drones

Review

The Evolution of Intelligent Transportation Systems: Analyzing the Differences and Similarities between IoV and IoFV

Dušan Herich *,† and **Ján Vaščák** *,†

Department of Cybernetics and Artificial Intelligence, Faculty of Electrical Engineering and Informatics, Technical University of Kosice, 042 00 Kosice, Slovakia

* Correspondence: dusan.herich@tuke.sk (D.H.); jan.vascak@tuke.sk (J.V.)

† These authors contributed equally to this work.

Abstract: The Internet of Vehicles (IoV) and the Internet of Flying Vehicles (IoFV) are integral components of intelligent transportation systems with the potential to revolutionize the way we move people and goods. Although both the IoV and IoFV share a common goal of improving transportation efficiency, safety, and sustainability, they possess distinct characteristics and face unique challenges. To date, the existing literature has predominantly focused on specific aspects of either the IoV or IoFV, but a comprehensive review comparing and contrasting the two domains is still lacking. This review paper aims to address this gap by providing an in-depth analysis of the key differences between the IoV and IoFV systems. The review will examine the technological components, network infrastructure, communication protocols, data management, objectives, applications, challenges, and future trends associated with both domains. Additionally, this paper will explore the potential impact of technologies such as artificial intelligence, machine learning, and blockchain. Ultimately, the paper aims to contribute to a deeper understanding of the implications and potential of these technologies, both in the context of transportation systems and beyond.

Keywords: IoV; IoFV; communication; computation; application; UAV; vehicle

check for updates

Citation: Herich, D.; Vaščák, J. The Evolution of Intelligent Transportation Systems: Analyzing the Differences and Similarities between IoV and IoFV. *Drones* **2024**, *8*, 34. https://doi.org/10.3390/drones8020034

Academic Editor: Emmanouel T. Michailidis

Received: 30 November 2023
Revised: 20 January 2024
Accepted: 22 January 2024
Published: 24 January 2024

1. Introduction

The steady growth of the traffic volume in all modes of transportation [1] results in the necessity to maintain and manage traffic flow effectively. Currently, human-operated traffic systems characterized by a low level of cooperation and information sharing are often approaching their capacity. For that reason, there are ongoing attempts [2] to optimize traffic flow by interconnecting individual vehicles. Such interconnection can enhance the effectiveness and safety of those systems by introducing fully or partially autonomous operation and improving operators' awareness by providing information relating to the system's condition, such as bottlenecks, accidents, or unsafe operating conditions. In addition, novel means of transport are being introduced to already busy transportation systems, while the underlying infrastructure remains unimproved. Growth in the popularity and utilization of quadrocopters, otherwise known as drones or Unmanned Aerial Vehicles (UAVs), can serve as an example. The increasing presence of quadrocopters operated by a person has been causing damage to infrastructures, vehicles, and health [3], which may be attributed to poor or nonexisting cooperation among vehicles in different systems, especially in areas characterized by high traffic flow and the operation of UAVs by a human, without the requirement for certification [4]. Effective cooperation could improve the effectiveness and safety of those systems by providing a means for the improved planning of routes, collision avoidance, collecting data about the environment more broadly, and sharing the infrastructure [5].

While earlier works have been primarily focused on the simple provisioning of information in a timely and reliable manner, newer approaches attempt to broaden the functionality of previous systems with the goal of autonomous operation. However, in the case of UAVs, autonomy is established more widely than in ground vehicles, such as cars. Building on advancements in communication technologies [6], hardware [7] and software, particularly artificial intelligence [8], the usage of (connected) vehicles is predicted to grow in consumer, civil, and military applications [9].

Additionally, the onset of light and ultralight UAVs, particularly quadrocopters, has expanded the application potential even further, primarily in the areas of healthcare for delivering and retrieving COVID-19 self-testing kits, surveillance systems for the identification of violent individuals [10], or pesticide application on crops [11].

A wide range of those applications relies on algorithms and methods that are resource-intensive. However, ground and aerial vehicles are constrained in resources for power, computation, and storage capacity. Those constraints become more pronounced under the consideration that vehicles are not only required to perform tasks of a specific application, but they are required to navigate in the environment safely [12]. Such applications undoubtedly require resources for sensing, communication, and navigation itself, which includes, but is not limited to, localization, mapping, path planning, obstacle avoidance, or the coordination of multiple vehicles. To overcome the limitation caused by scarce resources, vehicular networks using means of the cloud, edge, and fog computing, coupled with the concepts of big data and new generation mobile networks, provide transportation systems with more secure and reliable connections, as well as virtually unlimited computing and storage resources found in remote cloud data centers [13].

The accelerating need to interconnect vehicles to enhance the performance of traffic systems results in an increasing number of systems being proposed and implemented. Even though those systems have similar goals, they often undertake different approaches. They undergo evolutionary advancements, such as the introduction of cognition, which may not propagate to other designs caused by rapid development [14]. Therefore, this proposal focuses on summarizing the technologies and approaches used in transport systems for ground and aerial vehicles, thereby identifying the differences and common grounds to enable easier cooperation and infrastructure sharing. In particular, we will focus on vehicular ad hoc networks for both flying and vehicular vehicles and networks building on the Internet of Things, together with an enhancement that was introduced: the Internet of Vehicles, the Cognitive Internet of Vehicles, and the Internet of Flying Vehicles.

2. Background

The development of vehicular networks is tightly bound to the development of other so-called enabling technologies, particularly in communication and computation. This includes cloud computing with its related edge and fog computing paradigms or new generation cellular networks such as fifth generation (5G) or beyond 5G. The employment of those technologies in individual networks is diverse. Therefore, this section provides a brief description of those networks and the manner in which the enabling technologies are used. Table 1 provides a summary of the considered networks.

2.1. VANET

Vehicular ad hoc networks (VANETs) are an adaptation of mobile ad hoc networks (MANETs) for transport. In VANETs, each vehicle serves as a network node equipped with an onboard unit. The purpose of the onboard unit is to facilitate communication with other vehicles and infrastructure in the network. VANETs have inherent similarities to MANETs, especially in their capability to operate without a set infrastructure and mobility of nodes. However, the mobility of nodes, that is, individual vehicles, can be significantly higher than in VANETs, which means that the network topology of MANETs is subject to more rapid changes than in VANETs. The consideration of vehicles as network nodes has further implications, for example, in the variability of node density and the stability of the connection [15].

Table 1. Comparison of vehicular networks.

Feature	VANET	FANET	IoV	IoFV
Type of network	Vehicular	Flying	Vehicular	Flying
Communication range	Short	Medium to Long	Short to Medium	Medium to Long
Mobility	Road-based	Air-based	Road-based	Air-based
Infrastructure	Roadside units	Limited ground infrastructure	Roadside units, Cloud	Ground stations, Cloud
Challenges	Signal obstruction, Interference, Dynamic topology changes	Limited energy, Collision avoidance	Signal interference, Dynamic topology changes, Security concerns	Limited energy, Communication security concerns
Applications	Intelligent Transportation Systems, Emergency services	Surveillance, Environmental monitoring	Traffic management, Fleet management, Safety applications	Surveillance, Environmental monitoring, Disaster response

In contrast to MANETs, where nodes can move freely, the nodes in VANETs are usually constrained by available roads and by the flow of traffic. Therefore, suitable technologies for connection may differ in areas with dense traffic, where vehicles can use dedicated short-range communication (DSRC) for vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communication [16] to areas with sparse traffic, where a vehicle can be disconnected from the rest of the network. In such cases, the DSRC is nowadays replaced with 5G, thereby allowing the vehicle to stay connected [17]. However, the poor connection stability of VANETs initially contributed to their low usability, and the lack of computing and storage capacity, mostly restricted to onboard capacities, has made the implementation of intelligent applications arduous [18]. To overcome this setback, a range of work focused on introducing vehicles-as-cloud or the vehicular cloud has emerged [19], thereby enabling vehicles to pool their resources with, however, the disadvantage of inconsistent availability. The intermittent connections by which the VANET is characterized pose further risks and problems in the wide adoption of this technology. The short duration of connection and, therefore, frequent disconnections make it difficult to retain the confidentiality and integrity of messages, especially without a centralized governing authority, which requires the usage of a wide range of authentication and message encryption protocols [20].

Ad hoc-enabled automobile communities were one of the first uses for VANET systems. With the aid of this application, a group of automobiles might be identified or made to self-identify as a community. This group of automobiles would represent a subset of those on the road who share the same objectives. This objective can, for instance, transport a group of people to the exact location or get a group of emergency personnel to arrive to the same place. Once the vehicles come into contact on the road, they will likely remain concurrent as they travel, since they are all attempting to reach the same destination. This makes it possible to create a more reliable communication scheme, which in normal conditions is quite difficult for VANETs [21].

2.2. FANET

The flying ad hoc networks (FANETs) are developing on the basis of VANETs. However, the focus is primarily on flying vehicles. Even though both networks can be considered as a subclass of MANETs, there are constraints, such as node mobility, speed, and density, present that require distinction [22].

From a connection and communication standpoint, the primary difference is that no roadside units are present. Their futility stems from the assumption that vehicles may not necessarily operate on a set path; instead, they roam space freely [23]. Hence, FANETs use the concept of base stations serving as a gateway for communication. Under those circumstances, the usage of DSRC is obstructed in contrast to in VANETs. Instead, either satellite communication or 5G networks can be utilized to secure the connection. A suitable technology differs among applications and needs to be considered individually [24].

Similarly to vehicles in VANETs, the computing capability of individual vehicles is limited. However, especially in small UAVs, this limitation is amplified by the constrained carrying capacity of a singular vehicle. For this reason, mobile edge computing is frequently used to offload and load balance tasks among UAVs. This approach enables cooperation in solving complex tasks, but it is necessary to consider both energy and communication constraints [25].

Application scenarios of FANETs can be divided into three main categories [26]; the first one is surveillance, in which UAVs have the function of flying cameras. Usually, the duties entail processing real-time pictures, video, or audio from flying objects to gather critical information. For instance, UAVs may be used in search and rescue operations to locate a target, usually on the ground. Another situation that might utilize a FANET as an observational infrastructure is traffic and urban monitoring. Aerial reconnaissance operations can be used for everything from law enforcement efforts to gathering data about battlefields in a military environment. Another application setting is in agricultural management. Another class similar to the prior is environmental monitoring, in which UAVs serve as sensors gathering information from a specified area. Physical parameters, including temperature, humidity, pressure, light intensity, and pollution level, are frequently analyzed using UAV sensor networks [27]. The last class that has seen increased utilization in recent years is the deployment of connectivity in places that require a particular type of communication. In order to effectively and securely send data gathered by ground sensors to remote control centers and to extend the communication range of relaying ground nodes, autonomously flown UAVs are being employed as airborne communication relays [26].

2.3. IoV

In order to support requests arising from the new era of mobility, such as advanced driving assistants or autonomous driving, systems of intelligent vehicles are moving from communication models in VANETs toward the Internet of Vehicles (IoV) [28].

An IoV network may use concepts similar to its predecessor—VANETs. This can be observed mainly in communication models such as V2V, V2I, and others. The IoV, however, is not limited only to a few specific models; on the premise of the Internet of Things (IoT), it employs vehicle-to-everything communication (V2X). Due to the V2X communication model, the IoV may use various technologies for connection, including wireless LAN (WLAN) networks and cellular networks such as 5G or Bluetooth [29].

The limitations of VANETs in computation and storage are becoming overcome thanks to the employment of remote computation in the form of cloud, edge, and fog computing. This enables the IoV to process big data collected from the environment and consecutively improve the system's performance. The IoV networks can face security issues similar to those observed in the VANET; however, there are attempts to alleviate the constraints through the employment of novel concepts such as blockchain [30] or deep learning algorithms [31], wherein each is enabled by a higher communication throughput and generally better computation and storage resources. The four main kinds of IoV applications for intelligent transportation are safety-based, efficiency-based, comfort-based, and information/entertainment-based applications. By identifying potential collision scenarios within the transportation system, safety-based IoV applications seek to avoid or reduce the number of accidents. When collision avoidance system (CAS) information is shared with nearby vehicles in the IoV, these are known as the cooperative collision avoidance system (CCAS). IoV applications that focus on comfort try to inform drivers in a way that will make the journey enjoyable and comfortable. This could contain data on the weather, route navigation, parking lot information, and the locations of information kiosks for tourists, restaurants, gas stations, and other facilities. Applications that focus on efficiency try to increase the mobility of vehicle items inside the IoV network. The timing of traffic signals at intersections based on the volume of traffic to minimize waiting times is an example application. Applications based on information and entertainment are intended to provide drivers and passengers with information about amusement. Access to the internet and other file-sharing services would fall under this category. Due to the dynamic and evolving nature of the vehicle objects in the IoV network, it is currently difficult to provide vehicles with access to the global internet and maintain the information [32].

2.4. IoFV

The goal of the Internet of Flying Vehicles (IoFV) is, similarly to the IoV, the integration of the IoT and vehicles. Such integration could support an even wider adoption of UAVs by enhancing their applicability similarly as it was demonstrated with the IoV. The relationship between FANETs and the IoFV is comparable to the one observed in VANETs and the IoV. Therefore, both networks engage in similar communication models, especially UAV-to-UAV and UAV-to-base station. Differences between those two networks in connection and communication are less significant than in their ground vehicle counterparts due to the development of FANETs later in time. Like its counterpart of the IoV, the IoFV adopts cloud, edge, and fog computing to analyze data and accomplish complex tasks requiring the coordination, control, and analysis of collected data, which are then normally transmitted to the base stations for processing [33]. Eventually, when edge computing is integrated into the network, the computing load is reduced as a result of processing parts of the data locally, thus also reducing time latency and enabling real-time applications.

The applications of the IoFV remain similar to those observed in FANETs. A specific example is the usage of smart agriculture to improve the efficiency of production and optimize crop quality while simultaneously minimizing the negative impact on the environment. Other applications include disaster recovery, in which UAVs help manage natural disasters such as fires, floods, earthquakes, or storms. This application domain utilizes UAVs to collect environmental data from sensors in disaster-prone locations. The collected data describes critical environmental parameters, such as temperature, humidity, luminosity, strain, and stress, which enables undertaking and appropriate actions even before the disaster occurs [33].

3. Building Blocks of Vehicular Networks

Each vehicular network implements several components that are vital for its operation. Although they are known under various names, they frequently fulfill similar or equal operations. In order to enable closer cooperation between networks designed for ground vehicles and those for flying ones, it is essential to identify those components and their similarities and differences to outline possible modifications.

3.1. Sensors

This category of sensors mounted directly on a vehicle can aid in two primary tasks: motion control and data acquisition. In movement control, air and ground vehicles frequently utilize accelerometers and gyroscopes to determine the position and orientation of a vehicle, which enables the control system to maintain a desired path or position of a vehicle, particularly in cooperation with other sensory equipment such as modules for global positioning systems or cameras [34]. Several factors may determine the selection from a range of available sensors. Primarily, it is necessary to consider constraints on energy, weight, available space, connection, and a motion control system. Furthermore, an intended application must be taken into consideration. Analogously to the sensors for movement control, the use of data acquisition sensors is determined by available energy, weight, available space, and connection performance [30]. This category may include cameras, LiDARs, ultrasonic sensors, or radio frequency identification. Ideally, the selected sensors would function for movement control and data acquisition.

3.2. Onboard Units

The computing onboard of a vehicle is secured by an onboard unit (OBU). This typically includes several components, including single board computers for computing, read/write memory for information storage and retrieval, and network devices tasked with establishing a connection to the rest of the network [35]. The main objectives of the OBU are collecting data from onboard sensors, controlling actuators, transmitting messages, and ensuring data security.

Further onboard computing is provided by the application unit (AU), which is currently limited to use in ground vehicles. The AU is designed to run specific applications. It is defined as a device inside the vehicle communicating via an OBU, which also may function in the role of an AU, or it can be a personal device such as a smartphone [18]. Although the definition of an AU found in ground vehicle networks expects it to be onboard [18], it is possible to find components similar in function for UAVs. An example may be found in small quadrocopters where a smartphone runs an application that directly interacts with a UAV onboard unit, thereby enabling manual control of the vehicle and providing information about its state or invoking autonomous actions, which are then carried out by the onboard unit on a quadrocopter.

3.3. Base Stations

Even though some vehicular networks do not need to rely on pre-existing infrastructure for operation, many employ devices that can be denoted as base stations. These are known as roadside units in networks of ground vehicles, and in UAV networks, those are labeled as ground control stations or base stations [36].

RSUs are designated to extend the communication range in vehicular networks by forwarding information to either onboard units or other RSUs, thereby providing access to networks such as the internet. In some systems, they serve as edge computing devices enabling the reliable operation of time-critical applications by processing data before they are sent to a cloud or by running applications locally, thus ensuring a lower latency.

Similarly, base stations or ground control stations are used to extend the range of communication among UAVs, offload tasks from onboard units to enable time-sensitive applications, establish the connection of vehicular network to other networks, and preprocess data before they are moved to a cloud [37]. Both RSUs and base stations are intended to be placed in geographical proximity to vehicles. They can be installed at a fixed location, or other vehicles may operate in the role of base station/RSU. It may be a bus moving on a scheduled route at a scheduled time or a UAV hovering at a set altitude, which would then be known as an aerial base station [38].

3.4. Clouds

Remote computing in the form of cloud computing is gaining importance in vehicular networks. This paradigm distinguishes newer networks based on the IoT from earlier systems such as VANETs. Leveraging the capabilities of remote cloud data centers such as on-demand service, resource pooling, and rapid elasticity facilitates the usage of big data and artificial intelligence with the aim of providing improved performance for both networks and applications [39]. Even though cloud computing aids in the performance of those systems, it has been shown to be vital to employ edge and fog computing concepts due to the time sensitivity of some applications, which may be observed in using base stations as edge devices [40]. Even though these paradigms helped vehicular networks to gain traction by providing virtually unlimited means for computation and storage, several new problems arose, such as which processes should be moved to the cloud or edge and when.

4. Layered Models

The lack of standardization in the developing areas in interconnected transportation systems has led to numerous models being proposed. Systems concerned with ground vehicles often separate functionality among various layers as illustrated in the Figure 1, with each performing a particular function or a set of functions [41]. However, systems designed for UAVs frequently lack this distinct separation [42]. Therefore, this section identifies specific layers in systems designed for ground vehicles and delineates common points with UAV networks to facilitate structuring them into layers. This is vital because even though both ground vehicle networks and UAV networks are undergoing rapid evolution, advances in ground vehicle networks are rarely reflected in UAV networks and vice versa [37]. An example is Cognitive IoV, which introduces cognition to the networks for the more efficient management of infrastructure and resources; this approach is not clearly defined in UAV networks despite its use in certain applications. In addition, such unification may advance the cooperation of both transport modes.

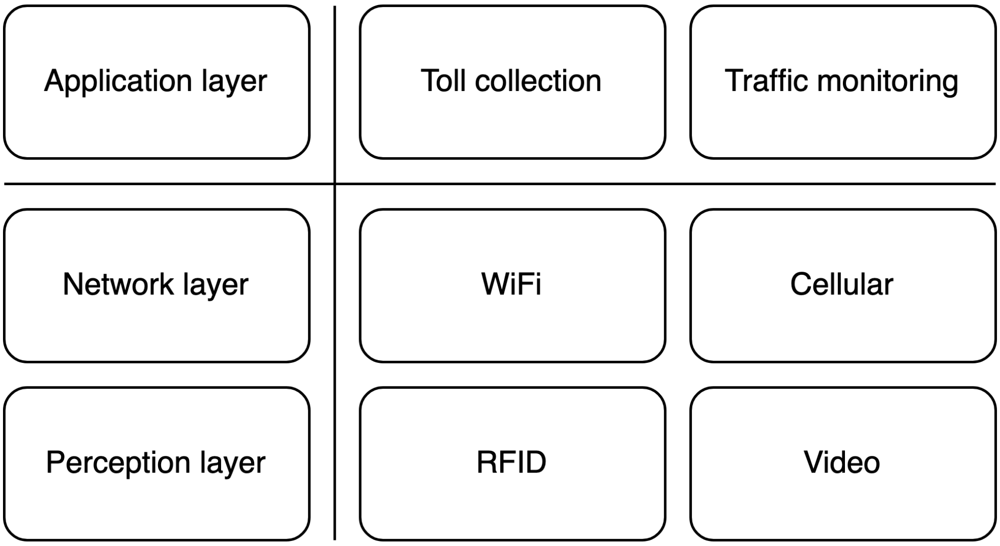

Figure 1. IoV layered model without the cognition layer. Adapted from [43].

While designs may vary, discernible patterns emerge in the layers and functionality of different models. Four fundamental layers can be identified, namely, sensory, communication, cognition, and application. The layers of some existing models and their characteristics are summarized in Table 2.

Table 2. Overview of current IoV architectures.

Reference	Layers	Applications
[44]	Data, Virtualization, Control, Application	See-Through, Collision Warning
[45]	Sensing, Communication, Cognition, Control, Application	Safety, Transportation Management
[46]	Perception, Communication, Application	Vehicle Collaboration
[47]	User, Data Acquisition, Filtering, Communication, Control, Processing	Traffic Efficiency, Safety

4.1. Sensory Layer

For the collaboration of vehicular networks, it is crucial to collect heterogeneous data describing the internal state of a vehicle and environmental data about the vehicle's surroundings. Furthermore, if the network is aimed to employ cognition to improve performance, those data should also encompass the state of the network [48]. The sensory layer, as the lowest one, encompasses all sensors present in the network, and its principal objective is to collect and potentially preprocess data collected from multiple sources, including the surroundings of a vehicle from both onboard and offboard sensors, data for movement control, and data regarding a network state, that is, traffic or resource utilization, among others. Vehicles can realize this functionality by integrating onboard sensors and units, which can collect and classify various types of data and transmit them to upper layers [49].

In certain designs, like the one depicted in Figure 2, this particular layer might not be explicitly delineated, as has been observed in prior work [44]. However, in architectures specifically detailing sensory components [45], its role involves aggregating diverse data from various origins, such as physical space, network traffic, and resource distribution within the network. Consequently, the collection of data extends to internal vehicle sensors, navigation systems [50], intervehicle communication, traffic lights, or other environmental devices [47].

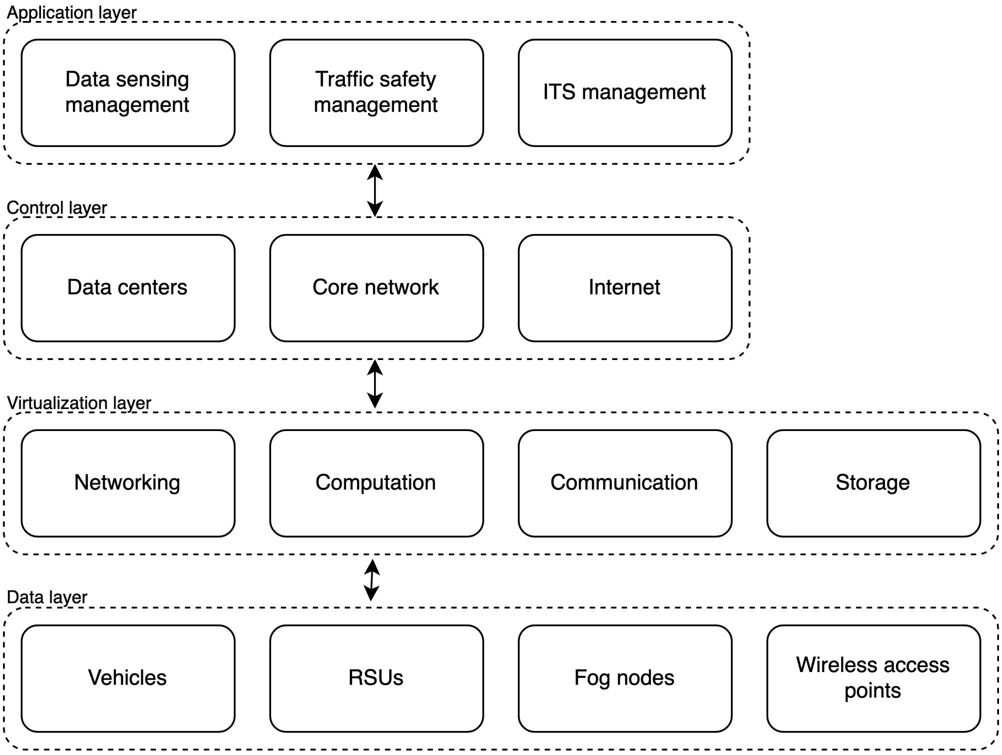

Figure 2. Architecture of IoV model merging sensing and communication layer [44].

4.2. Communication Layer

The second layer can be broadly characterized as a connectivity layer that supports previously delineated communication frameworks, particularly the V2X. Its fundamental role revolves around the establishment and sustenance of wireless links with established networks like Wi-Fi, Bluetooth, or 5G.

This functionality is incorporated into the data layer in the framework proposed by [51], where wireless communication nodes are endowed with additional resources for storage and computation. These resources are somewhat abstracted as fog nodes, thereby facilitating the decentralized provisioning of services. In a different approach outlined in [45], a hybrid cloud/edge architecture was employed for communication utilizing pertinent wireless technologies. The rationale behind adopting this architecture is the imperative need for real-time data exchange and processing among intelligent devices. Leveraging the edge computing paradigm allows models built on this architecture to handle time-sensitive data from moving vehicles, thus progressively offloading other data to the cloud for comprehensive computation and analysis.

In the work presented by [46], the layer employs conventional routing protocols that are contingent on the geographical positioning of nodes within the network, the topology, and vehicle clustering. Additionally, it incorporates graph and path planning algorithms for the discovery of the most efficient routing paths.

4.3. Cognitive Layer

The IoV and the IoFV cognitive layer is a key component in the implementation and planning of these networks. The cognitive layer has the task of providing the vehicles with the ability to perform complex tasks and to interact securely, efficiently, and intelligently with their environment and network [52].

In the context of the IoV, the cognitive layer can offer a range of services and functionalities that enable the vehicles to manage traffic, communicate with other vehicles and other objects, and utilize cooperative intelligent transportation systems (C-ITSs). The cognitive layer in the IoV can be presumed to be the layer that gives the underlying communication and control systems intelligence [53]. It also permits the vehicles to make rigorous decisions based on the information they receive from their surroundings. The cognitive layer in the IoFV has the responsibility for providing the vehicles the ability to communicate with one another and the infrastructure, as well as to make defensible decisions based on the information they gather from their surroundings. The cognitive layer, sometimes referred to as a cognitive radio [54], is likewise vital in the IoFV; however, it is primarily focused on providing the flying vehicles with the ability to sense and interact with their surroundings and the network in a safe and effective manner. Applications including collision avoidance, autonomous flight, and traffic management are frequently supported by this layer. The discussed layer provides flying vehicles with the ability to carry out enumerated tasks by providing them with the capability to sense their surroundings and the network's conditions and react to them in a secure and effective way [55].

This layer can be seen as a shared responsibility between the vehicles, infrastructure, and network. Vehicles feed sensor data and control signals to the layer; the infrastructure collects and shares environmental data to the layer and also enables the vehicles to communicate and cooperate with each other. Furthermore, the data from the network operation are processed in the cognitive layer to ensure a safe, efficient, and reliable network connection [56]. As such, this layer is vital for the further development of vehicular networks due to the fact that it allows the vehicles to perform advanced applications and interacts with the environment and network in a safe, efficient, and intelligent manner.

Within the realm of the Internet of Vehicles (IoV), the cognitive layer plays a role in applications including traffic prediction, management adaptive routing, and decision making for autonomous vehicles. By leveraging real-time data from interconnected vehicles, the cognitive layer can analyze traffic patterns to predict congestion and dynamically adjust routes to optimize traffic flow [57]. Additionally, it enables maintenance by monitoring vehicle health data, thereby reducing downtime and improving operational efficiency [58].

In the domain of the Internet of Flying Vehicles (IoFV) the cognitive layer tackles challenges associated with mobility. It facilitates navigation, collision avoidance, and airspace management for drones and other flying vehicles [59]. Through algorithms, the cognitive layer ensures efficient flight paths by considering factors like weather conditions, airspace regulations, and the presence of other aerial vehicles [60]. This capability is crucial for integrating flying vehicles into environments to enable applications such as aerial deliveries, surveillance operations, and emergency response.

In both the IoV and IoFV contexts alike, the cognitive layer also plays a role in communication protocols that enable intelligent vehicle-to-vehicle communication as well as interaction with infrastructure components. This communication is essential for synchronized decision-making processes and enhancing system resilience [61]. In general, the utilization of the layer in the Internet of Vehicles (IoV) and the Internet of Flying Vehicles (IoFV) plays a role in building transportation ecosystems that are intelligent, highly adaptable, and that prioritize safety.

In conclusion, the cognitive layer in the IoV and IoFV plays a critical role in enabling safe, efficient, and intelligent interactions between vehicles and their environments and networks. To maintain the progress and advancement of these networks, ongoing research and development efforts are necessary for the cognitive layer in both the IoV and IoFV.

4.4. Application Layer

The application layer, here referred to as the fourth layer, is tasked with the storage, analysis, and processing of data collected through network operations [62]. To fulfill this function, it incorporates high-capacity storage and processing infrastructure, as well as tools for the analysis of data sourced from the network and its components.

The fundamental objective of this layer is to equip nodes with the capability to process extensive data from diverse origins, thereby enabling the evaluation of various risks and circumstances arising in traffic scenarios [58]. Such scenarios may encompass hazardous vehicle movement conditions, traffic congestion, or emergency events.

The implementation described in [44] incorporates a pair of functionalities within this layer; they are specifically denoted as the “see-through” and “collision warning” services. The operation of these services relies on cloud computing technologies featuring adaptable resource scheduling.

In the work presented by [45], services designed for the coordination and collaboration of multiple vehicles and autonomous driving are instantiated. The model they employed facilitates the deployment of additional services, thereby categorizing them into two distinct groups: customized application services targeted at mitigating safety risks in traffic and intelligent transportation applications encompassing intelligent driving and transportation management.

The model outlined in [47] employs protocols like HTTP REST, advanced message queuing protocol, and extensible messaging. It elucidates the protocol employed within the Internet of Things (IoT) network, thereby illustrating its applicability in the context of the Internet of Vehicles (IoV).

5. Communication in Vehicular Networks

Despite the significant advancements these technologies have brought to transportation, they also pose unique communication challenges. Our investigation encompasses various connection and communication methods that enable vehicles to communicate with each other and with the infrastructure. The utilization of wireless communication technologies, such as cellular networks, ad hoc networks, and satellite communications, to support the IoV and IoFV will be thoroughly analyzed. Moreover, we scrutinize the critical considerations that must be taken into account in the design and implementation of these communication systems, including security, scalability, and reliability issues.

5.1. Communication Models

Due to the incorporation of various infrastructural elements in the Internet of Vehicles (IoV), a multitude of communication models is evident. These encompass the exchange of information among onboard units (OBUs), roadside units (RSUs), base stations, or transportation infrastructure. Consequently, three distinct categories can be identified based on the three primary components within vehicular networks, as illustrated in Figure 3—namely, onboard communication, vehicle-to-vehicle (V2V), and vehicle-to-infrastructure (V2I). These categories collectively form what is commonly known as the V2X communication model.

Onboard communication is facilitated by the OBU and, in the context of the IoV, also by the application unit (AU). The OBU establishes a communication link for the AU, thereby ensuring the functionality of various onboard applications.

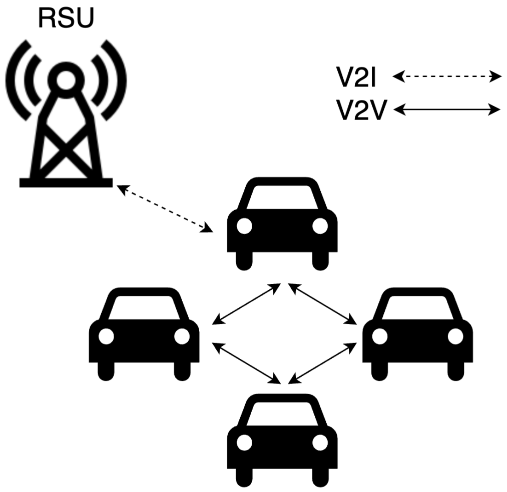

Figure 3. Communication models within IoV network [63].

The significance of intervehicle communication cannot be overstated in the context of IoV applications. V2V communication plays a pivotal role by enabling the broadcast of operational data related to traffic conditions, including the detection of collisions or emergencies [64]. Moreover, it serves as a crucial mechanism for network operations, thus allowing data forwarding to the infrastructure when the vehicle is not directly within the coverage of the IoV infrastructure. This functionality transforms vehicles into relay nodes in V2X communication, thereby effectively expanding the communication range. The ability to share data among vehicles through V2V communication facilitates the creation of ad hoc vehicular clouds, as well as enables the pooling of computational resources for enhanced IoV system efficiency [64]. These vehicular clouds eliminate the need to offload complex computational tasks, such as environment map formation or path planning, to remote clouds, thereby reducing solution delays.

Examining the last discussed communication model, V2I involves communication between vehicles and RSUs, thus establishing a vital channel for information exchange among vehicles and other networks [65]. This connection establishment from a vehicle to an RSU not only extends the communication range but also provides comprehensive information about the transportation environment. It allows for the processing and integration of data from individual components, thereby contributing to a more detailed understanding of the surroundings.

The adoption of these communication models brings significant advantages compared to earlier vehicular networks. These models enable communication for vehicles beyond their immediate range, expand computing and storage capabilities through resource pooling, and support the development of intelligent applications by processing data collected from the transportation system.

5.2. Communication Types

The heterogeneous nature of vehicular networks requires the implementation of various approaches to communication among vehicles and infrastructure. In this section, we present three approaches used in vehicular networks. Each approach is presented with its specifics, advantages, and disadvantages with appropriate use in specific scenarios; hence, vehicular networks frequently need to combine them with the goal of securing the most operational communication. They include the following:

- **Direct communication:** The usage of direct communication is possible in cases when vehicles are intended to communicate with base stations. In this scenario, vehicles are not able to communicate directly with each other due to the centralization of a network [66]. This type uses base stations as central nodes, thereby simplifying network architectures. A significant disadvantage is the possible failure of a central node, which would result in a failure of the whole network. Furthermore, due to limiting the communication only to a central node, the network may be prone to performance issues such as bottlenecks and is not suitable for dynamic environments [67].

- **Satellite and cellular networks:** Communication via satellite and cellular networks plays a vital role in interconnecting multiple vehicles. While satellite networks are suitable for communication in geographically distant nodes and find their use especially in flying vehicle networks, their use is also viable for ground vehicles in areas with sparse infrastructure and outside of cities, where there may not be other means of communication either directly to other vehicles or to an underlying infrastructure in the case that a vehicle is located outside of the coverage of cellular or other wireless networks [68]. On the other hand, cellular network coverage can provide fast and seamless communication in areas with sufficient coverage and is widely used in both ground and aerial vehicles [69]. Compared to satellite networks, cellular networks offer greater data transfer speed, lower latency—which is especially true in new generation networks such as 5G or beyond-5G networks—and a lower cost of operation [70].
- **Ad hoc networks:** In order to mitigate the disadvantages of the previous methods of communication, vehicular networks implement ad hoc networks. This approach was the primordial method of communication in earlier vehicular networks. Building on the MANET, nodes in the network with this type of communication enable nodes to communicate directly with each other without a need for centralization of the network's components [71]. The usage of such a method is convenient, especially with more vehicles, with each viewed as an end system in proximity, thereby allowing them to remain connected even in the case that a vehicle reaches a point without a coverage of centralized components [72]. This method finds applications in both ground and aerial vehicle networks. Even though this approach to communication has several benefits in comparison to the previously discussed methods, its usage may be hindered by the rapidly changing dynamic topology of such a network. To alleviate those drawbacks, some works are focusing on designing routing protocols for those networks with the goal of fast and reliable delivery of data while lowering the cost of operation and energy consumption [51].

5.3. Clustering in Communication

The dynamic character of the nodes in the IoV and IoFV and the resulting incessant changes in the topology of the network cause significant problems that hinder the ability to scale the network or route data effectively [73]. To address those issues, the clustering of nodes is commonly used, which is a strategy of dividing the network into groups of nodes as displayed in Figure 4 and Table 3. This division can be based on a multitude of metrics, such as the geographical distances of nodes.

Table 3. Overview of swarm intelligence-based clustering algorithms.

System	Algorithm	WoS	Scopus	Year	Citations WoS	Citations Scopus	Reference
EC-MOPSO	PSO	Yes	Yes	2022	2	1	[74]
MADCR	MOA	Yes	Yes	2021	7	11	[75]
AFS Clustering	AFS	No	Yes	2020	-	3	[76]
CACOIOV	ACO	Yes	Yes	2019	13	19	[77]
MFCA-IoV	MFO	Yes	Yes	2019	31	38	[78]
CAVDO	DFO	Yes	Yes	2018	52	64	[79]

Typically, there are three types of nodes that can be present in clusters [80], as portrayed in Figure 4. The first type is the cluster head (CH) node, which bears the responsibility of coordination and communication with other clusters, as well as the management of the node communication inside the cluster [81]. Therefore, this node should have added features in terms of power, processing, and storage capabilities [46]. Another type of node present in a cluster is the cluster member (CM) node. This represents an ordinary node that has been included in a cluster based on a similarity metric [82]. This type of node can only communicate directly with the cluster head. The last type of node that can be present in a cluster is the so-called cluster gateway (CG), which bears some similarity to the CH and therefore is frequently merged into one node for communication outside of the cluster. The CG is frequently located on the cluster border compared to the CH [82].

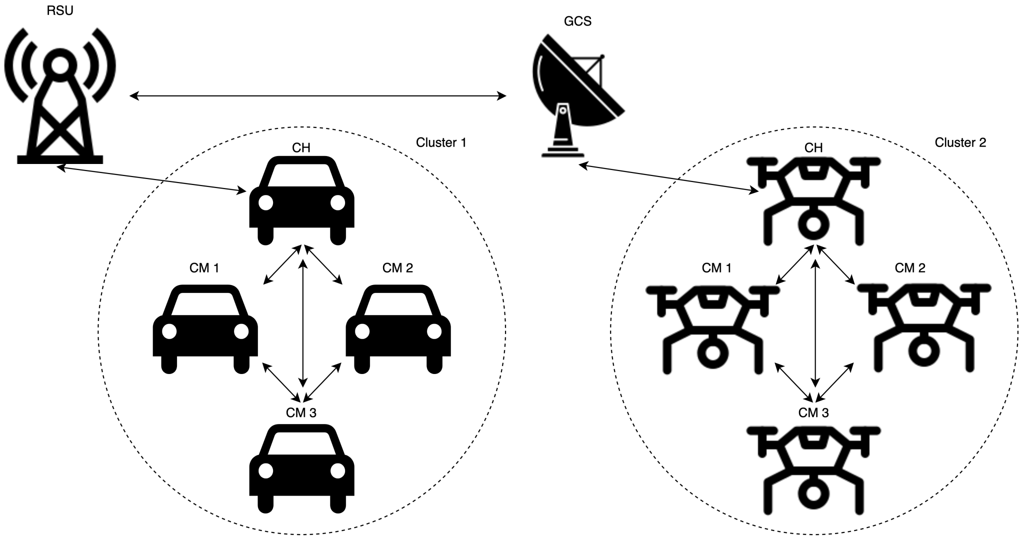

Figure 4. A model clustering in IoV.

The formation of clusters can have one of two forms: the centralized formation—in which a central node, usually an RSU, assigns nodes to appropriate clusters [83]—or the decentralized approach to formation—in which each node seeks its assignment locally [84].

The process of forming clusters in the network has several steps [85]:

- Discovery: In this stage, vehicles joining the network periodically broadcast messages reporting their state as unclustered along with the data required to assign the vehicle to a cluster.
- CH selection: Upon receiving broadcast messages from neighboring nodes, a vehicle will elect an appropriate node based on the gathered data.
- Notification: After a CH is elected, it announces its state to the other vehicles by broadcasting to the unclustered nodes.
- Association: Subsequently, other nodes request to join the cluster and change their state to clustered.
- Maintenance: Both the CH and CM monitor the communication state with each other. If the link is lost, a CM will change its state to unclustered and attempt to join a different cluster.

When this process is utilized in the network, clustering may have a number of advantages. The primary benefits are energy conservation and a reduction in data transfer delay [86]. However, the formation of optimal clusters in vehicular networks is considered to be an NP-hard problem; hence, it is beneficial to focus on near-optimal solutions. As a result, numerous systems have introduced swarm intelligence algorithms to perform clustering [79] such as those summarized in the Table 3. In order to determine their effectiveness, we have evaluated the available data from the experiments described in Table 4. As described earlier, the primary goal of clustering algorithms in the IoV is to generate the smallest possible amount of clusters. Therefore, we have collected the presented data, which are displayed in Figure 5 for systems using the freeway mobility model. The CAVDO system shows the most-generated clusters in each grid size compared to other systems. On the contrary, the CACOIOV system has generated the lowest amount of clusters in a grid of size 4 km × 4 km; however, the data for other sizes are not available. In addition, the MADCR shows the smallest number of generated clusters in each grid size except the 4 km × 4 km, where it is overcome by the MFCA-IoV system.

Regarding systems using the urban mobility model, the EC-MOPSO cannot be evaluated by the number of generated clusters, as this is one of the parameters of the simulation that is set manually. The AFS clustering with a transmission range set to 200 m generated eight clusters with 30 vehicles connected to the network and eleven clusters with 60 vehicles connected to the network.

Table 4. Parameters of clustering experiments.

Parameter	EC-MOPSO	MADCR	AFS Clustering	CACOIOV	MFCA-IoV	CAVDO
Grid size (km × km)	1	1, 2, 3, 4	1	4	1, 2, 3, 4	1, 2, 3, 4
Vehicles (count)	50–100	30–60	30–60	40–200	30–60	30–60
Speed (km/h)	30–100	72–108	30–50	79.2–108	79.2–108	79.2–108
Communication Range (m)	200	Dynamic	100–600	Dynamic	Dynamic	Dynamic
Mobility Model	Urban	Freeway	Urban	Freeway	Freeway	Freeway

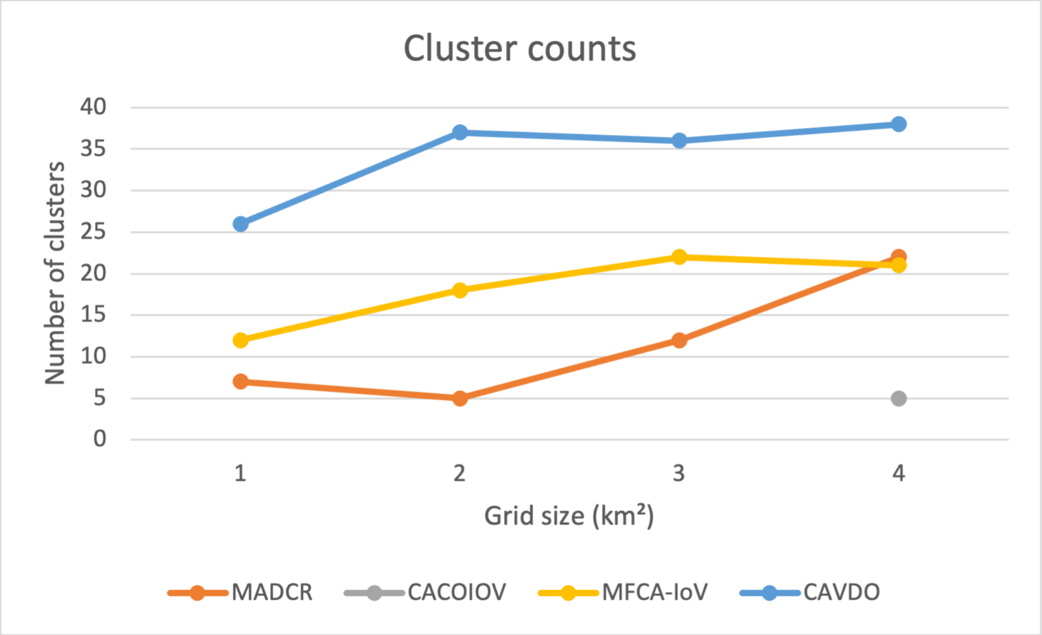

Figure 5. Number of generated clusters by algorithms using freeway mobility model at various grid sizes with 40 vehicles in the network.

5.4. Routing

Vehicular networks allow for the rapid movement of vehicle nodes, which can cause changes in the network's topology [66]. As a result, the malleability of the network topology is seen as an obstacle to the routing process in such networks. In addition, one of the most significant challenges is the size of the network, which can be small or large depending on the current traffic conditions [87]. For instance, the scale of the network might be much smaller in rural areas as opposed to urban regions, highways, or metropolitan cities. This is because large urban areas have a greater population density [88]. If the network has been severely disrupted in any circumstance, it has the potential to become fragmented, which makes the role of routing particularly important. Because the IoV and IoFV are dependent on VANETs and FANETs, respectively, many researchers have implemented numerous traditional VANET/FANET protocols to solve the problem of routing in vehicular networks [42]. As a result of the fact that VANETs and FANETs are a subset of MANETs, a significant number of studies on the implementation of MANET routing protocols have been carried out. In addition to conventional routing algorithms, the usage of swarm intelligence-based approaches is frequent, as is the case with clustering. Table 5 summarizes such algorithms.

There are numerous types of routing protocols that differ according to their application [89]. It is possible to categorize them according to several criteria [90], as indicated in the Figure 6.

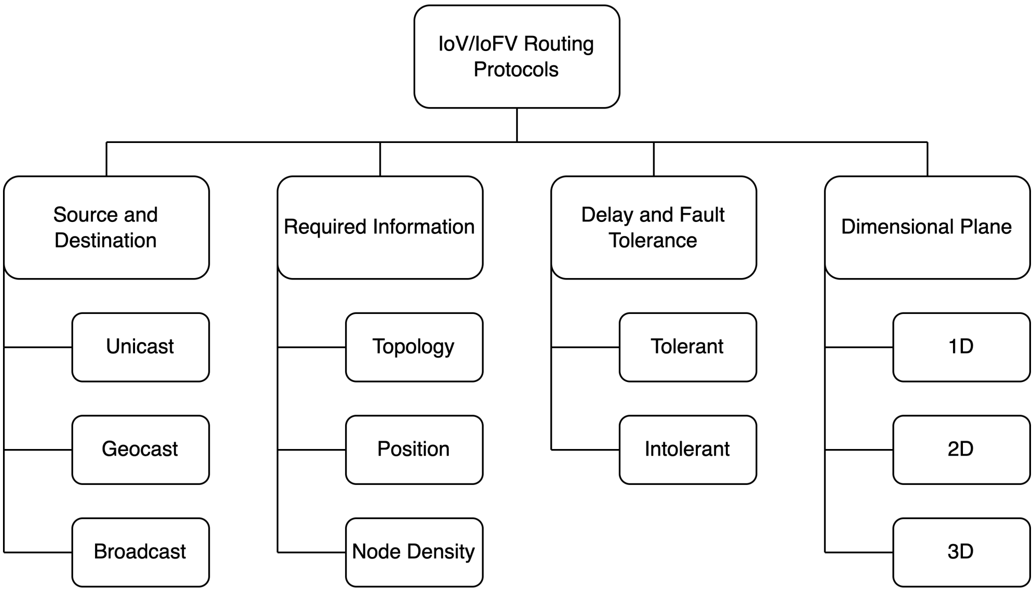

Figure 6. Taxonomy of routing protocols used in vehicular networks.

Table 5. Overview of swarm intelligence-based routing algorithms.

Algorithm	WoS	Scopus	Year	Citations WoS	Citations Scopus	Reference
PSO	Yes	Yes	2019	1	1	[91]
PSO	Yes	Yes	2021	1	1	[92]
PSO	Yes	Yes	2021	2	3	[93]
PSO	Yes	Yes	2020	2	3	[94]
PSO	Yes	Yes	2021	6	8	[95]
PSO	Yes	Yes	2020	6	8	[96]
F-Ant	Yes	Yes	2018	29	39	[97]
Glow-Worm Swarm	Yes	Yes	2022	1	0	[98]
Glow-Worm Swarm	Yes	Yes	2018	5	4	[99]
ACO	Yes	Yes	2022	18	27	[100]
Firefly	Yes	Yes	2019	6	5	[101]

Unicast routing means the data are transmitted from one source node to another destination node [102]. Therefore, it can be marked as point-to-point communication [103]. An example of such a protocol is the F-Ant protocol [97] leveraging the hybrid system of fuzzy logic, as well as the principles of ant colony optimization to route data between two nodes. This system considers data packets as ants laying pheromones on routes. Coupling the evaporation of the pheromone and indicators such as the received signal strength metric, congestion metric, and bandwidth of the node helps the system determine the best path to a destination. F-Ant routing ensures the fulfillment of quality of service and low delay. On the contrary, this protocol may be vulnerable to security threats.

Geocast routing refers to the delivery of messages to a subset of nodes outlined by a geographical region [104]. The implementation of these protocols in vehicular networks is deemed to be problematic due to the high mobility of nodes [105]. However, the employment of the particle swarm optimization algorithm may alleviate some hindrances, as demonstrated in [96]. The discussed protocol employs the particle swarm optimization in the selection of a next-hop vehicle, which is a crucial task in geocast routing because of frequent changes in topology, interference, and the high speed of nodes. The protocol disposes of a fitness function maximizing delivery ratio and throughput, as well as diminishes the delay in delivery, dropped packets, or communication overhead.

In the case of broadcast routing [106], the data packets must be delivered from one node to all other nodes present in the network [107]. Such a protocol includes, for example, the optimized link state routing protocol [92], which utilizes the particle swarm optimization algorithm to select multipoint relay nodes responsible for broadcasting messages, thereby consequently reducing the communication overhead in the network.

6. Computing in Vehicular Networks

The computation in vehicular networks plays an important role in the functioning of such systems. Nowadays, applications running in vehicular networks are characterized by the need for instant access to information and the decisions made upon them. As a result of such demands, means for powerful computation had to be deployed in those networks. Multiple paradigms have already been utilized, each of which is well suited for various scenarios.

6.1. Onboard

The primordial model for computing in earlier networks was the employment of onboard computing units. Those units, however, were limited in resources; they could not swiftly process large quantities of data collected from the sensors and make appropriate decisions such as those required for autonomous driving [108]. However, the improvement of V2V communication has enabled the sharing of resources among vehicles. This denotes the usage of the available resources of another vehicle by a different vehicle, thus forming a variation of an ad hoc cloud [13]. Even though this model is flexible and potentially allows for performance improvement by offering a larger set of resources for applications in vehicles, the high mobility of nodes and the resulting high variability of the topology of vehicular networks make it arduous to fully utilize shared resources [108]. Communication among vehicles can be disrupted at any time, thus resulting in a loss of access to shared resources. In addition, vehicles offering shared resources are often unknown, thus requiring authentication and security measures to ensure the safety of data.

To alleviate these drawbacks, methods aimed at providing reliable resource sharing are being designed. There are approaches using the digital twin in the cloud for modeling the physical states of vehicles in the network with the real-time synchronization of data such as location, velocity, or available fuel [109]. The location of a digital twin in a remote cloud facilitates the usage of artificial intelligence and allows for the digital twin to act as a broker for intravehicular communication to secure resource sharing among vehicles. In this system, a vehicle communicates with its digital twin, which then can retrieve data from the digital twin of a different vehicle. Even though this approach is not limited by the proximity of vehicles, as the communication takes place via digital twins, vehicles have to transmit data to a cloud, which can introduce an unwanted latency.

The other approaches introduce vehicular edge computing to share resources. In this case, the edge computing integration into vehicular networks is conducted via resources that are already available in the network. This means that rather than deploying dedicated edge computing servers, it involves utilizing the resources in vehicles to act as an edge node. Such an approach benefits from the geographical proximity of nodes, which may reduce latency but also may cause a disruption of service due to the limited timeframe in which they are able to interact via direct communication [110].

6.2. Edge and Fog

Edge computing and fog computing are critical concepts in vehicular networks and have been the subject of extensive research in recent years. These concepts improve the performance, security, and scalability of connected vehicles by processing data closer to the source, thereby reducing latency, and improving decision-making capabilities.

Edge computing is a distributed computing paradigm that brings computation and data storage closer to the network's edge, where devices such as vehicles are located. The objective of edge computing is to diminish the latency of processing and decision making, which is crucial for real-time applications such as traffic management, accident detection, and road safety [111]. Processing data at the edge reduces the need to transmit large amounts of data to a central location, thereby reducing network congestion and improving overall network performance [112]. This concept has been widely studied in the literature, with various edge-based solutions having been proposed for vehicular networks, such as edge-assisted vehicular ad hoc networks for VANETs and edge-assisted ITSs [113].

Fog computing extends edge computing by bringing computation and data storage even closer to the edge to the "fog" of devices that are located between the edge and the cloud [114]. This allows for even lower latency processing of data and can also improve security and privacy by keeping sensitive data closer to the source [115]. In vehicular networks, fog computing can be used to support advanced applications such as cooperative intelligent transportation systems (C-ITSs), and V2X communications. C-ITSs enable vehicles to communicate with each other, as well as with the infrastructure, to improve safety and traffic flow, while V2X communications allow vehicles to communicate with other devices such as smartphones and traffic lights [116].

Fog computing additionally facilitates the integration of machine learning and artificial intelligence algorithms, which can consequently improve the decision-making capabilities of connected vehicles [117]. For example, trajectory prediction, traffic prediction, and accident prevention are some of the applications that can be improved with the integration of machine learning algorithms. Additionally, fog computing can also help to improve the scalability of vehicular networks by processing and making decisions locally, thereby reducing the need for central processing [117].

Recently, fog-based solutions have gained traction as a promising approach for optimizing communication and data processing in vehicular networks. Fog-assisted V2X communication and fog-assisted C-ITSs are examples of such solutions [118]. The literature presents various architectures and protocols for fog-based vehicular networks, including fog-assisted VANETs [119] and fog-assisted ITSs [120]. These fog-based solutions offer a promising path toward improving communication and data processing in vehicular networks.

In addition, edge and fog computing can also help to improve the security and privacy of vehicular networks by processing data locally and encrypting data in transit. This can prevent malicious attacks on the network and protect sensitive information such as vehicle location and speed [121].

Furthermore, edge and fog computing can also help to improve the energy efficiency of vehicular networks by reducing the amount of data transmitted over the network, thereby reducing the need for large and power-hungry central servers and enabling the use of low-power devices [122].

In conclusion, the concepts of edge computing and fog computing have garnered significant attention in the realm of vehicular networks and have been extensively researched in recent years. These concepts offer the potential to enhance the performance, security, privacy, energy efficiency, and scalability of connected vehicles by processing data near their source, thereby reducing latency, improving decision making, enabling advanced applications such as C-ITS and V2X communications, and facilitating the integration of machine learning and artificial intelligence algorithms. The significance of edge computing and fog computing in shaping the future of vehicular networks and the IoV cannot be overstated.

6.3. Cloud

Due to the limitation of resources for computing and energy, it is common to employ cloud computing to allow vehicles to offload computation tasks consuming a lot of available resources to other nodes for processing [123]. As a consequence, cloud servers are generally located considerably far from vehicles, thereby resulting in significant latency induced by data transfer via core and backbone networks. For this reason, applications that are highly sensitive to latency, as well as reliability, are not appropriate to be offloaded to a cloud [124]. This category of applications includes emergency braking and collision avoidance or obstacle recognition. On the other hand, applications that are not latency-sensitive may be efficiently offloaded, which will result in conserving resources and a reduced computation time for the offloaded task. Preserved resources can then be used to promptly solve tasks that cannot be offloaded [125]. An illustration of a system utilizing cloud computing alongside onboard computing is provided in Figure 7.

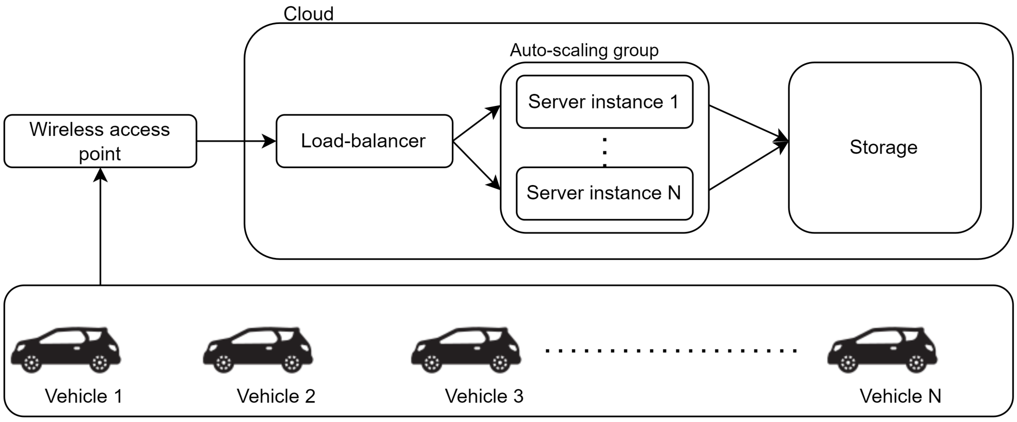

Figure 7. An example of computation in vehicular networks [126].

7. Security

Given the increasing prevalence of vehicles, it is crucial to understand the risks involved. Connected vehicles are vulnerable to attacks, which can be exploited by individuals to gain control. Unmanned aerial vehicles (UAVs) and unmanned ground vehicles pose a concern, as they have the potential to transport cargo and put human lives and property at risk [127]. In order for someone to use a UAV or unmanned ground vehicle for their purposes, they would first need to gain control over it.

To prevent attacks, it is important to ensure that both UAVs and unmanned ground vehicles are properly secured. This involves implementing security measures such as encryption, regular password updates, installing software updates, and securing the network [128]. Apart from the risk of misuse, operating both UAVs and unmanned ground vehicles raises safety concerns for people and property as considerations of privacy.

To tackle these concerns, regulatory authorities worldwide are establishing standards and regulations governing the operation of UAVs and unmanned ground vehicles. These guidelines differ from country to country [129]. They aim to define uses while minimizing the risks of injury or property damage associated with these vehicles. Complying with these regulations is essential.

Securing communication channels for both UAVs and unmanned ground vehicles requires implementing an AAA process. This approach guarantees the security, authentication, and privacy of communication channels, thereby promoting a more accountable utilization of these vehicles [130]. Security involves the following protocols:

- Authentication is the verification of a user’s identity so that the person or system trying to access resources is actually who they say they are.
- Authorization is the granting of permission to access resources. If a person is authenticated, the authorization process determines which parts of the system and resources are accessible to that person and what actions he or she can perform.
- Auditing is the process of recording information about who logged into the system and when, which resources were used, and what actions were performed. It is therefore about monitoring user activity and preventing illegal activities.

7.1. Countermeasures

Intrusion detection systems (IDSs) are developed and used to detect activities and potential cyberattacks. Their main goal is to identify and explore connections associated with types of cyber threats [131]. To achieve this, various approaches are used.

One approach is the rule-based IDS, which enables communication, between vehicles (UAVs) and unmanned ground vehicles. It focuses on detecting the insertion of data related to signal strength [132]. For example, the BRUIDS [133] system evaluates how well a UAV can survive an attack. However, this rule-based system has limitations in detecting attacks. It requires human intervention for configuring rules.

Another approach is the signature-based IDS, which relies on matching signatures or patterns of known attacks against the content of network messages [134]. If a match is found, it alerts the network administrator. Like the rule-based IDS, it may be less effective against types of attacks that do not resemble existing patterns. For instance, in the Air Force, ADS B technology has been used to detect the transmissions of messages.

The third approach is the anomaly-based IDS, which aims to identify behaviors in networks or systems as signs of an attack. This method involves training a model to understand behavior so that it can recognize anomalies when they occur [134]. As a measure against denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks and jamming, this approach is implemented.

To ensure the functioning of both unmanned aerial vehicles (UAVs) and unmanned ground vehicles, it is crucial to utilize algorithms that can detect anomalies. These anomalies include several measurements, such as changes in engine temperature. Additionally, these vehicles can benefit from identification systems for traffic analysis [135]. They can also make use of specifications-based systems equipped with embedded sensors and actuators.

When it comes to securing data and communication for UAVs and unmanned ground vehicles, the process goes beyond protecting the network. Measures need to be taken to prevent interception and to safeguard sensitive information. An algorithm that addresses transmission challenges over channels like 5G between the vehicle and the ground station based on the block coordinate descent method and sequential convex optimization may be used [136]. This algorithm minimizes functions that are dependent on variables by solving problems in blocks while optimizing a group of variables at each step [137].

Another approach used to maintain data confidentiality during communication is functional encryption [138]. This algorithm optimizes variables such as transmitting power or vehicle trajectory. In areas where UAV-assisted heterogeneous networks (HetNets) require security, this can be enhanced through secured functional encryption techniques that incorporate ECC, digital signatures, hashing, and other encryption mechanisms. These measures enhance security. Also, they protect against malicious activities while encrypting data [139].

When it comes to dealing with both UAVs and unmanned ground vehicles, there are several ways to take countermeasures [140]. One option is using drone catchers or vehicles equipped with nets to capture the vehicles if necessary. Another approach is using drone defenders that emit radio waves disrupting the remote control signals and rendering the vehicle inoperable. Additionally, a fence connected to a cloud-based unmanned aerial system (UAS) can detect any attempts by the vehicle to cross boundaries and disable it [141]. Among the most prominent attempts, there are the following:

- Wi-Fi jamming: This is the most common method used, and it operates at a frequency of 2.4 GHz. It is the jamming of wireless transmission signals sent between devices connected to a given Wi-Fi network [142]. It is also used, for example, to protect the network from unauthorized access. The disadvantage is that such interference is visible and can be easily detected. Also, the interference is quite limited, and nearby frequencies are interfered with in addition to the target frequency [143].
- Replay: This attack consists of repeated data transmission between two devices without the data being modified in any way. The attacker intercepts the original communication and later retransmits it to gain unauthorized access [144]. For connected vehicles, it can also be used to break the encryption key while replaying the ARP protocol. It is mainly used when the connection between the vehicle and other devices is secure [145].
- Buffer overflow: This is an attack intended to fill the vehicle's memory buffer with more data than it can process. Such data overflow can cause the vehicle to malfunction and execute arbitrary code, which is exploited to gain control of the device [146].
- DoS: This is performed either by deauthentication or Wi-Fi jamming, which causes devices in the vehicular networks to crash [147].
- ARP cache poisoning (ARP spoofing): An attacker sends spoofed ARP messages into the network in order to deceive other devices trying to communicate with the device. These spoofed ARP messages contain a physical MAC address to which other devices will send their messages. However, this MAC address is spoofed and it is the attacker's device, which gives him access to the data being sent and allows him to modify it and send it on. In vehicular networks, it is used to send malicious scripts repeatedly [148].

7.2. Threats

It is important to be aware not only of the potential but also of the potential threats that drones may encounter. Threats can be diverse and can affect their safety, functionality, and ability to successfully perform their operations and tasks. There are many threats, but the most common include the following:

- GPS signal manipulation: The GPS signal is crucial for navigation applications. It is transmitted by satellites orbiting the Earth. However, there is a vulnerability on Earth known as"GPS spoofing." This refers to the act of generating a GPS signal to manipulate the GPS receiver in a target device. The person behind the spoofing has access to information about the GPS signal from satellites. The person uses it to create a manipulated version, thus giving them control over the target device [149]. This poses a risk for vehicles (UAVs) and unmanned ground vehicles that follow predetermined routes [150]. GPS spoofing could potentially lead to the theft of assets or result in unsafe cargo delivery, such as biological weapons or explosives.
- Malware and data interception: The wireless and remote control methods used for piloting UAVs and unmanned ground vehicles are not completely secure. Hackers can secretly implant a message into the vehicle's memory by installing malware without detection in the system that controls the ground station [151]. Additionally, since these vehicles often monitor objects, their unsecured wireless transmission of sensor data makes them susceptible to hackers inserting malware.
- Wi-Fi interference: When deauthentication processes occur between an access point and a vehicle controller, it opens up opportunities for hijacking UAVs and unmanned ground vehicles. When hackers disrupt the Wi-Fi frequency of a drone, they manipulate it to connect to a network without authorization [152].
- Technical issues and nature: There are factors that can lead to crashes of UAVs and unmanned ground vehicles, such as the loss of connectivity, inexperienced piloting, or unfavorable weather conditions. These incidents can cause damage to property. Ref. [153] studied how these risks can even result in injuries. Additionally, technical problems like motors overheating or batteries exploding in temperatures can pose

risks. Inadequate security measures in the design of these vehicles may also contribute to the loss of control, thus further escalating harm [154].

- Privacy concerns: As the popularity of UAVs and unmanned ground vehicles increases, so does the concern surrounding privacy [155]. Equipped with cameras and sensors, these vehicles have the capability to capture high-quality images and collect data that may intrude upon an individual's privacy without their consent. Privacy concerns extend further when considering the risk of hackers gaining control over a vehicle's cameras and gaining access to data from military zones or private residences for purposes such as identity theft, blackmailing, or illegal activities [156].

Regulatory bodies worldwide are actively working on establishing rules and regulations concerning the use of UAVs and unmanned ground vehicles. However, these regulations vary across countries, with some regions still lacking guidelines. The measures being implemented include obtaining permits for operation that adhere to procedures during usage, as well as imposing limitations on vehicle use within certain areas or under specific circumstances [157]. To tackle privacy concerns, it is important to establish guidelines that mandate operators to seek consent from individuals before capturing images or collecting data. Furthermore, it is crucial to take measures to guarantee the usage of applications, especially considering that many vehicles have apps, which could potentially pose security risks [158].

8. Use Cases and Applications

Drones and autonomous ground vehicles have proven to be excellent tools with a wide range of applications that impact a variety of industries. Their flexibility, precision, and availability are some of the most important factors in their procurement. This chapter describes the various uses of drones and autonomous vehicles, thereby ranging from agriculture to surveys, monitoring, and beyond.

8.1. Agriculture

The use of drones in agriculture has gained a lot of popularity in recent years. Farmers are seeking efficient ways to monitor their crops, and specially designed drones offer a wide range of applications that are guaranteed to help them do just that [159]. One of the key advantages of such drones is the creation of high-quality images using NDVI (normalized difference vegetation index) technology. By combining these images with machine learning and computer vision, farmers are able to monitor plant health and even predict crop yields. Drones proved to be an attractive solution during the COVID-19 pandemic, particularly when physical contact was limited.

Drones used in the field include various models tailored to specific agricultural tasks. Bayer drones [160], for instance, are multipropeller drones powered by rechargeable batteries. Equipped with up to a 10-liter tank, these drones can cover a hectare of land in 10–15 min. Their autonomy allows them to detect and avoid obstacles or automatically fill the tank. Moreover, they can operate collaboratively in a group of drones, thereby enhancing their efficiency.

Similarly, the DJI Agras MG-1 drone [161] is designed specifically for the application of pesticides and fertilizers on crops. With a payload capacity of 10 kg, it can efficiently cover 1 hectare of area in about 20 min. The drone's efficiency and cost minimization are achieved through automated spray adjustment, which depends on the current speed of the drone, thus ensuring a uniform application of the product.

Expanding beyond aerial solutions, autonomous vehicles on the ground have also found application in modern agriculture. In the realm of autonomous ground vehicles, technology has been leveraged to optimize tasks such as planting, harvesting, and monitoring [162]. These vehicles offer a promising alternative, especially in scenarios where aerial drones may face limitations.

Autonomous ground vehicles, much like their airborne counterparts, leverage advanced technologies such as machine learning and computer vision to navigate through fields, assess crop health, and perform targeted interventions. These vehicles can operate efficiently in a variety of terrains, thus offering farmers a versatile tool for precision agriculture [163].

In the context of autonomous vehicles on the ground, one notable example is their application in autonomous farming vehicles for soil mapping. In regions, drones like those developed by Drones FAO are recommended to farmers when different operations, such as pesticide spraying or fertilizer application, are needed. These ground-based vehicles provide accurate information to help farmers achieve greater efficiency and quality in their crops, thereby showcasing the interdisciplinary nature of autonomous technologies in modern agriculture.

8.2. Warehouses and Logistics

The exponential growth of global e-commerce, represented by the surge in e-shops, has led to a proportional expansion in the size of warehouses. In these large-scale facilities, managing goods and intralogistics presents challenges that have spurred technological advancements in drones tailored for warehouse applications. These drones are currently in use performing automated inventories that streamline managerial tasks, alleviate tedious and hazardous work, and enhance overall efficiency beyond the capabilities of manual labor [164]. The Fourth Industrial Revolution, also known as Industry 4.0, has introduced various technologies that are applicable to and transformative for warehouses. These technologies include scanning, QR codes, RFID, and artificial intelligence, thereby enabling the automation of warehouses through drone control [165].

Drones deployed within warehouses are versatile and can contribute to various activities:

Inventory: Owing to their exceptional maneuverability and compact size, drones can undertake tasks such as audits, retrieving items, and conducting inventory assessments [166]. This capability enables warehouses to reduce labor costs or enhance the accuracy of inventory quantity assessments.

Intralogistics: Drones are also viable for intracompany logistics [167], thus transporting goods along predefined flight paths. Challenges such as weight capacity, gripping mechanisms, and precise location awareness need resolution to fully leverage the potential of drones in this activity.

Inspection and surveillance: Drones can play a crucial role in inspecting the condition of roofs, racks, walls, and ceilings, thereby contributing to enhanced workplace safety. By minimizing dangerous tasks performed by workers, drones offer a cost-effective alternative, particularly in interior inspections. Predefined routes equipped with cameras can be utilized to prevent theft and monitor against other unwanted activities [168].

However, the implementation of drones in warehouses is not without its challenges. Safety concerns for employees in the event of drone malfunctions, questions of liability in the case of failures, and the potential invasion of privacy due to camera-equipped drones are important considerations. Navigation can be problematic indoors due to the limitations of using GPS, and obstacle avoidance becomes challenging in warehouses with numerous obstacles.

While drones have proven effective for tasks within the warehouse, last-mile delivery, often carried out by courier services, poses its own set of challenges. Traditional parcel delivery using internal combustion engine vehicles is not environmentally friendly, and issues such as traffic congestion can disrupt delivery schedules. As online shopping continues to surge in popularity, there is a growing demand for efficient transport logistics solutions [169].

Single drone delivery: In certain situations, a single drone delivery proves sufficient. These drones can carry parcels weighing up to 2.5 kg, thus covering over 80% of online retailers' products. The drone's range is between 3 and 33 km, thus necessitating multiple recharges for longer-distance deliveries [164].

Drone swarm delivery: The concept of a drone swarm involves a group of drones working collaboratively to achieve a task. Synchronized and capable of communication, drone swarms can function as a unit. This approach becomes advantageous when multiple packages need delivery to the same location or for heavy packages beyond the capacity of an individual drone [170]. Drone swarms can be categorized as static or dynamic, with the latter offering parallel task execution. Drones forming a formation in flight can save energy by reducing drag forces and lift forces, thereby increasing the overall flight range.

A combination of trucks and drones emerges as an effective solution for parcel delivery. In this model, the truck serves as a launching and charging station for the drones while transporting the goods. This coordinated approach involves multiple vehicles interacting and acting as mobile stations for the drones [171]. The synchronized routing of trucks and drones optimizes the delivery route, thereby aiming to visit each customer only once—either by drone or vehicle—minimizing delivery time, and reducing costs.

8.3. Healthcare

The use of drones in public spaces faces global restrictions due to airspace and privacy regulations. While these constraints partially impact the development of healthcare-related drones, certain organizations, such as WeRobotics, persist in implementing solutions in this field worldwide. Notably, researchers at the Johns Hopkins University School of Medicine have discovered that transporting lab tests using drones did not compromise the accuracy of their results.

Drones exhibit the capability to transport biological samples, thus proving particularly valuable in scenarios where road transport is inefficient. This capability becomes especially indispensable during natural disasters. Drones excel in delivering medical supplies to communities where infrastructure and transportation are often limited, thereby significantly reducing the time required for supply delivery [172]. Addressing this challenge, Aidronix aims to create an unmanned system dedicated to providing medical assistance in rural communities. Their plan involves establishing distribution centers from which drones will transport medical supplies. An emerging concept known as "lab-on-a-drone" envisions drones as mobile laboratories providing diagnostic tools for disease diagnosis and treatment.

Unmanned aerial vehicles (UAVs) can also play a crucial role in controlling infectious diseases, particularly those caused by pathogens such as viruses or bacteria. Drones equipped with sensors and artificial intelligence can gather data on environmental factors like water or vegetation. The use of intelligent drones may gradually replace satellites employed for monitoring and ecological research [173].

Expanding beyond aerial solutions, autonomous ground vehicles add another dimension to healthcare logistics. These vehicles, leveraging technologies like machine learning and computer vision, offer efficient transport solutions [174]. Autonomous ground vehicles are well suited for scenarios where drones may face limitations, thereby providing a versatile tool for precision healthcare logistics.

Ensuring the safety of both medical drones and ground vehicles is paramount. Measures include preventing collisions with other objects to avoid property damage, personal injury, or harm to transmitted samples or instruments. Designated safe areas for takeoff and landing, along with weatherproof and rainproof features, are essential considerations. However, achieving these safety features may involve tradeoffs between payload capacity, performance, speed, and maximum the range of the drones and ground vehicles [175].

8.4. Space Exploration

There are various methods to observe space objects such as telescopes, spacecraft, landers, or rovers. However, these methods have their own drawbacks that hinder the effective search of space. The use of drones and autonomous ground vehicles for such exploration brings several advantages, such as the ability to map a larger area in less time compared to a rover and at the same time with a much higher resolution than current satellites provide. UAVs and ground vehicles can be used to correct engineering errors or to gain a comprehensive understanding of the atmosphere and surface/interior of the planet [176].

As is usual with any technology, it has its flaws and shortcomings. The very implementation of drones and ground vehicles for this purpose poses safety concerns, flight requirements, or data gain. Due to the vast distance between Earth and space, it is not possible to control drones and ground vehicles remotely from a ground station. The aim is to create a communication system that allows such communication. Data transmission would be handled through an intermediary in space, which would receive data from the drone or ground vehicle and send it to Earth. The intermediary is necessary because of the increased weight of the drone or ground vehicle due to the necessary antenna when sending directly to Earth [177]. Overall, the UAV and ground vehicle used must be very light and should consist of only the necessary components. Such a drone or ground vehicle should be powered using LiPo (lithium polymer) batteries combined with solar energy to increase flight time. The navigation and control subsystem also faces challenges, as there is no physical structure to rely on for computation. In other words, there are no clues on alien planets, such as buildings or markers on Earth, by which the drone or ground vehicle can navigate in space [178].

8.5. Search and Rescue

Drones and autonomous ground vehicles represent significant potential in rescue operations, particularly in rural and remote areas where the location of the person in need of help is unknown. Time is a critical factor in such situations, and the deployment of drones and ground vehicles can significantly reduce rescue time [179]. In the case of natural disasters such as avalanches, floods, fires, or contamination, these autonomous systems can move more efficiently than search teams. Equipped with various sensors, including those for radioactivity, they play a vital role in the search and scanning of an area.

For instance, a sensor for radioactivity on these autonomous systems can prevent further complications that may arise without their intervention. However, challenges can arise in navigation, as the position of the drone or ground vehicle may not always be accurate, thereby complicating the search action significantly [180]. In another scenario, such as the loss of a child in an amusement park, drones and ground vehicles using cameras to identify people may raise privacy concerns. By addressing these challenges, it becomes possible to utilize drones and ground vehicles efficiently in the search for individuals in need of assistance.

8.6. Other Applications of Drones and Autonomous Ground Vehicles

In addition to the aforementioned applications, both drones and autonomous ground vehicles showcase their versatility and impact on various industries. Some noteworthy applications include the following:

- Tourism, commerce, and cinematography: Drones play a pivotal role in the realms of tourism [181], commerce, and cinematography [182]. They provide high-quality images, thereby offering new perspectives to attract tourists and promote destinations at a whole new level. In cinematography, drones offer a cost-effective means to capture special shots that might be physically and financially challenging with alternative equipment.
- Underwater operations: Both aerial drones and unmanned underwater vehicles (UOVs) contribute significantly to monitoring marine life. Aerial drones can be used to survey coastlines and assess environmental conditions, while underwater drones are employed in surveys, checking underwater infrastructure, and searching for oil and gas. The advantage of underwater drones lies in their ability to withstand the dangerous and harsh conditions beneath the water's surface. Advancements in this technology are anticipated, thereby enabling more sophisticated research and exploration of deep sea locations [183].

- Traffic monitoring: Drones and autonomous ground vehicles have proven effective in traffic and accident monitoring, thus quickly providing necessary footage through high-quality cameras [184]. They find applications in areas with a high frequency of accidents, thereby assisting in assigning blame or facilitating decision making. Beyond traffic, these autonomous systems are utilized to monitor crowds at protests or refugee movements, therbey contributing to public safety [185].
- Military applications: In military contexts, both drones and autonomous ground vehicles serve various purposes, from simple surveillance and reconnaissance to more complex tasks. They play a role in targeted killing through artificial intelligence, thereby reducing the risk to personnel. However, concerns about the misuse of such technologies for personal gain, potentially leading to property damage or harm to innocent lives, have been raised.

9. Challenges

In this chapter, we will be exploring the challenges that come with combining the Internet of Vehicles (IoV) and the Internet of Flying Vehicles (IoFV) into one big network. This merging of connected cars and flying vehicles offers a lot of exciting possibilities, but it also comes with some tricky problems. We will look into issues like keeping everything secure, making sure different systems can communicate with each other, dealing with rules and regulations, and setting up the right infrastructure. This journey aims to uncover the obstacles and find ways to make a smoothly connected and airborne transportation future possible.

9.1. Regulations

The topic of regulations surrounding the IoV and the Internet of Flying Vehicles (IoFV) has several aspects that need to be taken into consideration. This primarily includes existing road traffic regulations, aviation frameworks, and broader legal considerations. Currently, traditional road traffic regulations form the foundation, especially when it comes to autonomous vehicles, for the IoV governing how vehicles move, traffic flows, and vehicle behavior [186]. However, with the integration of the IoV and IoFV, traditional regulations face challenges. Additionally, existing aviation regulations designed for aircraft need to be adapted to accommodate aerial vehicles (UAVs) and urban air mobility (UAM) systems in the IoFV [187].

One important aspect is how road and air traffic regulations converge due to the mobility paradigm introduced by the IoFV. Navigating through airspace effectively requires an approach that combines ground and aerial regulations [188]. This ensures that flying vehicles can seamlessly integrate into existing traffic frameworks. At the same time, clear guidelines must be established within environments to address airspace management issues, flight corridors, and integrating takeoff and landing zones [189].

Current aviation regulations primarily cater to manned aircraft and struggle with adapting to the increasing number of autonomous flying vehicles. The regulatory discussion focuses on matters such as air traffic control, collision avoidance, the certification of systems, and vehicle registration [190]. The evolving landscape of the Internet of Flying Vehicles (IoFV) requires an evaluation of the existing regulations to determine their adequacy and relevance.

When it comes to cybersecurity, it becomes more critical in the IoFV compared to the Internet of Vehicles (IoV). Aerial vehicles face cyber threats, so regulatory frameworks must address not only data protection and encryption but also the vulnerability of flying systems to hacking and unauthorized access. This involves creating rigorous cybersecurity protocols for flying vehicles to ensure operations within the IoFV [191].

In some jurisdictions, regulatory bodies are taking steps by exploring ways to integrate flying vehicles into urban areas through pilot projects and regulatory sandboxes. These initiatives provide controlled environments for regulators to test and refine their approaches, thereby fostering an atmosphere that promotes experimentation learning and the iterative development of regulations that can effectively accommodate the IoFV [192].

International collaboration plays as much of a role in regulating the IoFV as it does in regulating the IoV. Since flying vehicles operate beyond national boundaries, collaborative efforts between regulatory bodies, aviation authorities, and international organizations are essential in establishing unified frameworks for governing the IoFV [127]. This collaboration goes beyond managing airspace. It also includes aspects such as interoperability between countries having standardized certification processes and dealing with legal and liability issues in the case of incidents involving aerial vehicles [193].

To conclude, the regulations for the Internet of Vehicles (IoV) and the Internet of Flying Vehicles (IoFV) require an approach that takes into account existing road traffic rules, adjusts aviation frameworks, and addresses the challenges presented by flying vehicles. As technology progresses and changes how we travel on both land and in the air, regulatory frameworks must adapt dynamically to find a balance between innovation, safety, and societal impact. The coexistence of vehicles and flying vehicles creates a regulatory environment that requires ongoing dialogue, adaptation, and international collaboration.

9.2. Integration

The integration of the Internet of Vehicles (IoV) and the Internet of Flying Vehicles (IoFV) into a network is an undertaking that involves various considerations such as security, infrastructure, existing technologies, and frameworks. Ensuring security measures is crucial. Achieving successful integration also requires leveraging current infrastructure and technologies while accommodating the unique characteristics of both ground and aerial transportation systems.

When it comes to security, a comprehensive approach is needed. This includes implementing encryption techniques, secure communication protocols, robust authentication mechanisms, and measures to protect the infrastructure. These security measures should align with existing frameworks while addressing the challenges posed by merging the IoV and IoFV.

Infrastructure readiness plays a role in this integration [194]. The physical and communication infrastructure must be designed to cater to the needs of ground and flying vehicles. This involves deploying traffic management systems for ground vehicles, as well as establishing air traffic control mechanisms for flying vehicles [195].

Existing technologies and frameworks significantly influence how this integration takes shape. Utilizing communication protocols, such as V2X communication for ground vehicles and UTM for flying vehicles improves the efficiency and compatibility of communication [196]. By integrating with established intelligent transportation systems (ITS) frameworks, we can facilitate data exchange and contribute to a more cohesive and effective transportation ecosystem [197].

To ensure an integration process, it is important to examine existing models of the IoV (Internet of Vehicles) and IoFV (Internet of Flying Vehicles). Noteworthy examples in the IoV domain include the C-V2X (cellular vehicle to everything) platform, which employs networks for vehicle communication [198], as well as DSRC (dedicated short-range communication), which is a wireless technology designed specifically for vehicular communication [199]. On the IoFV front, UTM (unmanned traffic management) models offer a framework for managing and monitoring low-altitude airspace to enable efficient drone operations [200].

In order to meet the communication needs of ground and flying vehicles, it may be beneficial to consider a communication infrastructure. This approach involves combining DSRC for ground vehicles with satellite-based communication for flying vehicles to optimize coverage and reliability [154]. Additionally incorporating edge computing capabilities allows for critical data to be processed closer to their source, thereby reducing latency and improving real-time decision making in areas like collision avoidance and route optimization [201].

Furthermore, integration extends beyond software systems; retrofitting existing infrastructure with sensors and communication devices can enhance the responsiveness of our transportation network [202].

This involves implementing traffic lights with embedding sensors [203] in roadways and establishing communication infrastructure at landing pads and airports to enable operations within the Internet of Vehicles (IoV) and the Internet of Flying Vehicles (IoFV) [204].

Collaboration is crucial to tackle the challenges associated with integrating infrastructure and technology. Collaborations between government entities, technology providers, vehicle manufacturers, and urban planners through partnerships encourage a cooperative approach toward standardization, policy development, and the creation of interoperable frameworks [205].

To summarize, successfully combining the IoV and IoFV into a network requires the consideration of security measures, existing technologies, infrastructure requirements, and frameworks. By aligning these elements with the needs of ground and flying transportation systems, we can establish an integrated network that operates efficiently. Examining existing IoV and IoFV models offers insights, while collaborative efforts among stakeholders and the strategic implementation of technologies are crucial for navigating the complexities of this transformative convergence.

10. Conclusions and Future Directions

The proposed collaboration in vehicular networks, in particular among those used by ground vehicles—especially cars—and flying vehicles, could broaden the application possibilities of intelligent transport, especially in urban areas where, in accordance with the latest trend, the use of autonomous cars and autonomous quadrocopters is on the rise.

Currently, considering several specifics—mainly varying mobility ranges—those vehicles tend to use separate networks and infrastructure despite bearing significant similarities. Hence, we aim to create an architecture that will allow for the collaboration of ground and flying vehicles. Such an architecture bears the potential to reduce the costs of underlying infrastructure, simplify the deployment of those complex systems, and improve the performance and safety of intelligent transportation. Furthermore, as has been outlined in previous sections, progress in one type of vehicular network is frequently not reflected in other types of networks, despite the potential of use. Hence, an architecture for a unitary collaborative network has the potential to mitigate this negative effect.

In conclusion, the Internet of Vehicles (IoV) and the Internet of Flying Vehicles (IoFV) represent significant areas of investigation and advancement in the realm of vehicular networking. The potential of these networks to transform the transportation industry by enabling vehicles to interact with each other and their surroundings in a secure, efficient, and intelligent manner is substantial. The continued research and development in these areas holds the promise of realizing their full potential and shaping the future of the transportation sector.

The study of vehicular networks encompasses two important domains: the Internet of Vehicles (IoV) and the Internet of Flying Vehicles (IoFV). Both of these networks offer significant potential for the transportation sector and present opportunities for vehicles to interact with each other and their environment in a safe, efficient, and intelligent manner. The architecture, communication, and computing elements of these networks are critical in determining their overall performance and functionality. To achieve advanced capabilities, these networks necessitate the integration of cutting-edge technologies, such as cognitive radio and edge/fog computing. Despite similarities between the IoV and the IoFV, it is important to note that they possess distinct differences, particularly with respect to the challenges and requirements associated with communication and computing in a flying environment. These considerations, such as air-to-air communication and aerial navigation and control, are unique to the IoFV and must be addressed in its design and development.

In the field of vehicular networking, the Internet of Vehicles (IoV) and the Internet of Flying Vehicles (IoFV) are emerging as key areas of research and development. Both networks aim to revolutionize the transportation sector by enabling vehicles to interact with one another and with the environment in a secure, efficient, and intelligent manner. To achieve this goal, there is a need for the ongoing exploration and advancement of technologies such as cognitive radio and edge/fog computing, as well as the development of suitable network architectures that can accommodate the specific demands of the IoV and IoFV. The architecture, communication, and computing elements of these networks play a vital role in determining their overall performance and functionality, and it is important to consider both the similarities and differences between the IoV and IoFV to ensure effective implementation.

The Internet of Vehicles (IoV) and the Internet of Flying Vehicles (IoFV) hold great promise for the transformation of transportation and have wide-ranging implications for society. The realization of their potential necessitates continuous research efforts aimed at developing and improving advanced technologies, such as cognitive radio and edge/fog computing, as well as effective network architectures that can support the dynamic requirements of these networks.

Author Contributions: Conceptualization, D.H. and J.V.; methodology, D.H.; formal analysis, D.H.; investigation, D.H. and J.V.; resources, J.V.; writing—original draft preparation, D.H.; writing—review and editing, D.H. and J.V.; visualization, D.H.; supervision, J.V.; project administration, J.V.; funding acquisition, J.V. All authors have read and agreed to the published version of the manuscript.

Funding: This publication was supported by the VEGA grant EDEN: EDge-Enabled intelligeNt systems (1/0480/22).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AU	Application Unit
UAV	Unmanned Aerial Vehicle
VANET	Vehicular Ad Hoc Network
MANET	Mobile Ad Hoc Network
FANET	Flying Ad Hoc Network
WLAN	Wireless Local Area Network
IoT	Internet of Things
DSRC	Dedicated Short-Range Communication
IoV	Internet of Vehicles
IoFV	Internet of Flying Vehicles
5G	Fifth-Generation Network
V2	Vehicle-to-Vehicle
V2I	Vehicle-to-Infrastructure
V2X	Vehicle-to-Everything
CCAS	Cooperative Collision Avoidance System
CAS	Collision Avoidance System
C-ITS	Cooperative Intelligent Transportation Systems
OBU	Onboard Unit
RSU	Roadside Unit
CH	Cluster Head

CM	Cluster Member
CG	Cluster Gateway
ITS	Intelligent Transportation System
GPS	Global Positioning System
LiDAR	Light Detection and Ranging

References

1. Raghavan, K.; Ooi, K.J.; Tan, Q.Y.; Bhuiyan, M.A.; Kumar, B.V.; Yuen, C.W.; Reaz, M.B. Smart Traffic Systems Guided by Principles of Traffic Circuit Theorems. In Proceedings of the 2020 IEEE 8th R10 Humanitarian Technology Conference (R10-HTC), 1 December 2020; Kuching, Malaysia, pp. 1–5, .
2. Saleem, M.; Abbas, S.; Ghazal, T.M.; Khan, M.m.A.; Sahawneh, N.; Ahmad, M. Smart cities: Fusion-based intelligent traffic congestion control system for vehicular networks using machine learning techniques. *Egypt. Inform. J.* **2022**, *23*, 417–426. [CrossRef]
3. Yasin, J.N.; Mohamed, S.A.; Haghbayan, M.H.; Heikkonen, J.; Tenhunen, H.; Plosila, J. Unmanned aerial vehicles (uavs): Collision avoidance systems and approaches. *IEEE Access* **2020**, *8*, 105139–105155. [CrossRef]
4. Byun, H.S.; Rhim, J.K. A Study on Accident Prevention through Analysis of Industrial Drone Accidents and Their Causes. *J. Korean Soc. Saf.* **2019**, *34*, 88–95.
5. Arafat, M.Y.; Moh, S. Routing protocols for unmanned aerial vehicle networks: A survey. *IEEE Access* **2019**, *7*, 99694–99720. [CrossRef]
6. Ali, E.S.; Hasan, M.K.; Hassan, R.; Saeed, R.A.; Hassan, M.B.; Islam, S.; Nafi, N.S.; Bevinakoppa, S. Machine learning technologies for secure vehicular communication in internet of vehicles: Recent advances and applications. *Secur. Commun. Netw.* **2021**, *2021*, 8868355. [CrossRef]
7. Danba, S.; Bao, J.; Han, G.; Guleng, S.; Wu, C. Toward collaborative intelligence in IoV systems: Recent advances and open issues. *Sensors* **2022**, *22*, 6995. [CrossRef] [PubMed]
8. Alladi, T.; Kohli, V.; Chamola, V.; Yu, F.R.; Guizani, M. Artificial intelligence (AI)-empowered intrusion detection architecture for the internet of vehicles. *IEEE Wirel. Commun.* **2021**, *28*, 144–149. [CrossRef]
9. Al-Heety, O.S.; Zakaria, Z.; Ismail, M.; Shakir, M.M.; Alani, S.; Alsariera, H. A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for sdn-vanet. *IEEE Access* **2020**, *8*, 91028–91047. [CrossRef]
10. Singh, A.; Patil, D.; Omkar, S. Eye in the sky: Real-time drone surveillance system (dss) for violent individuals identification using scatternet hybrid deep learning network. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, Salt Lake City, UT, USA, 18–23 June 2018; pp. 1629–1637.
11. Hafeez, A.; Husain, M.A.; Singh, S.; Chauhan, A.; Khan, M.T.; Kumar, N.; Chauhan, A.; Soni, S. Implementation of drone technology for farm monitoring & pesticide spraying: A review. *Inf. Process. Agric.* **2022**, *10*, 192–203.
12. Alsamhi, S.H.; Afghah, F.; Sahal, R.; Hawbani, A.; Al-qaness, M.A.; Lee, B.; Guizani, M. Green internet of things using UAVs in B5G networks: A review of applications and strategies. *Ad Hoc Netw.* **2021**, *117*, 102505. [CrossRef]
13. Jamil, S.; Rahman, M. A Comprehensive Survey of Digital Twins and Federated Learning for Industrial Internet of Things (IIoT), Internet of Vehicles (IoV) and Internet of Drones (IoD). *Appl. Syst. Innov.* **2022**, *5*, 56. [CrossRef]
14. Cheng, J.; Cao, C.; Zhou, M.; Liu, C.; Gao, S.; Jiang, C. A dynamic evolution mechanism for IoV community in an urban scene. *IEEE Internet Things J.* **2020**, *8*, 7521–7530. [CrossRef]
15. Zeng, Q.; Tang, Y.; Yu, Z.; Xu, W. A geographical routing protocol based on link connectivity analysis for urban VANETs. *J. Internet Technol.* **2020**, *21*, 41–49.
16. Chehri, A.; Chehri, H.; Hakim, N.; Saadane, R. Realistic 5.9 GHz DSRC vehicle-to-vehicle wireless communication protocols for cooperative collision warning in underground mining. In *Smart Transportation Systems 2020*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 133–141.
17. Wang, P.; Chen, C.M.; Kumari, S.; Shojafar, M.; Tafazolli, R.; Liu, Y.N. HDMA: Hybrid D2D message authentication scheme for 5G-enabled VANETs. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 5071–5080. [CrossRef]
18. Ji, B.; Zhang, X.; Mumtaz, S.; Han, C.; Li, C.; Wen, H.; Wang, D. Survey on the internet of vehicles: Network architectures and applications. *IEEE Commun. Stand. Mag.* **2020**, *4*, 34–41. [CrossRef]
19. Sharma, S.; Kaul, A. VANETs cloud: Architecture, applications, challenges, and issues. *Arch. Comput. Methods Eng.* **2021**, *28*, 2081–2102. [CrossRef]
20. Hasrouny, H.; Samhat, A.E.; Bassil, C.; Laouiti, A. VANet security challenges and solutions: A survey. *Veh. Commun.* **2017**, *7*, 7–20. [CrossRef]
21. Lee, M.; Atkison, T. Vanet applications: Past, present, and future. *Veh. Commun.* **2021**, *28*, 100310. [CrossRef]
22. Yogarayan, S. Wireless Ad Hoc Network of MANET, VANET, FANET and SANET: A Review. *J. Telecommun. Electron. Comput. Eng.* **2021**, *13*, 13–18.
23. Chriki, A.; Touati, H.; Snoussi, H.; Kamoun, F. FANET: Communication, mobility models and security issues. *Comput. Netw.* **2019**, *163*, 106877. [CrossRef]
24. Khan, I.U.; Qureshi, I.M.; Aziz, M.A.; Cheema, T.A.; Shah, S.B.H. Smart IoT control-based nature inspired energy efficient routing protocol for flying ad hoc network (FANET). *IEEE Access* **2020**, *8*, 56371–56378. [CrossRef]

25. Albu-Salih, A.T.; Khudhair, H.A. ASR-FANET: An adaptive SDN-based routing framework for FANET. *Int. J. Electr. Comput. Eng.* **2021**, *11*, 4403–4412. [CrossRef]
26. Bujari, A.; Palazzi, C.E.; Ronzani, D. FANET application scenarios and mobility models. In Proceedings of the 3rd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications, Niagara Falls, NY, USA, 23 June 2017; pp. 43–46.
27. De Rango, F.; Potrino, G.; Tropea, M.; Santamaria, A.F.; Fazio, P. Scalable and ligthway bio-inspired coordination protocol for FANET in precision agriculture applications. *Comput. Electr. Eng.* **2019**, *74*, 305–318. [CrossRef]
28. Hakimi, A.; Yusof, K.M.; Azizan, M.A.; Azman, M.A.A.; Hussain, S.M. A Survey on Internet of Vehicle (IoV): A pplications & Comparison of VANETs, IoV and SDN-IoV. *ELEKTRIKA-J. Electr. Eng.* **2021**, *20*, 26–31.
29. Benalia, E.; Bitam, S.; Mellouk, A. Data dissemination for Internet of vehicle based on 5G communications: A survey. *Trans. Emerg. Telecommun. Technol.* **2020**, *31*, e3881. [CrossRef]
30. Kim, S.K.A. Enhanced IoV security network by using blockchain governance game. *Mathematics* **2021**, *9*, 109. [CrossRef]
31. Sharma, S.; Ghanshala, K.K.; Mohan, S. A security system using deep learning approach for internet of vehicles (IoV). In Proceedings of the 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 8–10 November 2018; pp. 1–5.
32. Ang, L.M.; Seng, K.P.; Ijemaru, G.K.; Zungeru, A.M. Deployment of IoV for smart cities: Applications, architecture, and challenges. *IEEE Access* **2018**, *7*, 6473–6492. [CrossRef]
33. Zaidi, S.; Atiquzzaman, M.; Calafate, C.T. Internet of flying things (IoFT): A survey. *Comput. Commun.* **2021**, *165*, 53–74. [CrossRef]
34. Garg, T.; Kagalwalla, N.; Churi, P.; Pawar, A.; Deshmukh, S. A survey on security and privacy issues in IoV. *Int. J. Electr. Comput. Eng.* **2020**, *10*, 5409–5419. [CrossRef]
35. Raja, G.; Dhanasekaran, P.; Anbalagan, S.; Ganapathisubramaniyan, A.; Bashir, A.K. SDN-enabled traffic alert system for IoV in smart cities. In Proceedings of the IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 6–9 July 2020; pp. 1093–1098.
36. Kurt, G.K.; Khoshkholgh, M.G.; Alfattani, S.; Ibrahim, A.; Darwish, T.S.; Alam, M.S.; Yanikomeroglu, H.; Yongacoglu, A. A vision and framework for the high altitude platform station (HAPS) networks of the future. *IEEE Commun. Surv. Tutorials* **2021**, *23*, 729–779. [CrossRef]
37. Khan, I.U.; Shah, S.B.H.; Wang, L.; Aziz, M.A.; Stephan, T.; Kumar, N. Routing protocols & unmanned aerial vehicles autonomous localization in flying networks. In *International Journal of Communication Systems*; John Wiley & Sons: New York, NY, USA, 2021; p. e4885.
38. Guerna, A.; Bitam, S.; Calafate, C.T. Roadside unit deployment in internet of vehicles systems: A survey. *Sensors* **2022**, *22*, 3190. [CrossRef] [PubMed]
39. Qiu, J.; Chen, Y.; Zhang, X.; Liu, Q.; Li, W.; Pei, Y.; Liu, L. Standardization evolution and typical solutions of IoV. In Proceedings of the 2019 28th Wireless and Optical Communications Conference (WOCC), Beijing, China, 9–10 May 2019; pp. 1–4.
40. Jayapandian, N. Cloud enabled smart firefighting drone using internet of things. In Proceedings of the 2019 International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 27–29 November 2019; pp. 1079–1083.
41. Dureja, A.; Sangwan, S. A Review: Efficient Transportation—Future Aspects of IoV. In Proceedings of ETCCS 2020, Evolving Technologies for Computing, Communication and Smart World; Noida, India, 31 January–1 February 2020; pp. 97–108.
42. Bindu, R.; Preethi Sejal, M.; Chetan, H. A Survey Paper on Evolution of Vanet Towards IOV. In Proceedings of the Optical and Wireless Technologies: Proceedings of OWT 2021, Jaipur, India, 17–20 March 2021; Springer: Berlin/Heidelberg, Germany, 2022; pp. 99–113.
43. Sadiku, M.N.; Tembely, M.; Musa, S.M. Internet of vehicles: An introduction. *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* **2018**, *8*, 11. [CrossRef]
44. Liu, K.; Xu, X.; Chen, M.; Liu, B.; Wu, L.; Lee, V.C. A hierarchical architecture for the future internet of vehicles. *IEEE Commun. Mag.* **2019**, *57*, 41–47. [CrossRef]
45. Chen, M.; Tian, Y.; Fortino, G.; Zhang, J.; Humar, I. Cognitive internet of vehicles. *Comput. Commun.* **2018**, *120*, 58–70. [CrossRef]
46. Alouache, L.; Nguyen, N.; Aliouat, M.; Chelouah, R. Toward a hybrid SDN architecture for V2V communication in IoV environment. In Proceedings of the 2018 Fifth International Conference on Software Defined Systems (SDS), Barcelona, Spain, 23–26 April 2018; pp. 93–99.
47. Contreras-Castillo, J.; Zeadally, S.; Guerrero-Ibañez, J.A. Internet of vehicles: Architecture, protocols, and security. *IEEE Internet Things J.* **2017**, *5*, 3701–3709. [CrossRef]
48. Muhammad, A.; Saqib, M.; Song, W.C. Sensor virtualization and data orchestration in internet of vehicles (iov). In Proceedings of the 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), Bordeaux, France, 17–21 May 2021; pp. 998–1003.
49. Hichri, Y.; Dahi, S.; Fathallah, H. Candidate architectures for emerging IoV: A survey and comparative study. *Des. Autom. Embed. Syst.* **2021**, *25*, 237–263. [CrossRef]
50. Pozna, C.; Precup, R.E.; Földesi, P. A Novel Pose Estimation Algorithm for Robotic Navigation. *Robot. Auton. Syst.* **2015**, *63*, 10–21. [CrossRef]
51. Gasmi, R.; Aliouat, M. Vehicular ad hoc networks versus internet of vehicles-a comparative view. In Proceedings of the 2019 International Conference on Networking and Advanced Systems (ICNAS), Annaba, Algeria, 26–27 June 2019; pp. 1–6.

52. Hasan, K.F.; Kaur, T.; Hasan, M.M.; Feng, Y. Cognitive internet of vehicles: Motivation, layered architecture and security issues. In Proceedings of the 2019 International Conference on Sustainable Technologies for Industry 4.0 (STI), Dhaka, Bangladesh, 24–25 Decemeber 2019; pp. 1–6.
53. Hasan, K.F.; Overall, A.; Ansari, K.; Ramachandran, G.; Jurdak, R. Security, privacy and trust: Cognitive internet of vehicles. *arXiv* **2021**, arXiv:2104.12878.
54. Dias Santana, G.M.; Cristo, R.S.d.; Lucas Jaquie Castelo Branco, K.R. Integrating cognitive radio with unmanned aerial vehicles: An overview. *Sensors* **2021**, *21*, 830. [CrossRef]
55. Aftab, F.; Khan, A.; Zhang, Z. Hybrid self-organized clustering scheme for drone based cognitive Internet of Things. *IEEE Access* **2019**, *7*, 56217–56227. [CrossRef]
56. Arooj, A.; Farooq, M.S.; Umer, T.; Shan, R.U. Cognitive internet of vehicles and disaster management: A proposed architecture and future direction. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e3625. [CrossRef]
57. Chen, C.; Liu, L.; Qiu, T.; Jiang, J.; Pei, Q.; Song, H. Routing with traffic awareness and link preference in internet of vehicles. *IEEE Trans. Intell. Transp. Syst.* **2020**, *23*, 200–214. [CrossRef]
58. Arooj, A.; Farooq, M.S.; Akram, A.; Iqbal, R.; Sharma, A.; Dhiman, G. Big data processing and analysis in internet of vehicles: architecture, taxonomy, and open research challenges. *Arch. Comput. Methods Eng.* **2022**, *29*, 793–829. [CrossRef]
59. Ouahouah, S.; Bagaa, M.; Prados-Garzon, J.; Taleb, T. Deep-reinforcement-learning-based collision avoidance in uav environment. *IEEE Internet Things J.* **2021**, *9*, 4015–4030. [CrossRef]
60. Ullah, Z.; Al-Turjman, F.; Mostarda, L. Cognition in UAV-aided 5G and beyond communications: A survey. *IEEE Trans. Cogn. Commun. Netw.* **2020**, *6*, 872–891. [CrossRef]
61. Li, X.; Gao, X.; Liu, Y.; Huang, G.; Zeng, M.; Qiao, D. Overlay cognitive radio-assisted NOMA intelligent transportation systems with imperfect SIC and CEEs. *Chin. J. Electron.* **2023**, *32*, 1258–1270.
62. Proos, D.P.; Carlsson, N. Performance comparison of messaging protocols and serialization formats for digital twins in IoV. In Proceedings of the 2020 IFIP Networking Conference (Networking), Paris, France, 22–26 June 2020; pp. 10–18.
63. Sanguesa, J.A.; Barrachina, J.; Fogue, M.; Garrido, P.; Martinez, F.J.; Cano, J.C.; Calafate, C.T.; Manzoni, P. Sensing traffic density combining V2V and V2I wireless communications. *Sensors* **2015**, *15*, 31794–31810. [CrossRef]
64. Peter, M.N.; Rani, M.P. V2V Communication and Authentication: The Internet of Things Vehicles (Iotv). *Wirel. Pers. Commun.* **2021**, *120*, 231–247. [CrossRef]
65. Wang, Y.; Hu, X.; Guo, L.; Yao, Z. Research on V2I/V2V Hybrid Multi-hop Edge Computing Offloading Algorithm in IoV Environment. In Proceedings of the 2020 IEEE 5th International Conference on Intelligent Transportation Engineering (ICITE), Beijing, China, 11–13 September 2020; pp. 336–340.
66. Duan, W.; Gu, J.; Wen, M.; Zhang, G.; Ji, Y.; Mumtaz, S. Emerging technologies for 5G-IoV networks: Applications, trends and opportunities. *IEEE Netw.* **2020**, *34*, 283–289. [CrossRef]
67. Cheng, J.; Yuan, G.; Zhou, M.; Gao, S.; Liu, C.; Duan, H.; Zeng, Q. Accessibility analysis and modeling for IoV in an urban scene. *IEEE Trans. Veh. Technol.* **2020**, *69*, 4246–4256. [CrossRef]
68. Li, X.; Feng, W.; Wang, J.; Chen, Y.; Ge, N.; Wang, C.X. Enabling 5G on the ocean: A hybrid satellite-UAV-terrestrial network solution. *IEEE Wirel. Commun.* **2020**, *27*, 116–121. [CrossRef]
69. Wu, Q.; Xu, J.; Zeng, Y.; Ng, D.W.K.; Al-Dhahir, N.; Schober, R.; Swindlehurst, A.L. A comprehensive overview on 5G-and-beyond networks with UAVs: From communications to sensing and intelligence. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 2912–2945. [CrossRef]
70. Zeng, Y.; Wu, Q.; Zhang, R. Accessing from the sky: A tutorial on UAV communications for 5G and beyond. *Proc. IEEE* **2019**, *107*, 2327–2375. [CrossRef]
71. Obaidat, M.; Khodjaeva, M.; Holst, J.; Ben Zid, M. Security and privacy challenges in vehicular ad hoc networks. In *Connected Vehicles in the Internet of Things: Concepts, Technologies and Frameworks for the IoV*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 223–251.
72. Sharma, S.; Ghanshala, K.K.; Mohan, S. Blockchain based internet of vehicles (IoV): An efficient secure ad hoc vehicular networking architecture. In Proceedings of the 2019 IEEE 2nd 5G World Forum (5GWF), Dresden, Germany, 30 September–2 October 2019; pp. 452–457.
73. Li, B.; Deng, X.; Deng, Y. Mobile-edge computing-based delay minimization controller placement in SDN-IoV. *Comput. Netw.* **2021**, *193*, 108049. [CrossRef]
74. Jamalzadeh, M.; Maadani, M.; Mahdavi, M. EC-MOPSO: An edge computing-assisted hybrid cluster and MOPSO-based routing protocol for the Internet of Vehicles. *Ann. Telecommun.* **2022**, *77*, 491–503. [CrossRef]
75. Sennan, S.; Ramasubbareddy, S.; Balasubramaniyam, S.; Nayyar, A.; Kerrache, C.A.; Bilal, M. MADCR: Mobility aware dynamic clustering-based routing protocol in Internet of Vehicles. *China Commun.* **2021**, *18*, 69–85. [CrossRef]
76. Cheng, F.; Shao, C. Research on Artificial Fish Swarm Clustering Algorithm in Urban Internet of Vehicles. In Proceedings of the 2020 IEEE International Conference on Smart Internet of Things (SmartIoT), Beijing, China, 14–16 August 2020; pp. 328–332.
77. Ebadinezhad, S.; Dereboylu, Z.; Ever, E. Clustering-based modified ant colony optimizer for internet of vehicles (CACOIOV). *Sustainability* **2019**, *11*, 2624. [CrossRef]
78. Khan, M.F.; Aadil, F.; Maqsood, M.; Bukhari, S.H.R.; Hussain, M.; Nam, Y. Moth flame clustering algorithm for internet of vehicle (MFCA-IoV). *IEEE Access* **2018**, *7*, 11613–11629. [CrossRef]

79. Aadil, F.; Ahsan, W.; Rehman, Z.U.; Shah, P.A.; Rho, S.; Mehmood, I. Clustering algorithm for internet of vehicles (IoV) based on dragonfly optimizer (CAVDO). *J. Supercomput.* **2018**, *74*, 4542–4567. [CrossRef]
80. Gasmi, R.; Aliouat, M.; Seba, H. Geographical Information Based Clustering Algorithm for Internet of Vehicles. In Proceedings of the International Conference on Machine Learning for Networking, Paris, France, 24–26 November 2020; pp. 107–121.
81. Mahmood, A.; Siddiqui, S.A.; Sheng, Q.Z.; Zhang, W.E.; Suzuki, H.; Ni, W. Trust on wheels: Towards secure and resource efficient IoV networks. *Computing* **2022**, *104*, 1337–1358. [CrossRef]
82. Senouci, O.; Harous, S.; Aliouat, Z. An efficient weight-based clustering algorithm using mobility report for IoV. In Proceedings of the 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 8–10 November 2018; pp. 614–620.
83. Senouci, O.; Harous, S.; Aliouat, Z. A new heuristic clustering algorithm based on RSU for internet of vehicles. *Arab. J. Sci. Eng.* **2019**, *44*, 9735–9753. [CrossRef]
84. Shivaraman, N.; Ramanathan, S.; Shanker, S.; Easwaran, A.; Steinhorst, S. Decoric: Decentralized connected resilient iot clustering. In Proceedings of the 2020 29th International Conference on Computer Communications and Networks (ICCCN), Honolulu, HI, USA, 3–6 August 2020; pp. 1–10.
85. Wang, S.; Chen, G.; Jiang, Y.; You, X. A Cluster-based V2V Approach for Mixed Data Dissemination in Urban Scenario of IoVs. *IEEE Trans. Veh. Technol.* **2022**, *72*, 2907–2920. [CrossRef]
86. Qureshi, K.N.; Idrees, M.M.; Lloret, J.; Bosch, I. Self-assessment based clustering data dissemination for sparse and dense traffic conditions for internet of vehicles. *IEEE Access* **2020**, *8*, 10363–10372. [CrossRef]
87. Ji, B.; Zhang, M.; Xing, L.; Li, X.; Li, C.; Han, C.; Wen, H. Research on optimal intelligent routing algorithm for IoV with machine learning and smart contract. *Digit. Commun. Netw.* **2023**, *9*, 47–55. [CrossRef]
88. Yang, H.; Liu, H.; Luo, C.; Wu, Y.; Li, W.; Zomaya, A.Y.; Song, L.; Xu, W. Vehicle-key: A secret key establishment scheme for LoRa-enabled IoV communications. In Proceedings of the 2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS), Bologna, Italy, 10–13 July 2022; pp. 787–797.
89. Harrabi, S.; Jaafar, I.B.; Ghedira, K. Survey on IoV Routing Protocols. *Wirel. Pers. Commun.* **2023**, *128*, 791–811. [CrossRef]
90. Alouache, L.; Nguyen, N.; Aliouat, M.; Chelouah, R. Survey on IoV routing protocols: Security and network architecture. *Int. J. Commun. Syst.* **2019**, *32*, e3849. [CrossRef]
91. Dhurandher, S.K.; Singh, J.; Woungang, I.; Gupta, M.; Sabharwal, N. Geometric Shapes-based PSO Approach for Routing in Vehicular Networks. In Proceedings of the 2019 IEEE AFRICON, Accra, Ghana, 25–27 September 2019; pp. 1–7.
92. BrijilalRuban, C.; Paramasivan, B. Energy Efficient Enhanced OLSR Routing Protocol Using Particle Swarm Optimization with Certificate Revocation Scheme for VANET. *Wirel. Pers. Commun.* **2021**, *121*, 2589–2608. [CrossRef]
93. Ramasamy, V.; Srirangan, J.; Ramalingam, P. Fuzzy and position particle swarm optimized routing in VANET. *Int. J. Electr. Comput. Eng. Syst.* **2021**, *12*, 199–206. [CrossRef]
94. AL-Shammari, M.Q.; Muniyandi, R.C. Optimised tail-based routing for VANETs using multi-objective particle swarm optimisation with angle searching. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*. [CrossRef]
95. Javadpour, A.; Rezaei, S.; Sangaiah, A.K.; Slowik, A.; Mahmoodi Khaniabadi, S. Enhancement in quality of routing service using metaheuristic PSO algorithm in VANET networks. *Soft Comput.* **2023**, *27*, 2739–2750. [CrossRef]
96. Husain, A.; Singh, S.P.; Sharma, S. PSO optimized geocast routing in VANET. *Wirel. Pers. Commun.* **2020**, *115*, 2269–2288. [CrossRef]
97. Fatemidokht, H.; Kuchaki Rafsanjani, M. F-Ant: An effective routing protocol for ant colony optimization based on fuzzy logic in vehicular ad hoc networks. *Neural Comput. Appl.* **2018**, *29*, 1127–1137. [CrossRef]
98. Saravana Kumar, N.; Pagadala, P.K.; Vijayakumar, V.; Kavinya, A. Multi Objective Glow Swarm Based Situation and Quality Aware Routing in VANET. *Wirel. Pers. Commun.* **2022**, *125*, 879–895. [CrossRef]
99. Rewadkar, D.; Doye, D. FGWSO-TAR: Fractional glowworm swarm optimization for traffic aware routing in urban VANET. *Int. J. Commun. Syst.* **2018**, *31*, e3430. [CrossRef]
100. Gawas, M.A.; Govekar, S.S. A novel selective cross layer based routing scheme using ACO method for vehicular networks. *J. Netw. Comput. Appl.* **2019**, *143*, 34–46. [CrossRef]
101. Singh, G.D.; Prateek, M.; Kumar, S.; Verma, M.; Singh, D.; Lee, H.N. Hybrid genetic firefly algorithm-based routing protocol for VANETs. *IEEE Access* **2022**, *10*, 9142–9151. [CrossRef]
102. Saini, T.K.; Sharma, S.C. Prominent unicast routing protocols for Mobile Ad hoc Networks: Criterion, classification, and key attributes. *Ad Hoc Netw.* **2019**, *89*, 58–77. [CrossRef]
103. Bhoi, S.K.; Sahu, P.K.; Singh, M.; Khilar, P.M.; Sahoo, R.R.; Swain, R.R. Local traffic aware unicast routing scheme for connected car system. *IEEE Trans. Intell. Transp. Syst.* **2019**, *21*, 2360–2375. [CrossRef]
104. Bousbaa, F.Z.; Kerrache, C.A.; Mahi, Z.; Tahari, A.E.K.; Lagraa, N.; Yagoubi, M.B. GeoUAVs: A new geocast routing protocol for fleet of UAVs. *Comput. Commun.* **2020**, *149*, 259–269. [CrossRef]
105. Gallego-Tercero, L.R.; Menchaca-Mendez, R.; Rivero-Angeles, M.E.; Menchaca-Mendez, R. Efficient time-stable geocast routing in delay-tolerant vehicular ad-hoc networks. *IEEE Access* **2020**, *8*, 171034–171048. [CrossRef]
106. Boucetta, S.I.; Johanyák, Z.C. Optimized Ad-hoc Multi-hop Broadcast Protocol for Emergency Message Dissemination in Vehicular Ad-hoc Networks. *Acta Polytech. Hung.* **2022**, *19*, 23–42. [CrossRef]

107. Nahar, A.; Sikarwar, H.; Das, D. Csbr: A cosine similarity based selective broadcast routing protocol for vehicular ad-hoc networks. In Proceedings of the 2020 IFIP Networking Conference (Networking), Paris, France, 22–26 June 2020; pp. 404–412.
108. LiWang, M.; Hosseinalipour, S.; Gao, Z.; Tang, Y.; Huang, L.; Dai, H. Allocation of computation-intensive graph jobs over vehicular clouds in IoV. *IEEE Internet Things J.* **2019**, *7*, 311–324. [CrossRef]
109. Tan, C.; Li, X.; Luan, T.H.; Gu, B.; Qu, Y.; Gao, L. Digital twin based remote resource sharing in internet of vehicles using consortium blockchain. In Proceedings of the 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall), Virtual, 27 September–28 October 2021; pp. 1–6.
110. Raza, S.; Wang, S.; Ahmed, M.; Anwar, M.R.; et al. A survey on vehicular edge computing: Architecture, applications, technical issues, and future directions. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 3159762. [CrossRef]
111. Ahmed, M.; Haskell-Dowland, P. *Secure Edge Computing: Applications, Techniques and Challenges*; CRC Press: Boca Raton, FL, USA, 2021.
112. Singh, J.; Singh, G.; Aggarwal, G. Inclusion of Aerial Computing in Internet of Things: Prospects and Applications. In Proceedings of the 2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT), Kannur, India, 11–12 August 2022; pp. 1664–1669.
113. Sodhro, A.H.; Obaidat, M.S.; Abbasi, Q.H.; Pace, P.; Pirbhulal, S.; Fortino, G.; Imran, M.A.; Qaraqe, M. Quality of service optimization in an IoT-driven intelligent transportation system. *IEEE Wirel. Commun.* **2019**, *26*, 10–17. [CrossRef]
114. Kadhim, A.J.; Naser, J.I. Proactive load balancing mechanism for fog computing supported by parked vehicles in IoV-SDN. *China Commun.* **2021**, *18*, 271–289. [CrossRef]
115. Li, Y.; Li, H.; Xu, G.; Xiang, T.; Lu, R. Practical Privacy-Preserving Federated Learning in Vehicular Fog Computing. *IEEE Trans. Veh. Technol.* **2022**, *71*, 4692–4705. [CrossRef]
116. Wang, H.; Liu, T.; Kim, B.; Lin, C.W.; Shiraishi, S.; Xie, J.; Han, Z. Architectural design alternatives based on cloud/edge/fog computing for connected vehicles. *IEEE Commun. Surv. Tutorials* **2020**, *22*, 2349–2377. [CrossRef]
117. Nazih, O.; Benamar, N.; Lamaazi, H.; Chaoui, H. Challenges and future directions for security and privacy in vehicular fog computing. In Proceedings of the 2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), Sakheer, Bahrain, 20–21 November 2022; pp. 693–699.
118. Rihan, M.; Elwekeil, M.; Yang, Y.; Huang, L.; Xu, C.; Selim, M.M. Deep-VFog: When artificial intelligence meets fog computing in V2X. *IEEE Syst. J.* **2020**, *15*, 3492–3505. [CrossRef]
119. Cui, M.; Han, D.; Wang, J.; Li, K.C.; Chang, C.C. ARFV: An efficient shared data auditing scheme supporting revocation for fog-assisted vehicular ad-hoc networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 15815–15827. [CrossRef]
120. Akyildiz, O.; Kök, I.; Okay, F.Y.; Özdemir, S. A P4-assisted task offloading scheme for Fog networks: An intelligent transportation system scenario. *Internet Things* **2023**, *22*, 100695. [CrossRef]
121. Saleem, M.A.; Mahmood, K.; Kumari, S. Comments on "AKM-IoV: Authenticated key management protocol in fog computing-based internet of vehicles deployment". *IEEE Internet Things J.* **2020**, *7*, 4671–4675. [CrossRef]
122. Al Ridhawi, I.; Aloqaily, M.; Boukerche, A. Comparing fog solutions for energy efficiency in wireless networks: Challenges and opportunities. *IEEE Wirel. Commun.* **2019**, *26*, 80–86. [CrossRef]
123. Ampatzidis, Y.; Partel, V.; Costa, L. Agroview: Cloud-based application to process, analyze and visualize UAV-collected data for precision agriculture applications utilizing artificial intelligence. *Comput. Electron. Agric.* **2020**, *174*, 105457. [CrossRef]
124. Nasir, A.A. Latency optimization of UAV-enabled MEC system for virtual reality applications under rician fading channels. *IEEE Wirel. Commun. Lett.* **2021**, *10*, 1633–1637. [CrossRef]
125. Zhou, Y.; Pan, C.; Yeoh, P.L.; Wang, K.; Elkashlan, M.; Vucetic, B.; Li, Y. Communication-and-computing latency minimization for UAV-enabled virtual reality delivery systems. *IEEE Trans. Commun.* **2020**, *69*, 1723–1735. [CrossRef]
126. Herich, D.; Vaščák, J. Multi-vehicle SLAM in IoV Networks. In Proceedings of the 2022 Cybernetics & Informatics (K&I), Visegrad, Hungary, 11–14 September 2022; pp. 1–6.
127. Fotouhi, A.; Qiang, H.; Ding, M.; Hassan, M.; Giordano, L.G.; Garcia-Rodriguez, A.; Yuan, J. Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges. *IEEE Commun. Surv. Tutorials* **2019**, *21*, 3417–3442. [CrossRef]
128. Karim, S.M.; Habbal, A.; Chaudhry, S.A.; Irshad, A. Architecture, protocols, and security in IoV: Taxonomy, analysis, challenges, and solutions. *Secur. Commun. Netw.* **2022**, *2022*, 1131479. [CrossRef]
129. Campanile, L.; Iacono, M.; Marulli, F.; Mastroianni, M. Privacy regulations challenges on data-centric and iot systems: A case study for smart vehicles. In Proceedings of the IoTBDS, Prague, Czech Republic, 7–9 May 2020; pp. 507–518.
130. Liu, J.; Wang, X.A.; Liu, Z.; Wang, H.; Yang, X. Privacy-preserving public cloud audit scheme supporting dynamic data for unmanned aerial vehicles. *IEEE Access* **2020**, *8*, 79428–79439. [CrossRef]
131. Ahmed, I.; Jeon, G.; Ahmad, A. Deep learning-based intrusion detection system for internet of vehicles. *IEEE Consum. Electron. Mag.* **2021**, *12*, 117–123. [CrossRef]
132. Fu, W.; Xin, X.; Guo, P.; Zhou, Z. A practical intrusion detection system for Internet of vehicles. *China Commun.* **2016**, *13*, 263–275. [CrossRef]
133. Fotohi, R.; Abdan, M.; Ghasemi, S. A self-adaptive intrusion detection system for securing UAV-to-UAV communications based on the human immune system in UAV networks. *J. Grid Comput.* **2022**, *20*, 22. [CrossRef]

134. Whelan, J.; Sangarapillai, T.; Minawi, O.; Almehmadi, A.; El-Khatib, K. Novelty-based intrusion detection of sensor attacks on unmanned aerial vehicles. In Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks, Alicante Spain, 16–20 November 2020; pp. 23–28.
135. Basan, E.; Lapina, M.; Mudruk, N.; Abramov, E. Intelligent intrusion detection system for a group of UAVs. In Proceedings of the Advances in Swarm Intelligence: 12th International Conference, ICSI 2021, Qingdao, China, 17–21 July 2021; Proceedings, Part II 12; Springer: Berlin/Heidelberg, Germany, 2021; pp. 230–240.
136. Ullah, Z.; Al-Turjman, F.; Moatasim, U.; Mostarda, L.; Gagliardi, R. UAVs joint optimization problems and machine learning to improve the 5G and Beyond communication. *Comput. Netw.* **2020**, *182*, 107478. [CrossRef]
137. Li, X.; Zhao, T.; Arora, R.; Liu, H.; Hong, M. On faster convergence of cyclic block coordinate descent-type methods for strongly convex minimization. *J. Mach. Learn. Res.* **2018**, *18*, 1–24.
138. Sharma, D.; Rashid, A.; Gupta, S.; Gupta, S.K. A functional encryption technique in UAV integrated HetNet: A proposed model. *Int. J. Simul.-Sci. Technol* **2019**, *20*, 7.1–7.7. [CrossRef]
139. Xu, F.; Ahmad, S.; Ahmed, M.; Raza, S.; Khan, F.; Ma, Y.; Khan, W.U. Beyond Encryption: Exploring the Potential of Physical Layer Security in UAV Networks. *J. King Saud-Univ.-Comput. Inf. Sci.* **2023**, *35*, 101717. [CrossRef]
140. Samad, A.; Alam, S.; Mohammed, S.; Bhukhari, M. Internet of vehicles (IoV) requirements, attacks and countermeasures. In Proceedings of the 12th INDIACom, INDIACom-2018, 5th International Conference on "Computing for Sustainable Global Development" IEEE Conference, New Delhi India, 14–16 March 2018; pp. 1–4.
141. He, Z.; Zou, E.; Guan, C.; Pang, B.; Tang, G.; Ding, J. Research and Application of 5G Remote Control UAV with Aerial Electronic Fence. *Proc. J. Physics: Conf. Ser.* **2023**, *2419*, 012109. [CrossRef]
142. Wang, Q.; Dai, H.N.; Wang, H.; Xu, G.; Sangaiah, A.K. UAV-enabled friendly jamming scheme to secure industrial Internet of Things. *J. Commun. Netw.* **2019**, *21*, 481–490. [CrossRef]
143. Hussain, A.; Abughanam, N.; Sciancalepore, S.; Yaacoub, E.; Mohamed, A. Jammer Localization in the Internet of Vehicles: Scenarios, Experiments, and Evaluation. In Proceedings of the 12th International Conference on the Internet of Things, Delft, The Netherlands, 7–10 November 2022;pp. 73–80.
144. Xi, N.; Li, W.; Jing, L.; Ma, J. ZAMA: A ZKP-based anonymous mutual authentication scheme for the IoV. *IEEE Internet Things J.* **2022**, *9*, 22903–22913. [CrossRef]
145. Chen, C.M.; Xiang, B.; Liu, Y.; Wang, K.H. A secure authentication protocol for internet of vehicles. *IEEE Access* **2019**, *7*, 12047–12057. [CrossRef]
146. Pitchai, M.P.; Ramachandran, M.; Al-Turjman, F.; Mostarda, L. Intelligent Framework for Secure Transportation Systems Using Software-Defined-Internet of Vehicles. *Comput. Mater. Contin.* **2021**, *68*, 3947. [CrossRef]
147. Vasconcelos, G.; Miani, R.S.; Guizilini, V.C.; Souza, J.R. Evaluation of dos attacks on commercial wi-fi-based uavs. *Int. J. Commun. Netw. Inf. Secur.* **2019**, *11*, 212–223. [CrossRef]
148. Watkins, L.; Ramos, J.; Snow, G.; Vallejo, J.; Robinson, W.H.; Rubin, A.D.; Ciocco, J.; Jedrzejewski, F.; Liu, J.; Li, C. Exploiting multi-vendor vulnerabilities as back-doors to counter the threat of rogue small unmanned aerial systems. In Proceedings of the 1st ACM MobiHoc Workshop on Mobile IoT Sensing, Security, and Privacy, Los Angeles, CA, USA, 26 June 2018; pp. 1–6.
149. Sakiz, F.; Sen, S. A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. *Ad Hoc Netw.* **2017**, *61*, 33–50. [CrossRef]
150. Li, M.; Kou, Y.; Xu, Y.; Liu, Y. Design and field test of a GPS spoofer for UAV trajectory manipulation. In Proceedings of the China Satellite Navigation Conference (CSNC) 2018 Proceedings, Harbin, China, 23–25 May 2018; Volume II, pp. 161–173.
151. Shrivastava, A. Distributed Denial of Service (DDoS) Attack on Unmanned Aerial Vehicle. Ph.D. Thesis, Delhi Technological University: New Delhi, India, 2022.
152. Jameii, S.M.; Zamirnaddafi, R.S.; Rezabakhsh, R. Internet of Flying Things security: A systematic review. *Concurr. Comput. Pract. Exp.* **2022**, *34*, e7213. [CrossRef]
153. Shafiee, M.; Zhou, Z.; Mei, L.; Dinmohammadi, F.; Karama, J.; Flynn, D. Unmanned aerial drones for inspection of offshore wind turbines: A mission-critical failure analysis. *Robotics* **2021**, *10*, 26. [CrossRef]
154. Hussain, S.A.; Yusof, K.M.; Hussain, S.M.; Singh, A.V. A review of quality of service issues in Internet of Vehicles (IoV). In Proceedings of the 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, 4–6 Feburbary 2019; pp. 380–383.
155. Zavvos, E.; Gerding, E.H.; Yazdanpanah, V.; Maple, C.; Stein, S. Privacy and Trust in the Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 10126–10141. [CrossRef]
156. Dahmane, S.; Yagoubi, M.B.; Kerrache, C.A.; Lorenz, P.; Lagraa, N.; Lakas, A. Toward a Secure Edge-Enabled and Artificially Intelligent Internet of Flying Things Using Blockchain. *IEEE Internet Things Mag.* **2022**, *5*, 90–95. [CrossRef]
157. Mfenjou, M.L.; Ari, A.A.A.; Abdou, W.; Spies, F. Methodology and trends for an intelligent transport system in developing countries. *Sustain. Comput. Inform. Syst.* **2018**, *19*, 96–111. [CrossRef]
158. Hahn, D.; Munir, A.; Behzadan, V. Security and privacy issues in intelligent transportation systems: Classification and challenges. *IEEE Intell. Transp. Syst. Mag.* **2019**, *13*, 181–196. [CrossRef]
159. Rejeb, A.; Abdollahi, A.; Rejeb, K.; Treiblmaier, H. Drones in agriculture: A review and bibliometric analysis. *Comput. Electron. Agric.* **2022**, *198*, 107017. [CrossRef]

160. Pathak, H.; Kumar, G.; Mohapatra, S.; Gaikwad, B.; Rane, J. Use of drones in agriculture: Potentials, Problems and Policy Needs. *Icar-Natl. Inst. Abiotic Stress Manag.* **2020**, *300*, 4–15.
161. Chyrva, I.; Jermy, M.; Strand, T.; Richardson, B. Evaluation of the pattern of spray released from a moving multicopter. *Pest Manag. Sci.* **2023**, *79*, 1483–1499. [CrossRef] [PubMed]
162. Bai, Y.; Zhang, B.; Xu, N.; Zhou, J.; Shi, J.; Diao, Z. Vision-based navigation and guidance for agricultural autonomous vehicles and robots: A review. *Comput. Electron. Agric.* **2023**, *205*, 107584. [CrossRef]
163. Ghobadpour, A.; Monsalve, G.; Cardenas, A.; Mousazadeh, H. Off-road electric vehicles and autonomous robots in agricultural sector: Trends, challenges, and opportunities. *Vehicles* **2022**, *4*, 843–864. [CrossRef]
164. Moshref-Javadi, M.; Winkenbach, M. Applications and Research avenues for drone-based models in logistics: A classification and review. *Expert Syst. Appl.* **2021**, *177*, 114854. [CrossRef]
165. Sah, B.; Gupta, R.; Bani-Hani, D. Analysis of barriers to implement drone logistics. *Int. J. Logist. Res. Appl.* **2021**, *24*, 531–550. [CrossRef]
166. Manjrekar, A.; Jha, D.S.; Jagtap, P.; Yadav, V. Warehouse inventory management with cycle counting using drones. In Proceedings of the 4th International Conference on Advances in Science & Technology (ICAST2021), Bahir Dar, Ethiopia, 27–29 August 2021.
167. Deja, M.; Siemiątkowski, M.S.; Vosniakos, G.C.; Maltezos, G. Opportunities and challenges for exploiting drones in agile manufacturing systems. *Procedia Manuf.* **2020**, *51*, 527–534. [CrossRef]
168. Ali, S.S.; Khan, S.; Fatma, N.; Ozel, C.; Hussain, A. Utilisation of drones in achieving various applications in smart warehouse management. *Benchmarking Int. J.* 2023. [CrossRef]
169. Zhang, T. Toward automated vehicle teleoperation: Vision, opportunities, and challenges. *IEEE Internet Things J.* **2020**, *7*, 11347–11354. [CrossRef]
170. Alkouz, B.; Bouguettaya, A.; Mistry, S. Swarm-based drone-as-a-service (sdaas) for delivery. In Proceedings of the 2020 IEEE International Conference on Web Services (ICWS), Beijing, China, 19–23 October 2020; pp. 441–448.
171. Baldisseri, A.; Siragusa, C.; Seghezzi, A.; Mangiaracina, R.; Tumino, A. Truck-based drone delivery system: An economic and environmental assessment. *Transp. Res. Part D Transp. Environ.* **2022**, *107*, 103296. [CrossRef]
172. Nyaaba, A.A.; Ayamga, M. Intricacies of medical drones in healthcare delivery: Implications for Africa. *Technol. Soc.* **2021**, *66*, 101624. [CrossRef]
173. Euchi, J. Do drones have a realistic place in a pandemic fight for delivering medical supplies in healthcare systems problems? *Chin. J. Aeronaut.* **2021**, *34*, 182–190. [CrossRef]
174. Khalid, M.; Awais, M.; Singh, N.; Khan, S.; Raza, M.; Malik, Q.B.; Imran, M. Autonomous transportation in emergency healthcare services: framework, challenges, and future work. *IEEE Internet Things Mag.* **2021**, *4*, 28–33. [CrossRef]
175. Rahman, M.M.; Khatun, F.; Sami, S.I.; Uzzaman, A. The evolving roles and impacts of 5G enabled technologies in healthcare: The world epidemic COVID-19 issues. *Array* **2022**, *14*, 100178. [CrossRef] [PubMed]
176. Carr, C.; Samnani, M.; Tani, J.; McKaig, J.; Hammons, E.; Newman, D.J.; Ho, K.; Ekblaw, A.; Truelove, N. Space Drones: An Opportunity to Include, Engage, Accelerate, and Advance. *EHT Zurich* **2020**.
177. De Simone, C.; Ceci, F.; Alaimo, C. Data Ecosystem and Data Value Chain: An Exploration of Drones Technology Applications. In *Sustainable Digital Transformation: Paving the Way Towards Smart Organizations and Societies*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 203–218.
178. Galvez-Serna, J.; Vanegas, F.; Gonzalez, F.; Flannery, D. Towards a probabilistic based autonomous UAV mission planning for planetary exploration. In Proceedings of the 2021 IEEE Aerospace Conference (50100), Big Sky, MT, USA, 6–13 March 2021; pp. 1–8.
179. Feraru, V.A.; Andersen, R.E.; Boukas, E. Towards an autonomous UAV-based system to assist search and rescue operations in man overboard incidents. In Proceedings of the 2020 IEEE International Symposium on Safety, Security, and Rescue Robotics (SSRR), Abu Dhabi, United Arab Emirates, 4–6 November 2020; pp. 57–64.
180. Valsan, A.; Parvathy, B.; GH, V.D.; Unnikrishnan, R.; Reddy, P.K.; Vivek, A. Unmanned aerial vehicle for search and rescue mission. In Proceedings of the 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI) (48184), Tirunelveli, India, 15–17 June 2020; pp. 684–687.
181. Ilkhanizadeh, S.; Golabi, M.; Hesami, S.; Rjoub, H. The potential use of drones for tourism in crises: A facility location analysis perspective. *J. Risk Financ. Manag.* **2020**, *13*, 246. [CrossRef]
182. Ashtari, A.; Stevšić, S.; Nägeli, T.; Bazin, J.C.; Hilliges, O. Capturing subjective first-person view shots with drones for automated cinematography. *ACM Trans. Graph.* **2020**, *39*, 1–14. [CrossRef]
183. Wang, G.; Yang, Y.; Wang, S. Ocean thermal energy application technologies for unmanned underwater vehicles: A comprehensive review. *Appl. Energy* **2020**, *278*, 115752. [CrossRef]
184. Bisio, I.; Garibotto, C.; Haleem, H.; Lavagetto, F.; Sciarrone, A. A systematic review of drone based road traffic monitoring system. *IEEE Access* **2022**, *10*, 101537–101555. [CrossRef]
185. Ahmed, H.U.; Huang, Y.; Lu, P.; Bridgelall, R. Technology developments and impacts of connected and autonomous vehicles: An overview. *Smart Cities* **2022**, *5*, 382–404. [CrossRef]
186. Burd, J.T. Regulatory sandboxes for safety assurance of autonomous vehicles. *Univ. Pa. J. Law Public Aff.* **2021**, *7*, 194.
187. Mahmood, Z. Connected vehicles in the IoV: Concepts, technologies and architectures. In *Connected Vehicles in the Internet of Things: Concepts, Technologies and Frameworks for the IoV*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 3–18.

188. Jones, T. *International Commercial Drone Regulation and Drone Delivery Services*; Technical Report; RAND: Santa Monica, CA, USA, 2017.
189. Calandrillo, S.; Oh, J.; Webb, A. Deadly drones: Why faa regulations miss the mark on drone safety. *Stan. Tech. L. Rev.* **2020**, *23*, 182.
190. Konert, A.; Dunin, T. A harmonized european drone market?–new EU rules on unmanned aircraft systems. *Adv. Sci. Technol. Eng. Syst. J.* **2020**, *5*, 93–99. [CrossRef]
191. Shafik, W.; Matinkhah, S.M.; Shokoor, F. Cybersecurity in unmanned aerial vehicles: A review. *Int. J. Smart Sens. Intell. Syst.* **2023**, *16*. [CrossRef]
192. Attrey, A.; Lesher, M.; Lomax, C. *The Role of Sandboxes in Promoting Flexibility and Innovation in the Digital Age*; OECD: Paris, France, 2020.
193. Konert, A.; Kotliński, M. U-Space–Civil Liability for damages caused by Unmanned Aircraft. *Transp. Res. Procedia* **2020**, *51*, 304–312. [CrossRef]
194. De Naeyer, V.S. Implementing Cooperative Intelligent Transportation Systems: A Maturity Model for Assessing the Readiness of Cities. Available online: https://digikogu.taltech.ee/et/Download/372dcfcf-214f-406d-b1b9-f01999c927b2/Koostalitavatejanutikatetranspordissteemidera.pdf (accessed on 14 January 2024).
195. Shrestha, R.; Bajracharya, R.; Kim, S. 6G enabled unmanned aerial vehicle traffic management: A perspective. *IEEE Access* **2021**, *9*, 91119–91136. [CrossRef]
196. Gohar, A.; Nencioni, G. The role of 5G technologies in a smart city: The case for intelligent transportation system. *Sustainability* **2021**, *13*, 5188. [CrossRef]
197. Yuan, T.; Da Rocha Neto, W.; Rothenberg, C.E.; Obraczka, K.; Barakat, C.; Turletti, T. Machine learning for next-generation intelligent transportation systems: A survey. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4427. [CrossRef]
198. Chen, S.; Hu, J.; Shi, Y.; Zhao, L.; Li, W. A vision of C-V2X: Technologies, field testing, and challenges with Chinese development. *IEEE Internet Things J.* **2020**, *7*, 3872–3881. [CrossRef]
199. Rymer, N.; Moore, A.; Young, S.; Glaab, L.; Smalling, K.; Consiglio, M. Demonstration of two extended visual line of sight methods for urban UAV operations. In Proceedings of the AIAA AVIATION 2020 FORUM, Online, 15–19 June 2020; p. 2889.
200. Alkadi, R.; Shoufan, A. Unmanned aerial vehicles traffic management solution using crowd-sensing and blockchain. *IEEE Trans. Netw. Serv. Manag.* **2022**, *20*, 201–215. [CrossRef]
201. Li, X.; Gong, L.; Liu, X.; Jiang, F.; Shi, W.; Fan, L.; Gao, H.; Li, R.; Xu, J. Solving the last mile problem in logistics: A mobile edge computing and blockchain-based unmanned aerial vehicle delivery system. *Concurr. Comput. Pract. Exp.* **2022**, *34*, e6068. [CrossRef]
202. Guillermo, B.; Jan, V.; Han, V.; Irena, K. Smart building and district retrofitting for intelligent urban environments. In *Intelligent Environments*; Elsevier: Amsterdam, The Netherlands, 2023; pp. 395–420.
203. Gholamhosseinian, A.; Seitz, J. Vehicle classification in intelligent transport systems: An overview, methods and software perspective. *IEEE Open J. Intell. Transp. Syst.* **2021**, *2*, 173–194. [CrossRef]
204. Nogar, S.M. Autonomous landing of a uav on a moving ground vehicle in a gps denied environment. In Proceedings of the 2020 IEEE International Symposium on Safety, Security, and Rescue Robotics (SSRR), Abu Dhabi, United Arab Emirates, 4–6 November 2020; pp. 77–83.
205. Gonzalez, R.A.; Ferro, R.E.; Liberona, D. Government and governance in intelligent cities, smart transportation study case in Bogotá Colombia. *Ain Shams Eng. J.* **2020**, *11*, 25–34. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.