system's validity in both IID and non-IID contexts with rigorous mathematical proofs. However, they do not provide numerical results of the metrics evaluated in their experiment.

Nie et al. [83]: The author developed a data-driven IDS by examining the link load characteristics of an RSU in an IoV in response to various attacks. They designed and tested different deep neural network models and discovered that a CNN-based model performs best at extracting spatio-temporal features of RSU link loads and thereby identifying intrusions. They used a testbed that included an RSU, 30 OBUs, and four attackers who carried out DDOS attacks on the network to simulate the scene of an IoV. They assessed the proposed method's accuracy and compared it to three existing techniques. However, they did not analyze other critical metrics such as FPR, FNR, and prediction latency that can be used to determine the feasibility of their research.

Goncalves et al. [84]: This paper proposed an Intelligent Hierarchical IDS that splits the network into four levels with several clusters at each level, allowing different ML-based detection approaches to be used. To test the performance of their various ML models, the authors used a simulated dataset reflecting different features and attack types.

Kosmanos et al. [85]: The proposed IDS uses a cross-layer set of attributes to train ML models to detect spoofing and jamming attacks against connected vehicle platooning communication. The proposed IDS's detection engine is built on Random Forest, k-Nearest Neighbor, and One-Class SVM, as well as cross-layer data fusion methods. The proposed IDS can generate probabilistic outcomes for both known and unknown attacks. The authors used Veins' simulation [86] to evaluate the proposed IDS for a platoon of four vehicles and obtained a dataset encompassing the two attacks studied. Their results showed that the proposed IDS can detect both attacks with great precision. However, the proposed IDS is attack-specific and key metrics like FPR, FNR, and detection latency were ignored in the study.

Ghaleb et al. [87]: This paper proposed a misbehavior-aware on-demand collaborative IDS based on distributed ensemble learning techniques. Individual vehicles in the proposed system use their data to train a local IDS classifier, which they then share with other vehicles on demand. The best-performing shared IDS are then combined with the locally trained IDS to create an ensemble of classifiers for usage on the local vehicle. The authors used SUMO simulations [88] to simulate various attacks and evaluate the proposed model's basic performance metrics. However, they did not give concrete numbers on the proposed model's savings in terms of communication costs. Moreover, the computational and memory overheads were overlooked.

Yang et al. [23]: The authors presented a multi-tiered hybrid IDS for IoVs that combines signature-based IDS and anomaly-based IDS to detect both existing and zero-day attacks on both intra-vehicle and external vehicular networks. There are four layers of learning models in the proposed multi-tier architecture. The authors used the car hacking datasets, which represent intra-vehicle networks, and the CICIDS2017 dataset, which represents external network traffic data, to evaluate the performance and efficiency of the proposed IDS. Their evaluation considered different performance metrics and demonstrated the proposed model's real-world feasibility on a vehicle-level Raspberry Pi 3 IoT device. However, while they assessed the proposed IDSs' processing time and memory requirements, they failed to evaluate the FNR, an equally important metric to consider.

Ashraf et al. [35]: The authors proposed a DL-based IDS for identifying suspicious V2X network traffic. The proposed IDS is not based on signatures and is designed to detect existing and new attacks. They used deep neural network

TABLE IV
IVN-IDS Feasibility Metrics.

	FPR	FNR	Accuracy	Threat Model	Unseen Attack	Latency(ms)	Placement	Validation
Zhang et al. [45]	$< 0.1\%$	n/a	$> 99\%$	Yes	n/a	0.55	C. Gateway	R. Traces
Hossain et al. [33]	$< 0.002\%$	$< 0.028\%$	$> 99.9\%$	Yes	n/a	n/a	n/a	R. Traces
Lin et al. [42]	$< 12.89\%$	$< 10.92\%$	$> 89\%$	No	n/a	n/a	n/a	R. Traces
Hanselmann et al. [43]	n/a	n/a	$> 99\%$	Yes	Yes	n/a	n/a	R&S Traces
Tariq et al. [44]	n/a	n/a	$> 90\%$	No	Yes	n/a	n/a	R. Traces
Song et al. [73]	$< 0.18\%$	$< 0.35\%$	$> 90\%$	No	No	5/6.7	n/a	R. Traces
Minawi et al. [74]	0	n/a	$> 95.7\%$	No	n/a	n/a	E-ware	R. Traces
Zhu et al. [75]	n/a	n/a	$> 90\%$	Yes	n/a	0.61	MEC	R. Traces
Agrawal et al. [76]	n/a	n/a	$> 99.9\%$	Yes	n/a	128.78	n/a	R. Traces
Desta et al. [77]	n/a	n/a	$> 97\%$	n/a	n/a	117	n/a	Traces & PoC
Cheng et al. [78]	$> 0.15\%$	n/a	$> 99\%$	Yes	No	3.4	n/a	Traces & PoC
Xie et al. [34]	n/a	n/a	$> 99\%$	No	n/a	0.09	n/a	R. Traces
Xun et al. [79]	$< 0.1\%$	$< 0.21\%$	$> 97\%$	Yes	n/a	n/a	G/E-ware	R. Traces
Javed et al. [80]	n/a	n/a	$> 93\%$	No	n/a	n/a	n/a	R. Traces

n/a: not applicable; R.: Real; R&S: Real and synthetic; C.: Central; G: Gateway; E-ware: External Hardware; PoC: Proof of Concept

model is based on the LSTM autoencoder algorithm and is designed to detect attacks at automobiles' central network gateways. The proposed IDS was evaluated using the vehicle hacking dataset for IVN and the UNSW-NB15 dataset for external vehicular networks. The authors only considered standard learning performance metrics, making it difficult to analyze the feasibility of their proposed IDS.

Khan et al. [89]: The authors proposed a hybrid IDS to detect IoV attacks. They train normal network traffic datasets using a bloom filter and a DNN bidirectional LSTM architecture to detect zero-day attacks. Their evaluation is based on a real CAN-based car hacking dataset and the UNSWNB-15 external vehicular network dataset. They investigated specific feasibility metrics to determine their system's suitability to real-world scenarios. The experiments showed that the proposed IDS has a 7-minute training period and an attack detection time of 0.023 milliseconds, and incurs a total memory overheads of 3655kb. However, the author's evaluation lacked important metrics such as FPR and FNR necessary for a complete feasibility assessment.

C. V2X Misbehavior Detection Systems

Hsu et al. [90]: The proposed VANET deep learning-based MDS uses CNN and LSTM-based models to rebuild a vehicle's position information based on incoming BSMs. Based on the received message, an SVM classifier is utilized as a binary classification method to determine if the receiver vehicle has been compromised or not. The proposed MDS was trained and assessed using the popular vehicular reference (VEREMI) dataset, which contains many types of misbehavior in a vehicular setting. The authors evaluated the accuracy of their proposed system but failed to consider other important metrics like FPR, FNR, and prediction latency.

Sharma et al. [91]: This paper presented a data-centric ML-based MDS model for IoVs. The proposed system integrates plausibility checks with six selected ML algorithms to find the best-performing model for misbehavior detection in VANETs. The proposed model was evaluated using the VEREMI dataset with standard ML-based metrics. The authors proposed deploying the proposed system on the vehicle's OBU to support local detection and privacy preservation. However, they did not evaluate FPR, FNR, and detection latency metrics which are necessary to validate that the proposed scheme can meet the real-time and privacy requirements of V2X communications.

Wang et al. [92]: This paper introduced an IoV MDS based on broad learning and incremental learning methods. Different ML/DL algorithms are trained in the detection module to detect false messages, and the trained model is continuously updated with new data using an incremental learning technique. They evaluated the proposed model's performance using three real-world datasets: VeRemi, NGSIM, and PeMS. They evaluated the accuracy of their proposed solution, and the results suggest that their system can detect misbehavior in real time while frequently updating the learning model. However, critical feasibility metrics such as FPR and FNR were not considered in the study.

Hawlader et al. [93]: The authors trained six different ML algorithms in a supervised method to detect position falsification attacks in VANETs. The proposed system was trained on the VEREMI dataset, which contains several position falsification attacks, and its performance was validated with Veins simulation. However, the authors did not consider FPR, FNR, and prediction latency in their study.

Sharma et al. [94]: The proposed MDS combines information from two consecutive BSMs to train multiple ML algorithms to detect position falsification attacks in VANETs. Evaluation using the VeReMi dataset showed high detection accuracy in identifying different misbehaviors by the trained classifier. The authors suggested a hierarchical architecture for the deployment of the proposed system, where the RSUs

TABLE V
V2X-IDS Feasibility Metrics (I)

	FPR	FNR	Accuracy	Threat Model	Unseen Attack	Latency (ms)	Placement	Validation
Alladi et al. [81]	n/a	n/a	$> 98\%$	No	n/a	14.29	MEC	S. Traces
Shu et al. [82]	n/a	n/a	$> 97\%$	No	n/a	n/a	Decentralized	R. Traces
Nie et al. [83]	0	n/a	$> 97\%$	No	n/a	n/a	n/a	S. Traces
Goncalves et al. [84]	$< 0.14\%$	n/a	$> 92\%$	No	n/a	n/a	n/a	S. Traces
Kosmanos et al. [85]	n/a	n/a	$> 90\%$	Yes	n/a	n/a	n/a	S. Traces
Ghaleb et al. [87]	$< 0.11\%$	$< 0.05\%$	$> 90\%$	Yes	n/a	n/a	n/a	S. Traces
Yang et al. [23]	$< 13.822\%$	n/a	$> 75\%$	Yes	Yes	0.574/0.509	Gateway	R. Traces
Ashraf et al. [35]	n/a	n/a	$> 97\%$	No	Yes	n/a	Gateway	R. Traces
Khan et al. [89]	n/a	n/a	$> 98\%$	No	Yes	0.02ms	Gateway	R. Traces

n/a: not applicable; R.: Real; S.: Simulated

TABLE VI
V2X-IDS Feasibility Metrics (II)

	Privacy Preservation	Comm. Overhead	Compute Overhead	Memory Overhead	Energy Costs	Model Update
Alladi et al. [81]	n/a	n/a	n/a	n/a	n/a	n/a
Shu et al. [82]	n/a	Considered	Considered	Considered	n/a	Yes
Nie et al. [83]	n/a	n/a	n/a	n/a	n/a	n/a
Goncalves et al. [84]	n/a	n/a	n/a	< 54497kb	n/a	n/a
Kosmanos et al. [85]	n/a	n/a	n/a	n/a	n/a	n/a
Ghaleb et al. [87]	n/a	n/a	n/a	n/a	n/a	n/a
Yang et al. [23]	n/a	n/a	n/a	16.21mb	n/a	n/a
Ashraf et al. [35]	n/a	n/a	n/a	n/a	n/a	n/a
Khan et al. [89]	n/a	n/a	n/a	3655kb	n/a	Yes

n/a: not applicable

are deployed with the detection model rather than OBUs as most other works have proposed. However, the proposed system was not validated using key feasibility metrics such as FPR, FNR, and prediction latency.

Ercan et al. [95]: The proposed MDS integrates three new features for training two separate ML approaches for detecting position falsification attacks in vehicular networks. Evaluation was conducted using the VeReMi dataset, and the results indicate that the proposed MDS outperforms alternative approaches. The authors also proposed a distributed detection method with centralized training. However, they failed to evaluate critical feasibility metrics including FPR, FNR and prediction latency defined in our study.

Gyawali et al. [96]: The proposed MDS detects and prevents false alarms and position falsification attacks in vehicular networks by combining ML and reputation-based methods. It is trained with datasets generated via Veins simulations in a realistic vehicular network environment, and performs well on the public VeReMi dataset according to the standard ML metrics considered. The authors also examined the proposed system's complexity for real-world applications. However, they did not present numerical results to assess the proposed system's computing cost and detection time.

Uprety et al. [39]: The authors proposed a privacy-preserving MDS to address the privacy trust issues associated with centralized misbehavior detection techniques. Local ML models are trained using BSM data received on each vehicle and a global federated model is computed using the parameters of the locally trained models. The authors used the public VeReMi dataset and an Artificial Neural Network (ANN) algorithm to train the local models on the received BSMs as a proof of concept. They used basic ML metrics to assess the proposed system's performance and obtain numerical results for detection accuracy and communication costs. However, the VeReMi dataset is not distributed, and due to the highly dynamic nature of the vehicular network environment, the proposed technique may be restricted by bandwidth constraints in real-world applications.

D. UAV Intrusion Detection Systems

Slimane et al. [55]: A Lightweight Gradient Boosting ML (LightGBM) algorithm to detect subtle jamming attacks on UAV networks is proposed. The authors trained and evaluated LightGBM on a dataset consisting of 10,000 samples of both jamming signals and regular traffic. The obtained performance is compared to that of three other ML models and found that the proposed model outperformed the others. The authors considered critical performance metrics previously overlooked by others, but the numerical results for the evaluated metrics were not clearly presented.

TABLE VII
V2X-MBD Feasibility Metrics (I)

	FPR	FNR	Accuracy	Threat Model	Unseen Attack	Latency (ms)	Deployment Technique	Validation
Hsu et al. [90]	n/a	n/a	$> 95\%$	No	n/a	n/a	OBU	Simulated traces
Sharma et al. [91]	n/a	n/a	$> 85\%$	No	n/a	n/a	OBU	Simulated traces
Wang et al. [92]	n/a	n/a	$> 90\%$	No	n/a	< 267	n/a	R&S Traces
Hawlader et al. [93]	n/a	n/a	$> 94\%$	Yes	n/a	n/a	n/a	R. Traces & Sim
Sharma et al. [94]	n/a	n/a	$> 98\%$	No	n/a	n/a	RSUs	R. Traces & Sim
Ercan et al. [95]	n/a	n/a	$> 84\%$	No	n/a	Considered	Decentralized	Simulated traces
Gyawali et al. [96]	n/a	n/a	$> 84\%$	Yes	n/a	n/a	OBUs	Simulated traces
Uprety et al. [39]	n/a	n/a	$> 78\%$	No	n/a	n/a	OBUs	Simulated traces

n/a: not applicable; R.: Real; R&S: Real & Simulated; Sim: Simulation

TABLE VIII
V2X-MBD Feasibility Metrics (II)

	Privacy Preservation	Communication Overhead	Compute Overhead	Memory Overhead	Energy Costs	Model Update
Hsu et al. [90]	n/a	n/a	n/a	n/a	n/a	n/a
Sharma et al. [91]	n/a	n/a	n/a	n/a	n/a	n/a
Wang et al. [92]	n/a	n/a	n/a	n/a	n/a	Yes
Hawlader et al. [93]	n/a	n/a	n/a	n/a	n/a	n/a
Sharma et al. [94]	n/a	n/a	n/a	n/a	n/a	n/a
Ercan et al. [95]	n/a	n/a	n/a	n/a	n/a	n/a
Gyawali et al. [96]	n/a	n/a	n/a	n/a	n/a	n/a
Uprety et al. [39]	Yes	Considered	n/a	n/a	n/a	Yes

n/a: not applicable

Whelan et al. [97]: The proposed Micro Air Vehicle Intrusion Detection System (MAVIDS) trains a dataset containing normal flight logs to detect GPS spoofing and jamming attacks using unsupervised machine learning techniques. This approach eliminates the difficulty of finding a labeled dataset for training the detection model by using the UAVs' normal flight data. The authors employed standard ML metrics and conducted experimental proofs with three microcontroller boards to demonstrate the effectiveness of the proposed solution when deployed aboard a UAV. In addition, they considered prediction latency and throughput as metrics to assess the feasibility of the proposed system, but they also overlooked metrics such as FPR and FNR in their study.

Moustafa et al. [98]: The authors proposed an IDS to detect cyberattacks in drone networks. Data acquired from a synthetic testbed is designed to mimic realistic UAV networks and train and evaluate five ML algorithms. The testbed's dataset included normal traffic as well as three attack events: probing, DoS, and DDoS. Standard ML metrics were evaluated, but little was said about the other metrics needed to evaluate the proposed scheme's computation performance and deployment strategy in the real world.

Abu et al. [24]: This paper proposed an autonomous IDS (UAV-IDS-ConvNet) that uses deep CNNs to detect attacks on UAVs. The proposed solution is based on encrypted WiFi traffic data from three different types of UAVs. The authors created UAV-IDS-2020, a dataset that contains multiple attacks on UAV networks in unidirectional and bidirectional communication flow modes. The dataset also includes homogeneous and heterogeneous networked UAV scenarios for evaluating the proposed system's performance. However, because the proposed IDS was modeled after specific UAV types, its performance may not be generalized to other UAVs.

Bouhamed et al. [36]: The proposed lightweight intrusion detection and prevention system (IDPS) uses a Deep Q-learning (DQN) model to autonomously detect and prevent network intrusions in UAVs. A periodic offline-learning mechanism for updating the DQN model parameters to learn and adapt to changes in attack patterns was also added to the proposed detection module. A global model is periodically updated with recently exchanged data by the fleet of UAVs in the proposed distributed architecture. The proposed prototype was evaluated on the CICIDS2017 dataset, which included various attack types, and standard ML performance metrics, including energy consumption were taken into account. However, key feasibility metrics such as FPR, FNR and detection latency were not considered in this study.

IV. Takeaways from our Thorough Review

In this section, we provide a summary of the key takeaways based on our thorough review of the surveyed papers.

TABLE IX
UAV-IDS Feasibility Metrics (I)

	FPR	FNR	Accuracy	Threat Model	Unseen Attack	Latency (ms)	Deployment Technique	Validation
Slimane et al. [55]	1.8%	2.4%	$> 98\%$	Yes	n/a	n/a	n/a	Real traces
Whelan et al. [97]	n/a	n/a	$> 90\%$	Yes	No	< 124ms	On-board agent	Real traces
Moustafa et al. [98]	$< 1\%$	n/a	99%	No	No	n/a	n/a	Real traces
Abu et al. [24]	$< 1\%$	$< 3\%$	$> 90\%$	No	Yes	2.77ms	n/a	Real traces
Bouhamed et al. [36]	n/a	n/a	$> 85\%$	No	n/a	n/a	On-board agent	S. Traces

n/a: not applicable; S.: Simulated

TABLE X
UAV-IDS Feasibility Metrics (II)

	Privacy Preservation	Comm Overhead	Compute Overhead	Memory Overhead	Energy Costs	Model Update
Slimane et al. [55]	n/a	n/a	Considered	Considered	n/a	n/a
Whelan et al. [97]	n/a	n/a	n/a	n/a	n/a	n/a
Moustafa et al. [98]	n/a	n/a	n/a	n/a	n/a	n/a
Abu et al. [24]	n/a	n/a	n/a	n/a	n/a	n/a
Bouhamed et al. [36]	n/a	n/a	n/a	n/a	22591mAh	Yes

n/a: not applicable

1) Failure to consider and report on false positive rates (FPR) and false negative rates (FNR) metrics

From Tables IV-IX, it is clear that most of the reviewed works fail to report on the FPR and FNR metrics. Almost all reviewed studies use standard ML metrics only, including accuracy, precision, and recall. But due to the safety-critical implications of an attack misclassification in vehicular networks, reporting the detection accuracy is just as important as presenting the results of the false alarm and miss rates. Only 31% (11/36) of the papers reported the FPR and only 17% (6/36) presented the FNR rates based on our review. Because of these low percentages, many of the current solutions are limited in terms of demonstrating their appropriateness for protecting the devices in the vehicular network. It is also noteworthy that none of the reviewed papers on misbehavior detection in V2X provided results on FPR and FNR (see Table VII).

2) Lack of clearly defined benchmark threat models

The majority of the reviewed papers did not present a clear threat model on which to base their proposed solutions. This is especially evident in studies investigating IDS and MDS solutions for V2X environments, see Tables V and VII. The reason for this trend is obvious since most V2X-based studies rely on simulated datasets for evaluation. Nonetheless, even for works based on datasets, the necessity of conveying a clear threat model cannot be overstated. Because most publicly available datasets are attack-specific, any system that relies on them must convey a specific-threat model rather than give a misleading sense of generalization. Some of the attacks modeled in the reviewed literature, on the other hand, require further real-world proof to establish their impact and validity. This is particularly beneficial given the lack of real VANET datasets and the fact that extrapolated data from other areas may not be equally applicable to vehicular network settings.

3) Lack of after-deployment updating/upgrading mechanisms

The majority of current solutions do not consider or provide information about their update mechanisms after deployment. This is especially concerning for the IVN IDS papers reviewed (see Table IV) because none of the eleven proposed models can be retrained with new data samples after deployment. Furthermore, researchers have devoted little, if any, attention to mitigating zero-day attacks with the IDS and MDS solutions proposed in recent studies. As our analysis reveals, either no thought is given to designing systems capable of detecting both existing and new attacks, or information on such systems is omitted if they ever exist. That said, it must be acknowledged that the hardware updating problem is not specific to the studied autonomous networked systems but rather exists in other ML and DL domains as well.

4) Lack of inference-time and update-time reporting

Only 11 out of the 36 reviewed articles considered and provided details on the time it takes for their proposed system to classify network traffic. Although some authors assess their model's training and testing duration, such metrics are sometimes not specific and insufficient to accurately determine how such models will respond to real-world scenarios when deployed. While evaluating ML models' training and testing times has its merits, it is far more necessary to provide details on the prediction and model update latency of the proposed systems. Furthermore, it acts as a standard for comparing different solutions for simple adoption by the industry and provides a safety guarantee for the prediction time of an IDS/MDS.

5) Absence of placement and deployment strategies

When it comes to the deployment of the IDS/MDS solutions presented in the literature, it is surprising to see how many implicit assumptions are made. Researchers appear to have given little thought to how these systems will fit into the existing architecture of automobiles, infrastructure, and UAVs. This tendency is particularly alarming for IDS solutions proposed in the literature for IVN (see Table IV), as indicated by our review. Most of the time, researchers do an excellent job of presenting the necessary ideas on the underlying learning models while omitting the finer details of the system's deployment in the real world.

6) Absence of energy cost estimation and consideration

Another noteworthy observation is the absence of an energy consumption metric in virtually all of the reviewed studies. The need for capturing such a metric might be of less importance in IVNs since they are powered by the CAN bus. However, in small (often battery-powered) devices, like drones, it is important to consider power consumption when designing such IDS/MDS solutions. It is rather surprising, though, that no other works, except Bouhamed et al. [36], considered and evaluated the amount of power consumed by their solution. This omission is quite striking as learning-based systems are notoriously power-hungry, constantly demanding more power resources from their host device.

7) Limited consideration of privacy preservation aspects

In a similar vein, just one paper (Uprety et al. [39]) among all reviewed papers considered privacy. Most of the other papers do not look into the privacy-preserving features of their proposed solutions. This includes IDS and MDS solutions for V2X networks, which have more interconnections than IVNs and UAV networks, increasing the likelihood of a privacy breach. Because user adoption of these systems is dependent on proof of privacy, researchers need to focus more on incorporating privacy as an evaluation parameter for establishing the feasibility of IDS/MDS solutions in vehicular environments.

8) Failure to consider computational, communication, and memory storage metrics

Another key finding from our analysis is that most of the reviewed literature gave minimal thought to evaluating the computational, communication, and memory overhead metrics. While these metrics are independent and should be evaluated separately, we have grouped them together because they are interrelated, and evaluating one without the others does not provide an adequate understanding of the proposed system's feasibility. However, according to our study, none of the recent IDS solutions proposed for IVN and UAVs examined any of these metrics, a surprising trend given the resource-constrained nature of these systems and the complexity of developing learning-based detection models. Similarly, for V2X communications, among all the works reviewed, just one approach (Shu et al. [82]) considered and evaluated all three metrics. This observation calls for more attention from researchers to evaluate these metrics for existing vehicle and UAV capabilities.

9) Limited testbed support and proof-of-concept feasibility

Based on our review, IDS/MDS researchers use essentially two validation approaches. Datasets that are either based on simulated data gathered from public sources or on data collected from real devices. The problem with simply depending on datasets to evaluate the effectiveness of the proposed systems has been discussed in the previous sections as well as in the works of [99] and [17]. The second approach, which has received the least attention, is the use of testbeds. Only 5 publications (3 V2X MBD and 2 IVN-IDS) performed a proof-of-concept through a test simulation to demonstrate the real-world feasibility of their proposed solution out of the 36 analyzed papers. While the reasons for the low percentage are understandable, greater prototyping of IDS/MDS systems is necessary to increase OEM and user trust.

10) Lack of attack prevention and root cause identification

Among all the reviewed papers covering UAVs, V2X, and IVN, only the work of Bouhamed et al. [36] tackled the intrusion prevention problem. The majority of current research focuses on successfully detecting anomalies, with little discussion of how to combat the threats detected in the network. Similarly, none of the studies reviewed looked into locating and determining the source of anomalies in impacted devices. A successful IDS should detect abnormal network traffic and be able to pinpoint where it originated and what triggered it. Thus, in vehicular network contexts, research activities on attack prevention and root cause analysis are required for proposing IDS and MDS solutions.

V. AL/ML-driven IDS/MDS Research Directions

In this section, we examine concepts from other areas of ML and DL with the aim of applying them to address the challenges that currently hinder the widespread adoption of learning-based IDS and MDS solutions in real-world scenarios. By reviewing these ideas, we hope to find ways to improve the effectiveness and practicality of these systems.

A. Concept Drift Issues

As our literature review showed, most proposed solutions are tested on static data, with no regard for the frequent and often dynamic events that happen in the vehicular network. As a result, a system that identifies attacks with a high degree of accuracy may fall short of the required standards soon after deployment. This problem is known as concept drift, and has plagued the field of machine learning for a long time, limiting its application for intrusion detection in highly dynamic contexts such as VANETs and UAVs. Concept drift happens when there is a shift in the data distribution upon which a learning-based detection system is modeled. Since real-world data traffic is generated continuously in non-stationary settings, the trained model struggles to respond dynamically to the constantly changing distribution of incoming data streams. That is why a previously tested high-performing model becomes somewhat ineffective after some time. Many existing methods have been proposed to handle this problem, but their performance and prediction accuracy are limited, prompting the development of alternatives. Next, we review and briefly summarize these techniques for interested readers.

Developing robust learning models with improved drift adaptation performance. Leveraging the ideas proposed by Li et al. [100] on how to design stable and robust drift adaptive models to overcome the performance issues with existing concept drift adaptation methods, an ensemble of base learners can be constructed following the approach outlined next: (i) Collect and sample incoming streams of data to generate a highly representative subset using a clustering algorithm. (ii) Select diverse state-of-the-art drift detection methods and drift adaptation methods to construct an ensemble of high-performing base learners for initial anomaly detection and drift adaptation. (iii) Construct an ensemble model by integrating the prediction probabilities of the base learners based on the methods described in [100]. (iv) Deploy the final ensemble model for anomaly detection and drift adaptation.

Developing robust intrusion detection models that are sustainable over time. Andresini et al. [101] devised a system that combines incremental, active, and transfer learning to solve the issues associated with the non-uniformity of data distribution across time. The proposed methodology updates the model using active learning based on only new data samples to maximize the information gain. It also uses the Nearest Centroid Neighbour classifier to reduce the latency caused by manual labeling and updating. Furthermore, the framework employs a permutation-based variable importance measure to explain how drifts present themselves over time. The proposed framework is divided into three phases:

i. Labeled traces are used to train the intrusion detection model during the initialization phase, while a separate oracle method is employed to estimate the true labels of the incoming data flow.
ii. In the incremental learning phase, new unlabeled traces are consumed and processed in batches of equal size sequentially. The intrusion detection model and the label estimator are updated continuously with new traces that are unlabeled at inference time and have been class-estimated prior to the model update.
iii. The explanation phase calculates the global relevance of features to the detection model's decisions in order to track how the model has evolved to meet the network traffic's drifting characteristics.

B. Decisions Interpretability

The lack of interpretation of learning-based detection systems is another deep concern for their application in safety-critical systems. While traditional decision tree-based ML models typically have good interpretability, the reverse is usually true for their DL counterparts, who typically have higher accuracy but are restricted by their theoretical black-box settings. This inability to gain semantic insights behind the predictions erodes users' and automakers' confidence in vehicular network applications. Although there has been considerable research in this field due to the obvious benefits, we next provide a brief overview of some of the core concepts.

Developing a theoretically provable framework for interpreting IDS decisions. Wang et al. [102] presented a framework based on Shapley Additive exPlanations (SHAP) that improves previous methods by providing a solid theoretical foundation applicable to any IDS model. The proposed framework provides local and global interpretability, and local explanations offer details into each feature value specifics that affect the predicted probabilities. The global explanations extract important features from a dataset and investigate the correlations between feature values and certain types of attacks. Interested readers can refer to [102] for details on implementing the proposed framework.

Producing better explanations and generalizations by infusing domain knowledge. Islam et al. [103] provided a novel approach for creating improved explanations and generalizations of model predictions in diverse network intrusion test cases using public domain knowledge based on the principles of Confidentiality, Integrity, and Availability (CIA). The infused domain knowledge generalizes the intrusion detection model to detect unknown threats while lowering training time and allowing for better model prediction. A feature generalizer and an evaluator are the two components of the proposed method. The feature generalizer takes the dataset's original features and combines them with domain knowledge to create a compact and understandable feature set. Feature mapping, feature ranking, and feature building are the other tasks covered in this step. On the other hand, the evaluator is responsible for executing and comparing the performance of various types of features.

C. Adversarial Attacks on Detection Models

Recent research in computer vision has shown that learning-based models are vulnerable to crafted adversarial attacks, resulting in misclassifications and prediction errors. The lack of interpretability of ML/DL models is one clear reason for this. Attackers leverage this knowledge to create adversarial examples to deceive deployed models in autonomous systems. However, developing secure and adversarially-resistant IDS and MDS is crucial due to the obvious safety-critical nature of such autonomous systems.

Explaining misclassifications using adversarial machine learning. Marino et al. [104] presented a method for generating explanations for a trained classifier's incorrect estimations by determining the smallest changes required to change the model's output. The magnitude of the difference between the modified and original samples is used to visualize the most important features and explain why the samples were misclassified in the first place. This methodology can be adaptable to any classifier with defined gradients and requires no changes to the classifier model. Finally, it gives a mechanism for understanding a classifier's decision boundaries, with the explanation produced from it closely resembling that of a human expert. The stages of the proposed method are briefly outlined below.

i. Misclassified samples from the model prediction are collected and fed into the next step.
ii. The samples are modified until they are successfully classified by solving an optimization problem imposed upon them with an adversarial constraint.
iii. The misclassified and corrected samples are visualized using a dimensionality reduction technique.
iv. Explanations are generated by visualizing the difference between the misclassified and modified samples.

D. Realtime Testbed Evaluations

One of the key issues researchers face when developing IDS and MDS approaches is the lack of real datasets, which is mainly due to the difficulty of launching large-scale tests and data collections. As a result, many of the solutions proposed in the literature are validated using simulated data, which does not accurately represent real-world testing conditions. Given this difficulty, testbed evaluation has been proposed to reproduce the onboard network and components of an external world, representing needed use-cases and driving scenarios in controlled settings.

Developing in-vehicle architecture suitable for real environment trials. Jadidbonab et al. [105] proposed a multi-component testbed representing a flexible and functional in-vehicle architecture for real-world trials of IDS solutions in training, testing, validation, and demonstration. The majority of the vehicle's architecture and CAN-bus network are simulated using the Vector CANoe network simulator. A car simulator, an onboard network simulator, a physical network, a real car's instrument cluster, and a spoofing hardware are all part of the proposed testbed. The driving scenarios are generated using the CARLA simulator data to recreate realistic CAN traffic as input into the CAN Bus. The ECUs used in the testbed were virtualized to resemble those found in a real car. According to the testing results, the proposed testbench can discover issues in attack detection that would otherwise go undetected in an offline test environment.

VI. Concluding Remarks

After conducting a thorough survey, we have examined the feasibility of using learning-based intrusion and misbehavior detection systems in vehicular communication systems for on-land vehicles and UAVs. Despite the significant amount of research in this area, few solutions have been deployed in real-world applications. We believe that this trend is partly due to a lack of emphasis on demonstrating the practicality of proposed approaches in real-world scenarios. Furthermore, current evaluation metrics used in the literature do not adequately measure the feasibility of IDS and MDS solutions.

To address these issues, we analyzed current architectures, realistic threats, and other factors relevant to autonomous vehicles, UAVs, and V2X communication systems. Based on this analysis, we defined baseline requirements for evaluating the feasibility of learning-based IDS/MDS techniques. Subsequently, we reviewed recent papers published in top journals over the past three years ($2020 - 2022$) using these baseline metrics. Our study revealed that most of the reviewed papers did not adequately consider these critical feasibility metrics.

Our analysis has led to the proposal of improvements to current learning-based IDS/MDS solutions based on techniques explored in other ML domains. By highlighting the limitations of current evaluation methods and providing ideas for improvement, we hope that researchers will pay greater attention to making realistic evaluations of their techniques. This, in turn, will lead to increased adoption by the industry, as well as a better understanding of the practicality and feasibility of proposed approaches in real-world scenarios.

References

[1] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: the next computing revolution," in *Design automation conference*. IEEE, 2010, pp. 731–736.

[2] R. Rajkumar, "A cyber–physical future," *Proceedings of the IEEE*, vol. 100, no. Special Centennial Issue, pp. 1309–1312, 2012.

[3] D. Serpanos, "The cyber-physical systems revolution," *Computer*, vol. 51, no. 3, pp. 70–73, 2018.

[4] H. Song, G. A. Fink, and S. Jeschke, *Security and privacy in cyber-physical systems: foundations, principles, and applications*. John Wiley & Sons, 2017.

[5] W. Sun, D. Yuan, E. G. Ström, and F. Brännström, "Cluster-based radio resource management for d2d-supported safety-critical v2x communications," *IEEE Transactions on Wireless Communications*, vol. 15, no. 4, pp. 2756–2769, 2015.

[6] J. E. Siegel, D. C. Erb, and S. E. Sarma, "A survey of the connected vehicle landscapeâarchitectures, enabling technologies, applications, and development areas," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 8, pp. 2391–2406, 2017.

[7] I. Bekmezci, O. K. Sahingoz, and Ş. Temel, "Flying ad-hoc networks (fanets): A survey," *Ad Hoc Networks*, vol. 11, no. 3, pp. 1254–1270, 2013.

[8] M. Quaritsch, K. Kruggl, D. Wischounig-Strucl, S. Bhattacharya, M. Shah, and B. Rinner, "Networked UAVs as aerial sensor network for disaster management applications," *e & i Elektrotechnik und Informationstechnik*, vol. 127, no. 3, pp. 56–63, 2010.

[9] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE J. on Sel. Areas in Comm.*, vol. 25, no. 8, pp. 1557–1568, 2007.

[10] N. Kumar and N. Chilamkurti, "Collaborative trust aware intelligent intrusion detection in vanets," *Computers & Electrical Engineering*, vol. 40, no. 6, pp. 1981–1996, 2014.

[11] H. Sedjelmaci, S. M. Senouci, and M. Feham, "An efficient intrusion detection framework in cluster-based wireless sensor networks," *Security and Comm. Networks*, vol. 6, no. 10, pp. 1211–1224, 2013.

[12] R. Mitchell and R. Chen, "Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications," *IEEE transactions on systems, man, and cybernetics: systems*, vol. 44, no. 5, pp. 593–604, 2013.

[13] J. Grover, N. K. Prajapati, V. Laxmi, and M. S. Gaur, "Machine learning approach for multiple misbehavior detection in vanet," in *International conference on advances in computing and communications*. Springer, 2011, pp. 644–653.

[14] R. van der Heijden, S. Dietzel, and F. Kargl, "Misbehavior detection in vehicular ad-hoc networks," *1st GI/ITG KuVS Fachgespräch Inter-Vehicle Communication. University of Innsbruck*, pp. 23–25, 2013.

[15] S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak, and I. Stojmenovic, "On data-centric misbehavior detection in vanets," in *IEEE Vehicular Technology Conf. (VTC Fall)*. IEEE, 2011, pp. 1–5.

[16] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *2010 IEEE symposium on security and privacy*. IEEE, 2010, pp. 305–316.

[17] Y. Luo, Y. Xiao, L. Cheng, G. Peng, and D. Yao, "Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities," *ACM Comp. Surveys*, vol. 54, no. 5, pp. 1–36, 2021.

[18] H. Bangui and B. Buhnova, "Recent advances in machine-learning driven intrusion detection in transportation: Survey," *Procedia Computer Science*, vol. 184, pp. 877–886, 2021.

[19] A. Boualouache and T. Engel, "A survey on machine learning-based misbehavior detection systems for 5g and beyond vehicular networks," *arXiv preprint arXiv:2201.10500*, 2022.

[20] A. Talpur and M. Gurusamy, "Machine learning for security in vehicular networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, 2021.

[21] W. Wu, R. Li, G. Xie, J. An, Y. Bai, J. Zhou, and K. Li, "A survey of intrusion detection for in-vehicle networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 3, pp. 919–933, 2019.

[22] O. Y. Al-Jarrah, C. Maple, M. Dianati, D. Oxtoby, and A. Mouzakitis, "Intrusion detection systems for intra-vehicle networks: A review," *IEEE Access*, vol. 7, pp. 21 266–21 289, 2019.

[23] L. Yang, A. Moubayed, and A. Shami, "Mth-ids: A multitiered hybrid intrusion detection system for internet of vehicles," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 616–632, 2021.

[24] Q. Abu Al-Haija and A. Al Badawi, “High-performance intrusion detection system for networked uavs via deep learning,” *Neural Computing and Applications*, pp. 1–16, 2022.

[25] J. Kamel, M. R. Ansari, J. Petit, A. Kaiser, I. B. Jemaa, and P. Urien, “Simulation framework for misbehavior detection in vehicular networks,” *IEEE Tran. on Vehicular Technology*, vol. 69, no. 6, pp. 6631–6643, 2020.

[26] X. Liu, L. Yang, I. Alvarez, K. Sivanesan, A. Merwaday, F. Oboril, C. Buerkle, M. Sastry, and L. G. Baltar, “MISO-V: Misbehavior detection for collective perception services in vehicular communications,” in *Intelligent Vehicles Symp.* IEEE, 2021, pp. 369–376.

[27] H. K. Verma, K. P. Sharma *et al.*, “Evolution of vanets to iov: Applications and challenges,” *Tehnički glasnik*, vol. 15, no. 1, pp. 143–149, 2021.

[28] R. Gasmi and M. Aliouat, “Vehicular ad hoc networks versus internet of vehicles-a comparative view,” in *2019 international conference on networking and advanced systems (ICNAS)*. IEEE, 2019, pp. 1–6.

[29] A. A. Yavuz, A. Mudgerikar, A. Singla, I. Papapanagiotou, and E. Bertino, “Real-time digital signatures for time-critical networks,” *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2627–2639, 2017.

[30] A. D. Kumar, K. N. R. Chebrolu, S. KP *et al.*, “A brief survey on autonomous vehicle possible attacks, exploits and vulnerabilities,” *arXiv preprint arXiv:1810.04144*, 2018.

[31] M. A. Khan, A. Safi, I. M. Qureshi, and I. U. Khan, “Flying adhoc networks (fanets): A review of communication architectures, and routing protocols,” in *2017 First International Conference on Latest trends in Electrical Engineering and Computing Technologies (INTELLECT)*. IEEE, 2017, pp. 1–9.

[32] M. O. Ozmen and A. A. Yavuz, “Dronecrypt - an efficient cryptographic framework for small aerial drones,” in *MILCOM 2018 - IEEE Military Communications Conference*, 2018, pp. 1–6.

[33] M. D. Hossain, H. Inoue, H. Ochiai, D. Fall, and Y. Kadobayashi, “An effective in-vehicle can bus intrusion detection system using cnn deep learning approach,” in *GLOBECOM 2020-2020 IEEE Global Communications Conference*. IEEE, 2020, pp. 1–6.

[34] G. Xie, L. T. Yang, Y. Yang, H. Luo, R. Li, and M. Alazab, “Threat analysis for automotive can networks: A gan model-based intrusion detection technique,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4467–4477, 2021.

[35] J. Ashraf, A. D. Bakhshi, N. Moustafa, H. Khurshid, A. Javed, and A. Beheshti, “Novel deep learning-enabled lstm autoencoder architecture for discovering anomalous events from intelligent transportation systems,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4507–4518, 2020.

[36] O. Bouhamed, O. Bouachir, M. Aloqaily, and I. Al Ridhawi, “Lightweight ids for uav networks: A periodic deep reinforcement learning-based approach,” in *IFIP/IEEE Int’l Symp. on Integrated Network Management*. IEEE, 2021, pp. 1032–1037.

[37] M. Xiong, Y. Li, L. Gu, S. Pan, D. Zeng, and P. Li, “Reinforcement learning empowered idps for vehicular networks in edge computing,” *IEEE Network*, vol. 34, no. 3, pp. 57–63, 2020.

[38] R. Sedar, C. Kalalas, F. Vázquez-Gallego, and J. Alonso-Zarate, “Reinforcement learning-based misbehaviour detection in v2x scenarios,” in *2021 IEEE International Mediterranean Conference on Communications and Networking*. IEEE, 2021, pp. 109–111.

[39] A. Uprety, D. B. Rawat, and J. Li, “Privacy preserving misbehavior detection in iov using federated machine learning,” in *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2021, pp. 1–6.

[40] 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, no. 14, p. e4905, 2021.

[41] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham *et al.*, “Experimental security analysis of a modern automobile,” in *2010 IEEE symposium on security and privacy*. IEEE, 2010, pp. 447–462.

[42] Y. Lin, C. Chen, F. Xiao, O. Avatefipour, K. Alsubhi, and A. Yunianta, “An evolutionary deep learning anomaly detection framework for in-vehicle networks-can bus,” *IEEE Tran. on Industry Apps.*, 2020.

[43] M. Hanselmann, T. Strauss, K. Dormann, and H. Ulmer, “Canet: An unsupervised intrusion detection system for high dimensional can bus data,” *Ieee Access*, vol. 8, pp. 58 194–58 205, 2020.

[44] S. Tariq, S. Lee, and S. S. Woo, “Cantransfer: Transfer learning based intrusion detection on a controller area network using convolutional lstm network,” in *Proceedings of the 35th annual ACM symposium on applied computing*, 2020, pp. 1048–1055.

[45] L. Zhang and D. Ma, “A hybrid approach toward efficient and accurate intrusion detection for in-vehicle networks,” *IEEE Access*, vol. 10, pp. 10 852–10 866, 2022.

[46] S.-F. Lokman, A. T. Othman, and M.-H. Abu-Bakar, “Intrusion detection system for automotive controller area network (can) bus system: a review,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1–17, 2019.

[47] Z. Bi, G. Xu, G. Xu, M. Tian, R. Jiang, and S. Zhang, “Intrusion detection method for in-vehicle can bus based on message and time transfer matrix,” *Security and Communication Networks*, vol. 2022, 2022.

[48] H. Lee, S. H. Jeong, and H. K. Kim, “Otids: A novel intrusion detection system for in-vehicle network by using remote frame,” in *2017 15th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2017, pp. 57–5709.

[49] M. D. Hossain, H. Inoue, H. Ochiai, D. Fall, and Y. Kadobayashi, “Long short-term memory-based intrusion detection system for in-vehicle controller area network bus,” in *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 2020, pp. 10–17.

[50] C. Miller and C. Valasek, “Remote exploitation of an unaltered passenger vehicle,” *Black Hat USA*, vol. 2015, no. S 91, 2015.

[51] I. Foster, A. Prudhomme, K. Koscher, and S. Savage, “Fast and vulnerable: A story of telematic failures,” in *9th USENIX Workshop on Offensive Technologies (WOOT 15)*, 2015.

[52] M. Han, P. Cheng, and S. Ma, “Ppm-invids: Privacy protection model for in-vehicle intrusion detection system based complex-valued neural network,” *Vehicular Communications*, vol. 31, p. 100374, 2021.

[53] G. Choudhary, V. Sharma, T. Gupta, J. Kim, and I. You, “Internet of drones (iod): threats, vulnerability, and security perspectives,” *arXiv preprint arXiv:1808.00203*, 2018.

[54] A. Mairaj and A. Y. Javaid, “Game theoretic solution for an unmanned aerial vehicle network host under ddos attack,” *Computer Networks*, p. 108962, 2022.

[55] H. O. Slimane, S. Benouadah, T. T. Khoei, and N. Kaabouch, “A light boosting-based ml model for detecting deceptive jamming attacks on uavs,” in *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 2022, pp. 0328–0333.

[56] N. Adem, B. Hamdaoui, and A. Yavuz, “Mitigating jamming attacks in mobile cognitive networks through time hopping,” *Wireless Communications and Mobile Computing*, vol. 16, no. 17, pp. 3004–3014, 2016. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/wcm.2745

[57] R. Guo, B. Wang, and J. Weng, “Vulnerabilities and attacks of uav cyber physical systems,” in *Proceedings of the 2020 International Conference on Computing, Networks and Internet of Things*, 2020, pp. 8–12.

[58] H. S. Sánchez, D. Rotondo, M. L. Vidal, and J. Quevedo, “Frequency-based detection of replay attacks: application to a quadrotor uav,” in *2019 8th International Conference on Systems and Control (ICSC)*. IEEE, 2019, pp. 289–294.

[59] O. Schell, J. P. Reinhard, M. Kneib, and M. Ring, “Assessment of current intrusion detection system concepts for intra-vehicle communication,” *INFORMATIK 2020*, 2021.

[60] E. T. ETSI, “103 415 v1. 1.1: Intelligent transport systems (its),” *Security; Prestandardization study on pseudonym change management*.

[61] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, “Security analysis of drones systems: Attacks, limitations, and recommendations,” *Internet of Things*, vol. 11, p. 100218, 2020.

[62] Y. Mekdad, A. Aris, L. Babun, A. E. Fergougui, M. Conti, R. Lazzeretti, and A. S. Uluagac, “A survey on security and privacy issues of uavs,” *arXiv preprint arXiv:2109.14442*, 2021.

[63] D. Fallstrand and V. Lindström, “Applicability analysis of intrusion detection and prevention in automotive systems,” Master’s thesis, 2015.

[64] F. Sagstetter, M. Lukasiewycz, S. Steinhorst, M. Wolf, A. Bouard, W. R. Harris, S. Jha, T. Peyrin, A. Poschmann, and S. Chakraborty, “Security challenges in automotive hardware/software architecture design,” in *2013 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2013, pp. 458–463.

[65] A. I. Hentati and L. C. Fourati, “Comprehensive survey of uavs communication networks,” *Computer Standards & Interfaces*, vol. 72, p. 103451, 2020.

[66] S. Stachowski, R. Gaynier, D. J. LeBlanc *et al.*, "An assessment method for automotive intrusion detection system performance," United States. Department of Transportation. National Highway Traffic Safety âŠ, Tech. Rep., 2019.

[67] 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.

[68] 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, no. 2, pp. 373–389, 2019.

[69] J. Lastinec and M. Keszeli, "Analysis of realistic attack scenarios in vehicle ad-hoc networks," in *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*. IEEE, 2019, pp. 1–6.

[70] M. Dibaei, X. Zheng, K. Jiang, S. Maric, R. Abbas, S. Liu, Y. Zhang, Y. Deng, S. Wen, J. Zhang *et al.*, "An overview of attacks and defences on intelligent connected vehicles," *arXiv preprint arXiv:1907.07455*, 2019.

[71] J. den Hartog, N. Zannone *et al.*, "Security and privacy for innovative automotive applications: A survey," *Computer Communications*, vol. 132, pp. 17–41, 2018.

[72] 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.

[73] H. M. Song, J. Woo, and H. K. Kim, "In-vehicle network intrusion detection using deep convolutional neural network," *Vehicular Communications*, vol. 21, p. 100198, 2020.

[74] O. Minawi, J. Whelan, A. Almehmadi, and K. El-Khatib, "Machine learning-based intrusion detection system for controller area networks," in *Proceedings of the 10th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, 2020, pp. 41–47.

[75] K. Zhu, Z. Chen, Y. Peng, and L. Zhang, "Mobile edge assisted literal multi-dimensional anomaly detection of in-vehicle network using lstm," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 5, pp. 4275–4284, 2019.

[76] K. Agrawal, T. Alladi, A. Agrawal, V. Chamola, and A. Benslimane, "Novelads: A novel anomaly detection system for intra-vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, 2022.

[77] A. K. Desta, S. Ohira, I. Arai, and K. Fujikawa, "Rec-cnn: In-vehicle networks intrusion detection using convolutional neural networks trained on recurrence plots," *Vehicular Communications*, vol. 35, p. 100470, 2022.

[78] P. Cheng, K. Xu, S. Li, and M. Han, "Tcan-ids: Intrusion detection system for internet of vehicle using temporal convolutional attention network," *Symmetry*, vol. 14, no. 2, p. 310, 2022.

[79] Y. Xun, Y. Zhao, and J. Liu, "Vehicleeids: A novel external intrusion detection system based on vehicle voltage signals," *IEEE Internet of Things Journal*, 2021.

[80] A. R. Javed, S. Ur Rehman, M. U. Khan, M. Alazab, and T. Reddy, "Canintelliids: detecting in-vehicle intrusion attacks on a controller area network using cnn and attention-based gru," *IEEE transactions on network science and engineering*, vol. 8, no. 2, pp. 1456–1466, 2021.

[81] T. Alladi, V. Kohli, V. Chamola, F. R. Yu, and M. Guizani, "Artificial intelligence (ai)-empowered intrusion detection architecture for the internet of vehicles," *IEEE Wireless Communications*, vol. 28, no. 3, pp. 144–149, 2021.

[82] J. Shu, L. Zhou, W. Zhang, X. Du, and M. Guizani, "Collaborative intrusion detection for vanets: a deep learning-based distributed sdn approach," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4519–4530, 2020.

[83] L. Nie, Z. Ning, X. Wang, X. Hu, J. Cheng, and Y. Li, "Data-driven intrusion detection for intelligent internet of vehicles: A deep convolutional neural network-based method," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 4, pp. 2219–2230, 2020.

[84] F. Gonçalves, J. Macedo, and A. Santos, "Intelligent hierarchical intrusion detection system for vanets," in *2021 13th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*. IEEE, 2021, pp. 50–59.

[85] D. Kosmanos, A. Pappas, F. J. Aparicio-Navarro, L. Maglaras, H. Janicke, E. Boiten, and A. Argyriou, "Intrusion detection system for platooning connected autonomous vehicles," in *2019 4th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*. IEEE, 2019, pp. 1–9.

[86] C. Sommer, D. Eckhoff, A. Brummer, D. S. Buse, F. Hagenauer, S. Joerer, and M. Segata, "Veins: The open source vehicular network simulation framework," in *Recent advances in network simulation*. Springer, 2019, pp. 215–252.

[87] F. A Ghaleb, F. Saeed, M. Al-Sarem, B. Ali Saleh Al-rimy, W. Boulila, A. Eljialy, K. Aloufi, and M. Alazab, "Misbehavior-aware on-demand collaborative intrusion detection system using distributed ensemble learning for vanet," *Electronics*, vol. 9, no. 9, p. 1411, 2020.

[88] P. A. Lopez, M. Behrisch, L. Bieker-Walz, J. Erdmann, Y.-P. Flötteröd, R. Hilbrich, L. Lücken, J. Rummel, P. Wagner, and E. Wießner, "Microscopic traffic simulation using sumo," in *2018 21st international conference on intelligent transportation systems (ITSC)*. IEEE, 2018, pp. 2575–2582.

[89] I. A. Khan, N. Moustafa, D. Pi, W. Haider, B. Li, and A. Jolfaei, "An enhanced multi-stage deep learning framework for detecting malicious activities from autonomous vehicles," *IEEE Transactions on Intelligent Transportation Systems*, 2021.

[90] H.-Y. Hsu, N.-H. Cheng, and C.-W. Tsai, "A deep learning-based integrated algorithm for misbehavior detection system in vanets," in *Proceedings of the 2021 ACM International Conference on Intelligent Computing and its Emerging Applications*, 2021, pp. 53–58.

[91] P. Sharma and H. Liu, "A machine-learning-based data-centric misbehavior detection model for internet of vehicles," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4991–4999, 2020.

[92] X. Wang, Y. Zhu, S. Han, L. Yang, H. Gu, and F.-Y. Wang, "Fast and progressive misbehavior detection in internet of vehicles based on broad learning and incremental learning systems," *IEEE Internet of Things Journal*, 2021.

[93] F. Hawlader, A. Boualouache, S. Faye, and T. Engel, "Intelligent misbehavior detection system for detecting false position attacks in vehicular networks," in *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2021, pp. 1–6.

[94] A. Sharma and A. Jaekel, "Machine learning based misbehaviour detection in vanet using consecutive bsm approach," *IEEE Open Journal of Vehicular Technology*, vol. 3, pp. 1–14, 2021.

[95] S. Ercan, M. Ayaida, and N. Messai, "Misbehavior detection for position falsification attacks in vanets using machine learning," *IEEE Access*, vol. 10, pp. 1893–1904, 2021.

[96] S. Gyawali, Y. Qian, and R. Q. Hu, "Machine learning and reputation based misbehavior detection in vehicular communication networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 8871–8885, 2020.

[97] J. Whelan, A. Almehmadi, and K. El-Khatib, "Artificial intelligence for intrusion detection systems in unmanned aerial vehicles," *Computers and Electrical Engineering*, vol. 99, p. 107784, 2022.

[98] N. Moustafa and A. Jolfaei, "Autonomous detection of malicious events using machine learning models in drone networks," in *Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond*, 2020, pp. 61–66.

[99] G. Loukas, E. Karapistoli, E. Panaousis, P. Sarigiannidis, A. Bezemskij, and T. Vuong, "A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles," *Ad Hoc Networks*, vol. 84, pp. 124–147, 2019.

[100] L. Yang, D. M. Manias, and A. Shami, "Pwpae: An ensemble framework for concept drift adaptation in iot data streams," *arXiv preprint arXiv:2109.05013*, 2021.

[101] G. Andresini, F. Pendlebury, F. Pierazzi, C. Loglisci, A. Appice, and L. Cavallaro, "Insomnia: towards concept-drift robustness in network intrusion detection," in *Proceedings of the 14th ACM Workshop on Artificial Intelligence and Security*, 2021, pp. 111–122.

[102] M. Wang, K. Zheng, Y. Yang, and X. Wang, "An explainable machine learning framework for intrusion detection systems," *IEEE Access*, vol. 8, pp. 73 127–73 141, 2020.

[103] S. R. Islam, W. Eberle, S. K. Ghafoor, A. Siraj, and M. Rogers, "Domain knowledge aided explainable artificial intelligence for intrusion detection and response," *arXiv preprint arXiv:1911.09853*, 2019.

[104] D. L. Marino, C. S. Wickramasinghe, and M. Manic, "An adversarial approach for explainable ai in intrusion detection systems," in *IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society*. IEEE, 2018, pp. 3237–3243.

[105] H. Jadidbonab, A. Tomlinson, H. N. Nguyen, T. Doan, and S. Shaikh, "A realtime in-vehicle network testbed for machine learning-based ids training and validation," in *AI-CyberSec 2021: Workshop on Artificial Intelligence and Cyber Security*. CEUR Workshop Proceedings, 2021, pp. In–Press.