applied sciences

MDPI

Review

SDN-based VANETs, Security Attacks, Applications, and Challenges

Muhammad Arif [1], Guojun Wang [1,*], Oana Geman [2], Valentina Emilia Balas [3], Peng Tao [1], Adrian Brezulianu [4] and Jianer Chen [1]

1 School of Computer Science, Guangzhou University, Guangzhou 510006, China; arifmuhammad36@hotmail.com (M.A.); pengtao_work@163.com (P.T.); jianer@gzhu.edu.cn (J.C.)
2 Department of Health and Human Development, Stefan cel Mare University, 720229 Suceava, Romania; oana.geman@usm.ro
3 Department of Automation and Applied Informatics, Aurel Vlaicu University of Arad, 310032 Arad, Romania; balas@drbalas.ro
4 Gheorghe Asachi Technical, University from Iasi, 700050 Iasi, Romania; adi.brezulianu@greensoft.com.ro
* Correspondence: csgjwang@gmail.com

Received: 18 March 2020; Accepted: 28 April 2020; Published: 5 May 2020

Abstract: Vehicular ad-hoc networks (VANETs) are the specific sort of ad-hoc networks that are utilized in intelligent transportation systems (ITS). VANETs have become one of the most reassuring, promising, and quickest developing subsets of the mobile ad-hoc networks (MANETs). They include smart vehicles, roadside units (RSUs), and on-board units (OBUs) which correspond through inconsistent wireless network. The current research in the vehicles industry and media transmission innovations alongside the remarkable multimodal portability administrations expedited center-wise ITS, of which VANETs increase considerably more attention. The particular characteristics of the software defined networks (SDNs) use the vehicular systems by its condition of the centralized art having a complete understanding of the network. Security is an important issue in the SDN-based VANETs, as a result of the effect the threats and vulnerabilities can have on driver's conduct and personal satisfaction. This paper opens a discourse on the security attacks that future SDN-based VANETs should confront and examines how SDNs could be advantageous in building new countermeasures. SDN-based VANETs encourage us to dispose of the confinement and difficulties that are available in the traditional VANETs. It helps us to diminish the general burden on the system by dealing with the general system through a single wireless controller. While SDN-based VANETs provide us some benefits in terms of applications and services, they also have some important challenges which need to be solved. In this study we discuss and elaborate the challenges, along with the applications, and the future directions of SDN-based VANETs. At the end we provide the conclusion of the whole study.

Keywords: vehicles; software defined networks; security; privacy; applications; challenges; vehicular ad-hoc networks

1. Introduction

Since the presentation of the Internet in 1969, from the Advanced Research Projects Agency Network (ARPANET) military errand, the advancement of framework has been upheld and predicted, with a goal of around 5 billion connections by the end of 2019 [1,2]. It is definitely not a top secret for specialists who organize the framework system in dissimilar associations and affiliations. Once created, it is important to keep up perfect working and check for issues such as the development of contraptions and interoperability, among others [3]. Instead, there has been a necessity to ensure the system wherever key and crucial material is taken care of for associations and affiliations, principally in game

plans with sophisticated datasets of clients and suppliers. In this sense, perfect models have been developed, for instance, Cloud Computing, that have empowered these data to be taken care of and set away remotely by the highest availability, protection, and validity, and abusing the advantages of the framework [1].

The idea of an software defined network (SDN) depends on the model made out of the three layers—application, control, and information plane—that ideally repeat and robotize the system framework [3]. Engineering expects to integrate the control and information planes in organized gadgets, for example, in routers and switches [1]. The control plane is answerable for choices in regard to the traffic which associates through any gadget in system, although the information plane performs the assignments of shipping information parcels. The design of programming characterized systems is reasonably made out of the three layers: foundation, control, and application [1]. Additionally, the application program interface (API) that conveys these three planes is the northbound API and the southbound API, which are contingent upon the correspondence discourse regarding the SDN-based controller. Inside the SDN condition, the advancement of the open source APIs is advanced, which provides greater adaptability and dynamism [3].

As a result, a setting for this system worldview will be given, centered on current mechanical patterns and their point of view. The applications, modes, controllers, and architectures of SDNs can be seen in Figure 1.

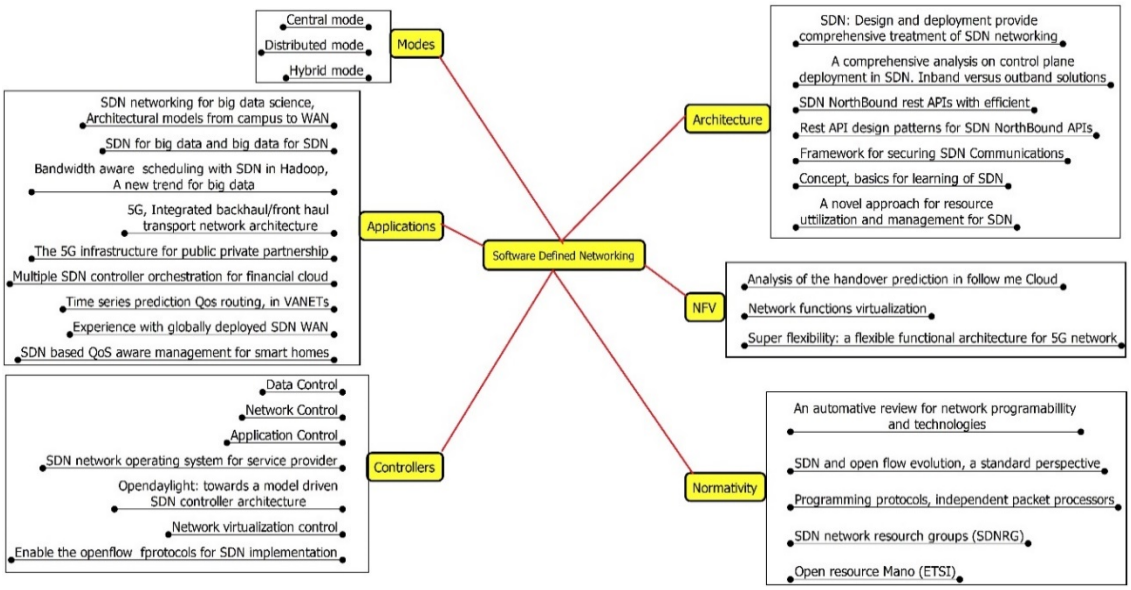

Figure 1. Architecture, modes, controllers, and applications of software defined networking (SDN).

1.1. Data Plane

The data plane, also known as the foundation plane, is comprised of the system gadgets, among which include routers, switches, and passages liable for moving all the data of the clients that circulate through the network. These system gadgets do not extend, and already have a defined and static usefulness; yet they are described by a lot of guidelines provided by the control layer. In this manner, similar equipment could function as a switch or as a firewall, contingent upon what the system supervisor has characterized [1,4].

1.2. Control Plane

The control plane is liable for concentrating the control of the whole progression of data that circles by the data or the foundation layer. This comprises the approaches of sending or redirecting information, stream boards, and has the general point of view of the whole system facilitated in a

SDN-based controller [4]. As shown in Figure 2, there is the API southbound interface (SBI), for example, the OpenFlow convention, which permits the controller like open sunlight, or the VMware NSX (e.g., network virtualization and security platform) to forward the arrangement of approaches and setups to every one of the gadgets that build up the information plane. The APIs are of vital significance for exacting partition of the elements of information and the control planes [1]. There are additionally northbound interface (NBI) APIs, for example, restful API [5] or the software defined mobile networks (SDMN) API [1], that characterize a crucial spot in the foundation to intervene among the global applications approaches and system strategies, permitting application planes to correspond with the control plane [1].

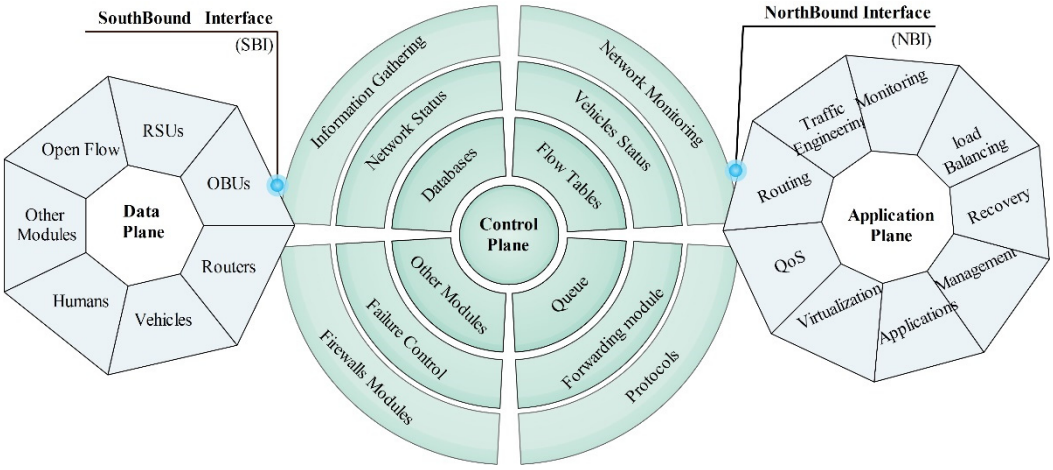

Figure 2. The three planes of the software defined network (SDN) architecture (data plane, control plane, and the application plane).

1.3. Application Plane

The final plane or layer is the application layer. This is the place of the advancement of different application programs that permit a correspondence and cooperation with all the other designs. It is completed quickly, altogether with the help of NBI APIs that accomplish the correspondence of this plane against other planes. This piece of design can get a progressively unique point of view of the system, meaningful from the amount and dispersion of the associated gadgets to assortment of measurements of the system conduct, and which are the places where choices about its organization are made [5].

Consequently, it is important that particular advancement of these significant level programs and applications are made and executed by networks that advance improvement by the open source stages, adding to adjustment [6], and including highlights, such as security, encryption, and adaptability. In such a manner, the improvement of uses with the Representational State Transfer (REST5) engineering has made progress in the SDN, giving advantageous administration-arranged applications that pay little respect to the programming languages and the executables in the different stages. The applications design is bolstered by novel dialects, for example, JSON6, JavaScript, and Python [1], which empower the administration and organization of the systems to be accepted on adaptable stages.

In the course of recent periods, the promising thought of the vehicular ad-hoc networks (VANETs) has been completely examined and thoroughly looked into by analysts in both the scholarly world and industry [7]. However, the rising and promising standards of distributed computing, Fog, or potentially Edge computing, SDN and the system capacities virtualization have totally changed the remote systems administration industry, however they have additionally pushed extensive imaginative headways for the transportation division. This is combined by other huge mechanical approaches appropriate to the development of associated and autonomous vehicles and unavoidable use of various new tangible gadgets introduced on-board vehicles that encourage in the different scope of agreeable vehicular

security applications and programs (i.e., send the crash cautions, crisis vehicles help, (powerless) walker impact relief, overwhelm crossing point cautions and dangerous area cautions). These security applications are basic in nature, yet necessitate a low-dormancy foundation with the most extreme middle-of-the-road postponement running between 10 ms and 50 ms [8].

Moreover, advanced associated vehicles are outfitted with 120 sensors and this number is foreseen to increment up to 250 towards the end of 2020 [9]. These sensors produce the bulk of useful information, yet in addition they assume a fundamental job in making and sharing knowledge for vehicular correspondence. Moreover, according to a gauge of Intel [4], the averagely-determined associated vehicles (i.e., individual vehicles utilized for everyday schedule purposes and not for any business tasks) sooner rather than later would produce around 40 TB of information and this number is growing speedily [9]. The SDN architecture, modes, technologies, and opportunities are shown in Figure 3.

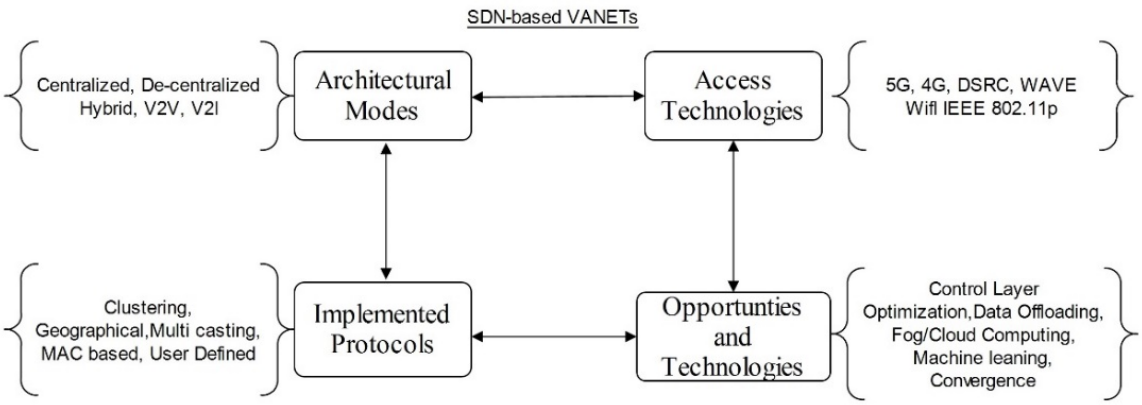

Figure 3. SDN architecture modes, technologies, and opportunities.

The rising and promising global view of SDNs show a potential answer for these vehicular system administration challenges [10]. SDNs have been created, and in this way conveyed, for wired systems. However, recently there has been increased enthusiasm towards sending SDNs for both remote and specially appointed areas. This has increased the enthusiasm of the scholarly network to investigate the probability of planning SDN-based VANETs which not only empower security and highest data transfer capacity correspondence administrations, but also provide low inactivity to the well-being of basic VANET applications and programs [11]. The SDN disjoints the control layer from the information layer, and the general administration and coordination of the system assets are completed through a programmable controller. This, accordingly, encourages empowering a seller-free control of the whole system for both system bearers and undertakings, thus extensively streamlining the system plan and tasks and establishing frameworks for an exceptionally adaptable and programmable system administration foundation. Subsequently, by providing a programmable SDN-based controller, it is simpler to arrange unique system gadgets and convey a wide cluster of new applications immediately [12].

Nevertheless, in spite of a few favorable circumstances that SDNs bring to a systems administration framework, it is additionally defenseless against various security attacks since noxious elements may dispatch the attacks on either the information plane by means of focusing on the system components from inside the system itself and by means of the SBI API, by legitimately attacking the control layer as it goes about as they brought together purpose of knowledge for the whole fundamental system or on the applications plane by focusing on assured specific applications, and programs by the NBI API [13]. However, guaranteeing security in an SDN-based VANET is out of the scope of this article. Although various models have been as of late proposed to ensure an improved system asset, a large portion of the executives in VANETs have not represented the one of a kind VANETs related characteristics and qualities in their structures (i.e., visit deviations in organize topologies inferable from the exceptionally

unique conduct of vehicles in the information plane, very enormous and disseminated organization, stringent postponed imperatives, the requirement for effective and smooth handovers, and so forth) [14]. In addition, some of these designs essentially depend on gathering unified insight in an SDN-based controller, which from one perspective, gives the global perspective on the whole hidden system, yet then again, may turn into a solitary purpose of system disappointment if there should be an occurrence of any unexpected occasion. Therefore, a re-structure of the current vehicular systems administration design is extremely fundamental [15].

1.4. The relationship of SDN and Network Function Virtualization (NFV)

In essence, the software defined network (SDN) is a method to build data network devices and software that separate and abstract the elements of these systems. It does so by decoupling the control plane and the data plane from each other, so that the control plane is centrally located, and the forwarding components remain distributed. The control plane interacts with the north and south. In the north direction, the control plane uses an API to provide high-level applications and programs with a general abstraction view of the network. In the south direction, the control plane uses the device-level APIs of the physical network devices distributed in the network to program the forwarding behavior of the data plane [16].

Therefore, NFV is not based on SDN or SDN concepts. Using the existing network paradigms and business processes, it is completely possible to implement virtualized network functions (VNFs) as independent entities. However, the use of SDN concepts to implement and manage NFV infrastructure has inherent benefits, especially when studying VNF management and orchestration; thus, it is necessary to define a multi-vendor platform that integrates SDN and NFV into a coordinated ecosystem [17]. The NFV infrastructure requires a central orchestration and management system that receives requests from operators related to VNFs and translates them into the appropriate processing, storage, and network configurations required to put VNFs into operation. Once in operation, the capacity and utilization of VNFs should be controlled and adjusted if necessary. All these functions can be achieved using SDN concepts, and NFV can be considered as one of the main cases of SDN use in a service provider environment. It is also clear that many cases of SDN use can include concepts introduced in the NFV plan. Examples include when a centralized controller is controlling a distributed forwarding function, which can actually be virtualized on existing processing or routing equipment [18].

2. Evolution of SDN Control Architecture for VANETs

The SDN-based VANET systems support all three SDN unified and appropriated control models. The three models have an explicit foundation and prerequisites. The explanations of these three models are given below.

2.1. Centralized Controller Model

This mode is comprised of a solitary controller that is utilized to deal with the whole system. This indicates that the SDN is boosted by OpenFlow rules convention, which is utilized and incorporated by the controllers to control and deal with the whole system [13]. Thus, on the grounds that a solitary controller is utilized it must have a global visualization of the whole system. The controllers correspond through the gadget that is straightforwardly associated with the system to distinguish the deficiency and the attacks that happen on the whole system. These legitimately associated gadgets forward data to the controller. By utilizing the single controller, it is anything but difficult to deal with the usefulness of the whole system. Notwithstanding, a solitary controller has a few impediments. It needs to refresh the entire system more often than the customary system does on the grounds that when the stream changes, the stream table must be refreshed so as to look after productivity. This procedure delivers a high over-burden in light of the fact that the makers should be completed by the controller, and this maker builds the handling cost of the controller. A model is grouping streams with various needs into numerous classifications. Expanding the usefulness in a solitary hub requires higher measures of

intensity in handling, information stockpiling limit, and throughput to convey the information [13]. Figure 4A represents the centralized model.

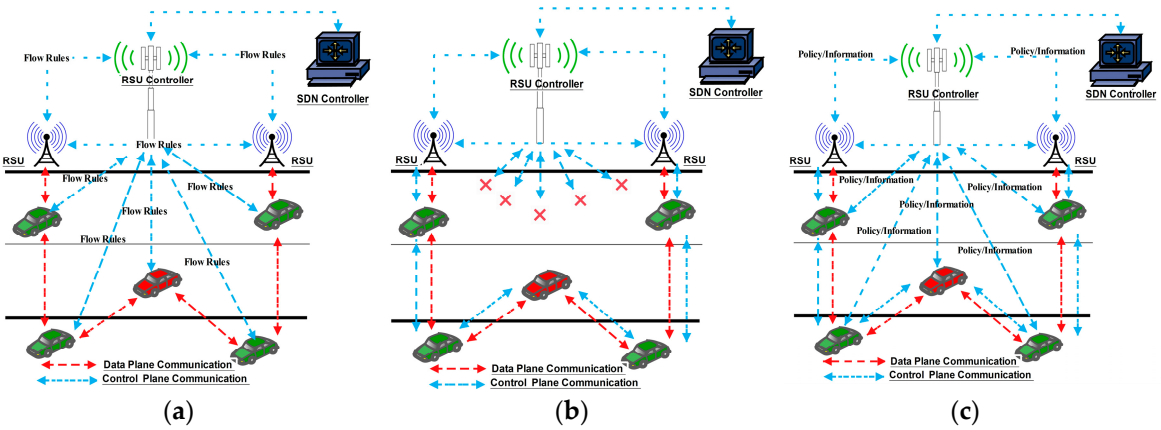

Figure 4. (**a**) Centralized controller model, (**b**) distributed controller model, (**c**) hybrid controller architecture.

After some time, new rules and streams are acquainted with encouraged correspondence, yet the memory of the controller must be extended over and over [19]. The third problem in the unified system is that paying little attention to where the main pack of the new stream is presented, it is first sent to the incorporated controller for assessment. The controller decides the way for the stream and stretches out this data to every one of the gadgets for the whole system. The smash utilized through the controllers to characterize the guidelines can be over-burdened by the huge measure of essential information to be handled. In this circumstance, some disappointments in the controller may cause dissatisfaction of the whole network [11]. After some time, the SDN organized framework turns out to be progressively mind boggling due to new prerequisites of the job of traffic. They are intended to help variable correspondence with the expansion of the security, loading, adjusting, and firewalls [7]. Various administrations are intended to arrange through the control plane to accomplish their objective. In utilizing these conflicting steering topologies, it is hard for controllers to accomplish ideal execution [20].

2.2. Distributed Controller Model

The conveyed SDN-based model was acquainted with the disappointments and confinements of the single SDN-based controller [13]. The disseminated SDN-based model is utilized to adjust the heap among various controllers and multi-center frameworks in the controllers. The model is utilized to deal with the whole system adequately. The disperse controllers are utilized to share the lot of information, in this way guaranteeing the reliability of correspondence [19]. The examination of a circulated SDN-based model by the focal controls model shows that the appropriated frameworks are progressively more responsive, quicker, and increasingly productive regarding enormous worldwide system zones. Nonetheless, in spite of the advantages of the dispersed SDN model, numerous difficulties must be defeated before the appropriated controller can be executed [21]. The mapping of the control plane and sending plane must be designed consequently rather than physically. The controller must have a wide perspective on the whole system to help the framework. Much of the time, it is hard for each controller to have wider access to the systems. These controllers utilize nearby calculations to create coordination between various controllers. Hence, a calculation or technique is essential to coordinate the whole system and give a global image of it. Figure 4B represents the distributed controller model.

2.3. Hybrid Controller Architecture

The hybrid control design is another way to deal with tending to the constraints of central and conveyed SDN controller frameworks. This hybrid framework was intended to help with the structures

of both focal and appropriated frameworks [22]. The sensible framework utilized in the half and half model is equivalent to that utilized in the focal controller. In any case, it utilizes the information correspondence design that is utilized in the appropriated controller. The half and half SDN model supports the straightforward control of the executives example of a solitary controller, and it has the adaptability of disseminated models [23]. The crossbreed SDN-based model enables the controllers to utilize assets effectively to build the exhibition of the system. The crossbreed model additionally enables approaches to elevate the security of the whole system. Moreover, it permits the refreshing of the framework without the need to change the present system settings [22]. Figure 4C represents the hybrid controller model.

3. SDN-based Intelligent Transportation System

The future capability of the Internet as a global sensation has prompted an expanding number of gadgets that are web-engaging [24]. The integration of intelligent transportation systems (ITS) with SDNs and other technologies is represented in Figure 5. In addition, traffic in the transportation system by the Internet has become simpler as the quantity of advances in the Internet of Things (IoT) is utilized for the traffic which executives (i.e., smart ITS) imagine to altogether enhance the traffic and environment on the roads. This is essential to screen the traffic through utilizing various methods (i.e., check the speed limit, contamination validations, and crisis reaction if there should be an occurrence of street mishaps). Customarily, to illuminate such issues, closed circuit television (CCTV) cameras are utilized. However, such programs and applications are not palatable in situations where few vehicles are proceeding on the roads or highways [25]. To adapt to imitations, IoT innovation thought of various strategies in rush hour gridlock the board; for instance, ITS is imagined to fundamentally enhance the transportation and security of highways. The idea of the ITS is that all vehicles proceeding on the highways are in consistent correspondence with one another, through vehicle to vehicle (V2V) or vehicle to infrastructure (V2I) correspondence [26]. The arrangement of different advancements expected to achieve this undertaking has been moderate and pricey [27]. It includes the establishment of numerous bits of huge gear both on the highways like roadside units (RSUs) and onboard units (OBUs) [28]. This recommends a total immersion of these units essential to empower a completely useful ITS [29]. As of late, a few research networks have concentrated on discovering snappy organization and lower cost elective strategies for ITS. As of now there exist numerous conventions and models that guarantee the arrangement of ITS, since it is steady over all states and vehicles. As of late, different parts of ITS have been inquired about. ITS can give a few administrations, yet from the nature of administration, quality of service (QoS) perspective, the necessities of client fulfillment are not acceptable [30].

Moreover, the capacity of dealing with a huge solicitation is irreplaceable. Thus, as of late, a rising term, called SDN, has considered the systems administration worldview among wired and remote gadgets from a programming point of view. SDN is a rising system worldview that isolates the control rationale from the system gadget (switch or sensor hub), leaving the gadget with just information sending usefulness [31]. SDN can improve adaptability and proficiency as well as give a stage to organize the board. It additionally empowers an adaptable system of executives, which is a basic component of the Internet of Things (IoT). To adapt to these restrictions and difficulties, programming characterized organizing is the precursor, shaping the foundation of system applications. In this way, SDN shows up as a distinct advantage innovation that has upset the whole systems administration component. It decouples the system control layer from the data plane to the control and deals with the system gadgets and administrations by utilizing the deliberation of lowest level usefulness [25]. It offers help for the dynamic, versatile registering and capacity requirements of the current difficult computerized arranges and permits versatile control and activities of systems cost-adequately. SDN conquers the impediment of customary systems and gives a smart stage to determine and organize security issues. As of now, two planes of traditional systems administration, control and information plane, have been successfully isolated [6]. Due to this detachment, the information plane is left with a sending system, although the control layer is moved to the controllers. This results in a unified

application hurrying to convey organizing strategies, board instruments, safety efforts, and so on, and each method arranges virtualization. It likewise gives information streamlining and greater adaptability, exactness, and consistency in the design when contrasted with the manual arrangement of systems administration gadgets for a customary system [32].

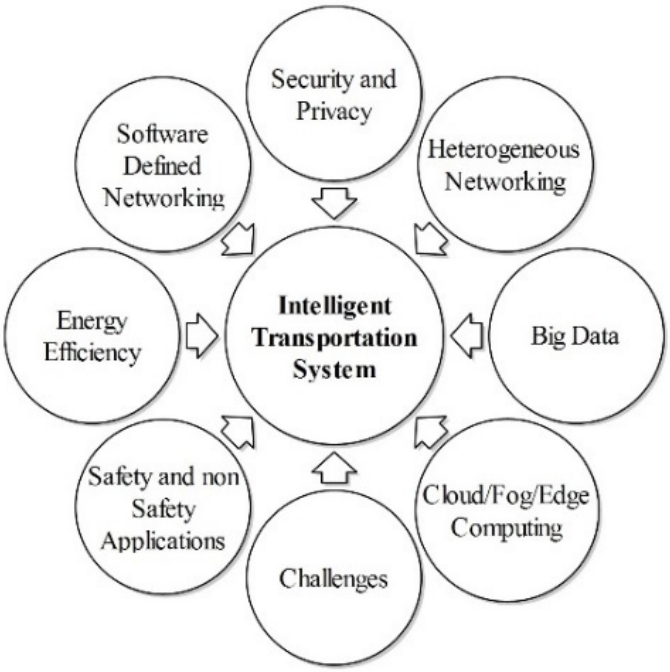

Figure 5. Integration of intelligent transportation system with SDNs and the other technologies.

In addition, programming characterized organizational difficulties are still being looked at (i.e., to adapt to the highest versatility of vehicles shows additional difficulties while utilizing the SDN idea). There are other significant difficulties is the network among the SDN controllers and the vehicles [33]. Some of the time, it is likewise conceivable that the SDN controller is not reachable. The greater part of the exploration directed in earlier research did exclude such problems as they pursued the old style of the vehicular systems, for example, the specially ad-hoc on demand distance vector (AODV) [8] and global positioning system receiver (GPSR) [34]. Through an important association among SDN and the Internet of Vehicles (IoV), the idea of programming characterized SDN-IoV is developing. SDN-IoV gives an adaptable and proficient association, ensures administration QoS, and helps with different simultaneous clients [35]. SDN-IoV generally controls and manages vehicular correspondence in a unified way by amassing the system state data and choosing as indicated by the environment. Furthermore, the association among the SDN-based controllers and the vehicle requires a legitimate association that keeps up its network all through the correspondence. In such manner, a portion of past investigations have misused the long term evolution (LTE), 4G advanced systems [35]. However, these innovations do not bolster a high and effective transfer speed. The SDN-based ITS is shown in Figure 6.

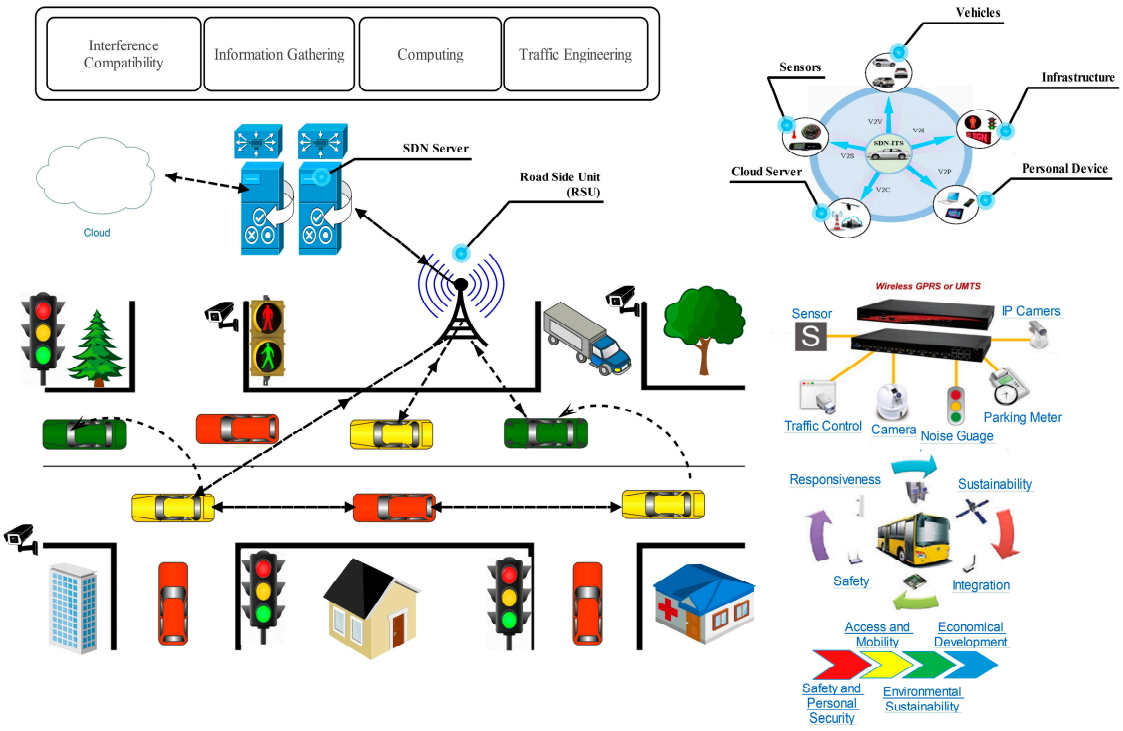

Figure 6. SDN-based intelligent transportation system.

4. SDN-based VANETs

Previously we have seen a few recommendations on the recently inferred territory vehicular correspondence systems, where a large portion of the investigations have concentrated on programming characterized organizing [8]. In the previous decade, a recently determined idea of region VANETs has pulled in a lot of research consideration. The driving inspiration among the scientists involves an examination for correspondence among vehicles, consistent web network for the improvement of the roads' well-being, vital alarms, and accessibility to solace and stimulation [36]. One of the largest VANET applications and programs are related to the ITS, which is developed to reduce mishaps and save lives [37]. As indicated by the idea of ITS, all vehicles can communicate with each other in terms of V2V and V2I [22,38,39]. All types of communications (V2X) are shown in Figure 7, and Figure 8 represents the high-level architecture of the traditional VANETs.

Modeling and Implementations of SDNs for Vehicular Networks

The investigation of current deals with SDN-based VANETs is dependent on four components [40]. To begin with, we recognize analysts' focus on disadvantages. The subsequent component is the characterization of the current SDN put together with VANETs in respect to those which have tended to downside. The third is the framework investigation which permits recognizing portions of the SDN-based VANETs that are significant to the issue. At long last, the model of the proposed arrangement, thus, gives the execution of the model identified with the SDN-based VANETs in thinking about the yields of its framework examination [41]. Figure 9 represents the abstract level architecture of the SDN-based VANETs.

Displaying and reproduction plan of current work on SDN-based VANETs was developed to think about the challenges of a few issues that begin from the multifaceted nature of vehicular network applications and programs under study in the SDN-based VANETs. In this manner, the approaches of programming characterized SDN-based VANETs to contribute as a system innovation to give an answer for current VANETs applications. What is more, SDN-based VANETs are considered as a framework since it is a piece of VANETs innovation that will impact the structure of future vehicular

system designs [42]. For the most part, a VANET manages its targets by filling the partition between heterogeneity brought about by correspondence interfaces prepared in vehicle- or foundation-based correspondence. For example, let us acknowledge the way that highest versatility of the vehicles causes dynamic topology changes which create bundles of misfortunes in the system; in this way directing conventions in portable elements to adequately deal with the shortest lifetime connections are essential [43]. To this, Maio et al. [12] describe the SDN-based VANET issue well and the examination network proposes what should be possible to take care of the issue. The framework examination which speaks to the substances of the framework that are applicable to the issue unveils a hint of communication overhead among the vehicles (information planes elements) and the SDN controllers. To this end, analysts ought to rapidly translate that communication overhead among the vehicles (information plane) and the SDN controller is the main driver; in this way, the execution of the answer for another issue identified with steering conventions that can break interface quality would begin on communication overhead on the SDN controller. Therefore, the method developed by Todorova et al. [44] includes another steering convention that improves the bundle conveyance proportion by choosing stable routes with the most minimal dormancy to control the communication overhead on the SDN-based controller.

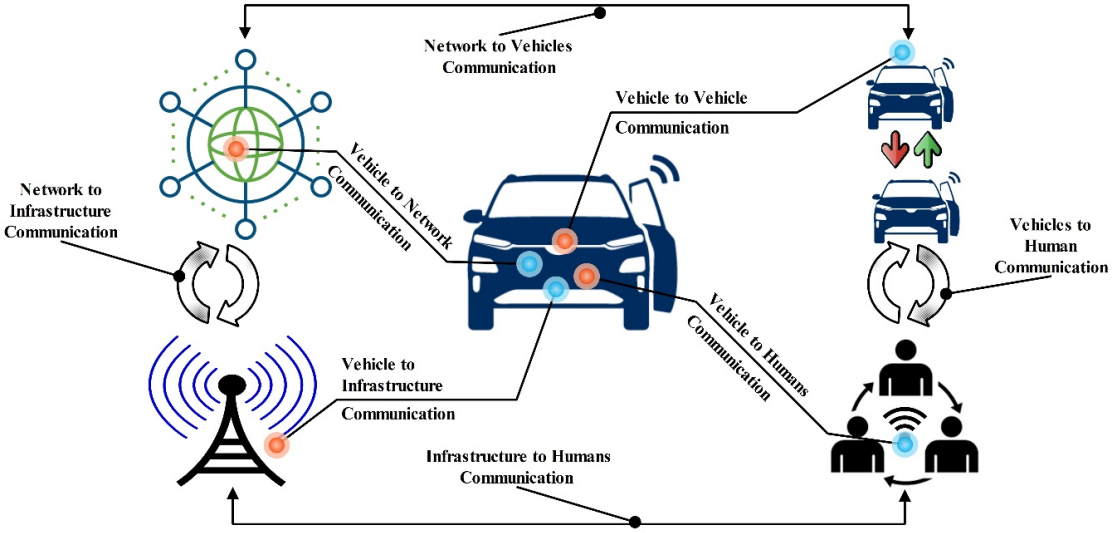

Figure 7. Vehicles to Every Things (V2X) communication including (Vehicles to Vehicles (V2V), Vehicles to Infrastructures (V2I), Vehicles to Humans (V2H), Infrastructures to Humans (I2H), Vehicles to Networks (V2N), Infrastructures to Infrastructures (I2I), Networks to Vehicles (N2V)).

Changes in capacity in conventional arrangement due to the heterogeneity of remote frameworks motivated by Venkatramana et al. [45] to give a framework investigation that focused on abstracting heterogeneous remote hubs as SDN switches empowered Open Flow and planning SDN controller to oversee progressively organized assets. The yield of the framework investigation prompted by Thun et al. [46] to propose an answer model that incorporates a versatile convention for heterogeneous multi-hope steering, a topology that empowers SDN executives overhead by means of the status of the SDN routers which lastly gives usage of the instances of SDN-based VANETs empowered by V2I, V2V, and vehicle to human (V2H). To enhance the presentation in correspondence by moderating the availability misfortune among the vehicles and focal SDN-based controller [39], Thun et al. recommended a framework investigation dependent on choosing neighborhood SDN-based controller areas by the grouping of ideas. They proposed a various leveled SDN-based VANET as the usage model to diminish availability misfortune at the SDN-based controller; in this way they improved the vigor of systems administration of information plane substances. ITS situations in the upcoming VANETs need QoS and proficient use of system assets for empowering self-governing driving. Borcoci et al. [47] tended to the test of proficient asset use. In their study [47], the framework on the issue is related to

utilizing the fog/edge figuring innovation, therefore the SDN-based cloud organization is assessed to develop locally aware administrations with less correspondence inactivity.

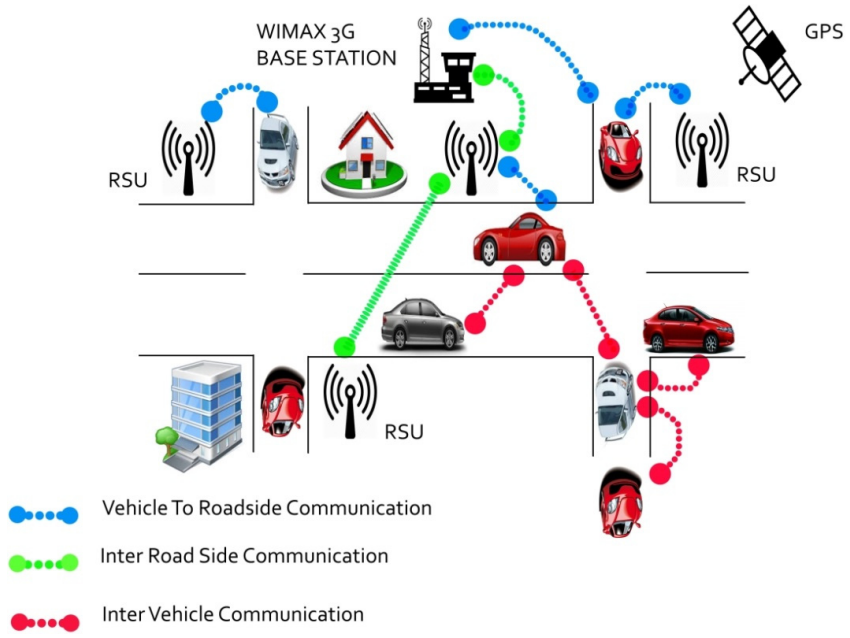

Figure 8. Architecture of the vehicular ad-hoc networks.

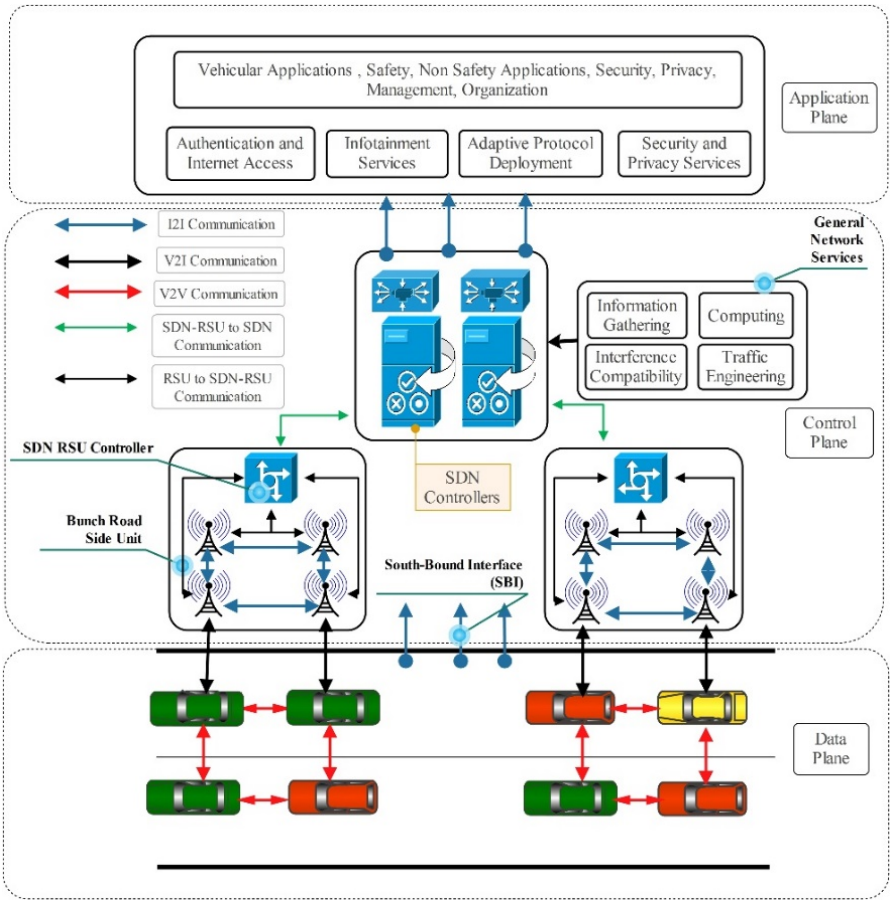

Figure 9. SDN-based vehicular ad-hoc networks architecture.

To this end, the framework examination focuses on organization of SDN to help hybrid mode and the design of the control plane (SDN-based controller) in appropriated mode with the base station (BS) and RSUs. As the yields of SDN-based fog imagining, Gao et al. [48] elaborated a method that consolidates edge/fog processing administrations for permitting various correspondence access for V2I, V2V, and V2H. Other studies [49,50] provide a framework examination that focuses of topology organization of the SDN-based controller and the likelihood to display correspondence hubs as a SDN-based switch utilizing the open-source reproduction device known as the Mininet-WiFi. The developed method suggests the proficient usage of the system asset subsequent to demonstrating the vehicles as a hub utilizing Mininet-WiFi. Making versatile edge processing stride further, Kazmi et al. [42] explored the plausibility of sending VANET applications and programs with lowest inertness and highest unwavering quality correspondence delay in programming characterized portable edge imagining. The framework investigation given by Truong et al. [13] considers an over the fog vehicular system design which in turn gives a demonstrating arrangement on the best way to control the correspondence dormancy through radio access directing at the BS. The progression of 5G in the car field brings the reconciliation of the VANETS and the 5G innovation to develop 5G programming characterized VANETs with the SDN innovation as an essential key empowering influence. Peng et al. [51] researched the test of correspondence idleness and expense on numerous center systems for independent driving vehicles.

Another study [52] gives an efficient investigation dependent on the control of inactivity at a VANET's position, the cell net-specialist SDN-based VANETs, and cell position. The yields of the framework examination brief the authors [52] to show their answer for diminishing correspondence inertness by enhancing southbound correspondence by means of both a refunding system and the utilization of game balance related with the two-arrange pioneer devotee game so as to choose the best steering ways among vehicles and the controller. In a study by Chekired et al. [53], the authors examine the framework dependent on communicating V2V beaconing communication with the goal that nearby information on environment hubs and their topologies is accessible at SDN-based controllers. After framework examination, the developed method gives a model that incorporates the mix of the SDN-based controllers, Evolved Node B (eNodeB or eNB) foundations, RSU, and 5G to plan an SDN-based 5G idea. The full change of VANETs into SDN-based VANETs necessitates showing SDN-based VANET arrangements not only founded on framework models of SDN put together VANETs but also based on numerical examination. Since the SDN-based VANETs coordinate the utilization of the SDN idea with VANETs, a numerically based method is the regular displaying language to separate intricacy issues and make VANETs and SDN-based VANETs challenges tractable. A numerical based hypothesis applied to SDN-based VANETs ought to bring further upgrades and varieties for permitting SDN to completely improve VANETs, therefore limiting idleness and cost, and using security message conveyance to utilize heterogeneous correspondence interfaces [54].

In the coming section we discuss the security threats and possible attacks in the SDN-based VANETs. Although SDNs provide security protection, there are still some loopholes available where the attacker can attack the SDN-based VANETs. A possible SDN security taxonomy is given in Figure 10.

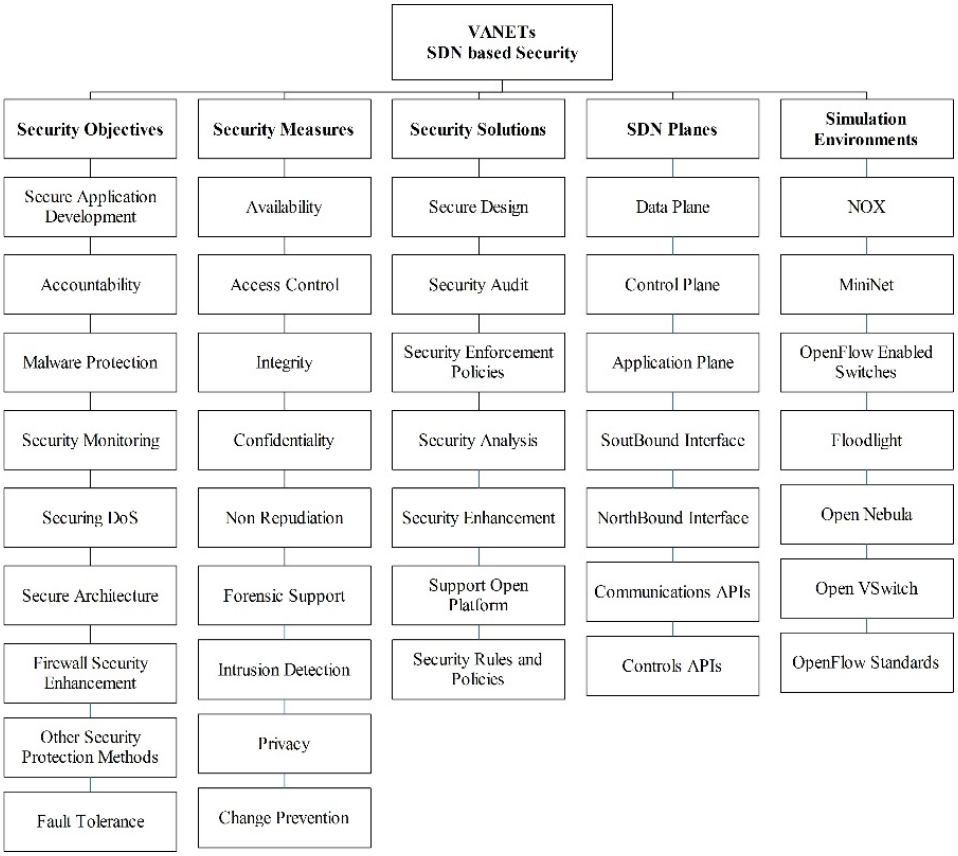

Figure 10. SDN security taxonomy.

5. SDN-based VANETs Security Challenges

Security remains a significant test, as the spread of falsehood from unapproved elements can prompt genuine mishaps. The key purposes of carefulness from a security angle are discussed below [55]. To begin, the SDN controller remains the focal basic leadership point, and ought to be firmly ensured. A barrier top to bottom methodology is prescribed, likewise to verify regular SDN frameworks [12]. Second, firmly coupled SDN layers encourage the spread of dangers between layers. APIs between layers should in this manner be solidified and institutionalized. Third, vehicle versatility and receptiveness in the lower information plane enhance SDN dangers to the control and application layers [56]. Hence, the two layers of the information plane ought to be verified, with the requirement for ongoing confirmation. A portion of these difficulties may likewise affect both connected and autonomous vehicle (CAV) security and safety. As CAVs are a firmly coordinated network of networks, disappointments on a sub framework may proliferate to other sub-frameworks and make recuperation troublesome. Digital hazards on the vehicle basic leadership rationale remain basic; vulnerabilities of artificial intelligence (AI) designs (e.g., to create injection attacks) in the "cerebrum" of the self-ruling vehicle, can cause disastrous results as far as wellbeing if information trustworthiness is undermined [56,57].

The basic concern in a vehicular systems administration condition is security. Throughout the years, various security arrangements have been conceived for VANETs that principally depend on customary cryptographic plans using open key frameworks and endorsements [55]. By and by, cryptologic based arrangements are not attainable for vehicular systems since the vehicles are profoundly unique in environment and are disseminated all through the system, the accessibility of a systems administration framework cannot be ensured consistently, and customary cryptography-based arrangements are likewise helpless against insider attacks. Subsequently, trust has been as of late presented as an option for guaranteeing security in vehicular systems [55].

5.1. Security Threats

A few threats bargain sending, control, and application layers [58]. Man in-the-middle attacks between a switch and the controller are brought about by the absence of transport-layer security [59]. Such types of attacks can be moderated by reinforcing physical system security. Refusal of administration attacks could soak stream tables and cushions. Such attacks are brought about by the inclusion of receptive principles as opposed to embracing a proactive methodology. They can be averted by utilizing different controllers. Different threats may originate from disseminated multi-controllers, applications, unlawful access, or clashes of security rules or arrangements. In spite of existing arrangements, high portability requires security components that can perform continuous validation. In addition, dormancy can cause traffic jams that hinder the acknowledgment of SDN-based VANETs. This ongoing element creates trouble in fortifying security [59,60]. Possible SDN-based VANETs security threats are given in Figure 11.

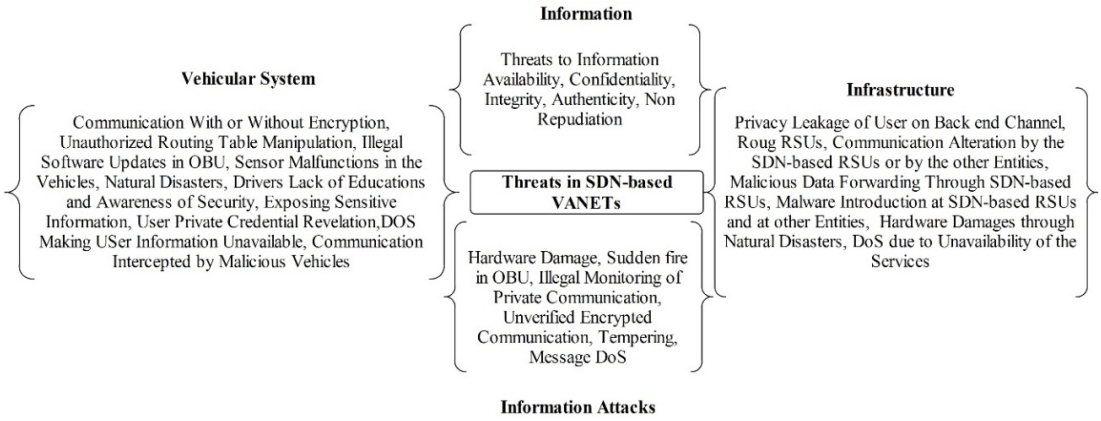

Figure 11. Threats taxonomy in SDN-based vehicular ad-hoc networks (VANETs) with respect to vehicular system, information, and infrastructure.

5.1.1. Application-Level

Poisonous applications may degenerate the SDN controller and cause contravention of approval, benefit acceleration, debilitating accessible assets, infringement of administration chains, or injecting malignant control messages in the system which can have disastrous outcomes in the system conduct (e.g., bundle dropping, re-steering, and SDN controller end). Outsider applications may present similar genuine dangers because of seller heterogeneity, absence of interoperability in security arrangements, and trust issues [61].

5.1.2. Control Plane

Traded off switches may prompt harming of the SDN controller perspective on the system or system topology or make counterfeit connections. Control messages might be controlled for parodying system assets or acquiring sensitive data. Progressively broad attacks incorporate damaging approvals in the SDN controller, trading off system disengagement, or compromising controller accessibility. The controller being the sole point for basic leadership makes the control plane especially powerless against attacks and disappointments. Its information on the system may similarly be utilized to dispatch new attacks. Interoperability issues between various controllers may likewise be a source of vulnerabilities [62].

5.1.3. Communication APIs

Significant dangers are instability of APIs and absence of institutionalization. The southbound API is commonly presented to man-in-the-center, listening stealthily, or accessibility attacks. SDN-based VANETs need institutionalized and tweaked OpenFlow APIs and northbound APIs. NBI/SBI

APIs between controllers are additionally not institutionalized [63] in the upper information plane. Vindictive programmable switches can publicize counterfeit system topologies or upset the lower information plane. Dangers originate from vulnerabilities of the numerous, heterogeneous remote correspondence conventions, and from programming characterized radio, as new applications and highlights might be downloaded through remote connections with reconfiguration abilities, potentially causing honesty infringement in various programming layers [64]. Threats additionally incorporate gadget cloning (Sybil attacks) empowering unapproved access from another gadget (i.e., another vehicle). Heterogeneity of gadget and systems is a significant source of weakness and disappointments. Factors, for example, portability, dynamic topology, and low-dormancy infringement (e.g., for emergency administrations) may likewise complex the system security checking or lead to street mishaps such as traffic (re-steering, seizing, denial of service (DoS)), or issues with the controller. Dangers likewise incorporate depleting system assets, or performing side-channel attacks to remove delicate data [65].

5.2. Possible Security Attacks on SDN-based VANETs

The main attackers are categorized in three types:

- Internal and the external attackers;
- Rational or malicious attackers;
- Passive or active attackers.

Internal attackers are verified individuals from a system, while untouchable aggressors. They are objective adversaries that attack the framework for individual advantage. Vindictive aggressors expect to annihilate the system without the objective of any close to home advantage. Dynamic assailants produce a bogus sign to make a bunch of information at any hub, though uninvolved aggressors just sense the nearness of the system. At the point when the correspondence framework is autonomous of the SDN controller, numerous difficulties must be considered in planning the framework [66].

5.3. Attacks on the Resource Consumption of the Control Plane

The greater part of the SDN-based VANET models proposed in the literature [40,56,67–70] have been planned without security as a top priority. Specifically, they are helpless against control plane asset utilization which is a significant shortcoming in the SDN. The attack is activated when there are numerous solicitations to the control layer from the information layer. In SDN-based VANETs, the control layer is formed by various RSU-SDN controllers that uphold stream rules, and afterward control the system productively. In any case, this control mode can cause major issues specifically because of numerous solicitations forwarded to the control layer. In SDN-based VANETs, like models, the RSU-SDN controller [40] bolsters less solicitations than expected. For example, in certain circumstances, arranged bundles in a few RSUs should hold up until vehicles erase old stream rules. At long last, the effect of the attack, which devours assets of the control layer by the quantity of stream, is taken care of, as is the information plane by the quantity of stream rule passages.

Potential assistance to the control layer asset utilization in SDN-based VANET structures could be an appropriation of present arrangements in the SDN [71–74]. Wang et al. [71] developed a method to retain both the control and information layer in any event when there is an information to control plane immersion attack. Specifically, they embraced the information movement idea. Likewise, they utilized the information plane store idea so as to diminish counterfeit bundles by recognizing them from ordinary ones. In a normal SDN-based VANET design, the two modules are included in the controller level. In another study [73], Ambrosin et al.developed line switch, an answer dependent on two ideas identified with likelihood and boycotting. The arrangement gives both strength against SYN (SYN is a short form of synchronize) flooding immersion attacks and security from support immersion. In a study by Shang et al. [74], flood defender depends on three procedures, namely table less designing, bundle separating, and stream rule the board. The principle objective of this arrangement is to lessen the data

transmission sticking and spare the memory space of switches. Nonetheless, receiving these arrangements with no alteration probably will not be useful for the SDN-based VANETs because of the qualities (highest portability, dynamic system topologies, and asset requirements) of SDN-based VANET information plane components that are altogether different from the information plane components of SDN-based VANETs.

5.4. Poisoning Attack on the Network Topology

The topologies data are generally identified with upper layer programs and applications, for example, bundle steering, organization virtualization, and streamlining and versatility [75]. At the point when a system topology harming attack happens, this will affect risky circumstances since all the reliant administrations and applications will be influenced. For example, the information directing could be influenced and this will bring about a man-in-the-middle attack (MiMA) or the black hole attack. Another situation shows the effect of an assailant prevailing to capture the area of a system server so as to phish its supporters. In a brilliant stopping application utilizing the SDN-based VANETs model [36], the aggressor can capture the area of a controller to phish its administration supporters. In addition, an aggressor can even make dark gap courses by injecting bogus connections in the topology. Models in other studies [40,67,68,76] are defenseless against the system topologies harming. Two well-known arrangements, Topo-Guard [75] and SPHINX [77], identify these topology harming attacks by the means of bundle checking. Topo-Guard distinguishes bogus systems using social profiling. Specifically, creators of Topo-Guard developed a topology update organizer module so as to screen system topologies and approve topology refreshes. In SPHINX, the creators proposed an abnormality discovery method dependent on confirming the irregularities in organized states. Hong et al. [75] developed an augmentation to Topo-Guard referred to as Topo-Guard+. The arrangement screens the trademark control layer communication examples, and afterward shields alongside out-of-band ports amnesia attacks.

5.5. Denial of Service Attacks (DoS)

This is the most conspicuous attack. The adversaries keep a particular hub from getting to administrations. The DoS attacks [56] are the most renowned and hazardous in the vehicular system, where the assailants send enormous solicitations to the framework so as to close down the system and stop correspondence among vehicles and among vehicles and RSUs. The objective of DoS is to quit sending or accepting data to vehicles about the system, for example, street status. As SDN-based VANETs manage content names rather than Internet Protocol (IP) addresses, DoS attacks depend on the utilization of names [11] and may target customers, makers, or middle-of-the-road hubs. From the SDN-based VANET's perspective, a fundamental DoS attack could be Interest flooding, where an assailant sends a tempest of Interest requesting an alternate substance that may not be accessible in the reserve store.

Figure 12 describes a straightforward DoS attack; vehicles, RSUs, and other system foundation components are associated with this situation. However, because of the Interest collection, middle-of-the-road hubs may have increasing opportunity to be focused or contrasted with the substance supplier, particularly while mentioning a phony substance (i.e., content with a substantial name prefix and invalid addition). The aftereffect is Interest dropping at the supplier level and pending interest table passages after lifetime termination at the middle-of-the-road hubs level. In any case, mentioning a unique substance that ought to be created by the first substance supplier after getting the Interest (e.g., requesting a new patient report) may cause DoS at the supplier level because of the way that the dynamic substance is not well known and may not be collected by middle hubs.

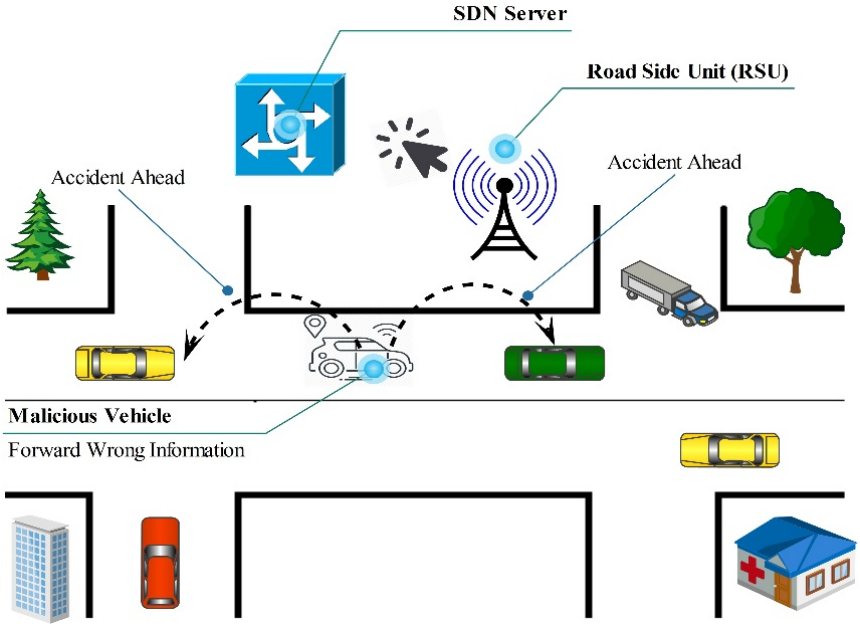

Figure 12. Denial of Service (DoS) attack in SDN-based VANETs.

A pernicious vehicle sends a tempest of various Interests requesting diverse substance names, as an RSU does not have the substance, and it advances the solicitation and makes another request. In light of the immense number of malignant interests, an authentic vehicle cannot send more demands and may not profit from the store abilities of the RSU or on occasion send its solicitations to different hubs. The attack is progressively serious with regards to delicate and critical correspondences that may influence an individual's life. Different countermeasure arrangements have been proposed to survive and alleviate DoS attacks, by utilizing either rate constraining systems (e.g., per face or per name-prefix) [78] or factual displaying approaches. The previous comprises of checking the face/name-prefix break rates as well as the pending interest table size, when distinguishing DoS attacks, and as far as possible the intrigue appearance rate (IAR) on the suspicious face, while the last depends on factual data about the request and interfaces to recognize the irregular traffic design. However, these arrangements need to make a broad adjustment to the ordinary request structure or inordinate stockpiling insights [78].

Distributed Denial of Service (DDoS)

SDN-based VANET structures [56] are defenseless against DDoS attacks. Since SDN-based VANET structures are divided into three primary practical layers—foundation plane (vehicles, RSUs), control plane (RSU controller), and the application plane—probable DDoS attacks could be propelled on any one of these planes. To quickly assist the DDoS, one may utilize the arrangement of Alrehan et al. [79], who developed an AI method for DDoS recognition. Specifically, the stream measurements are gathered from switches or from the vehicle sensors and afterward prepared. Although utilizing such an answer at vehicles could be dangerous because of the asset requirement nature of the sensors when contrasted and the nonexclusive SDN switch. Another arrangement, flood-protect, comprises counteracting DDoS attacks by utilizing information relocation and the information plane reserve. The information relocation method means confirmation from both the controller and switches, and the information plane reserve system stores the table less bundles and separates atypical bundles from the typical ones [80]. The DDoS attack is shown in Figure 13.

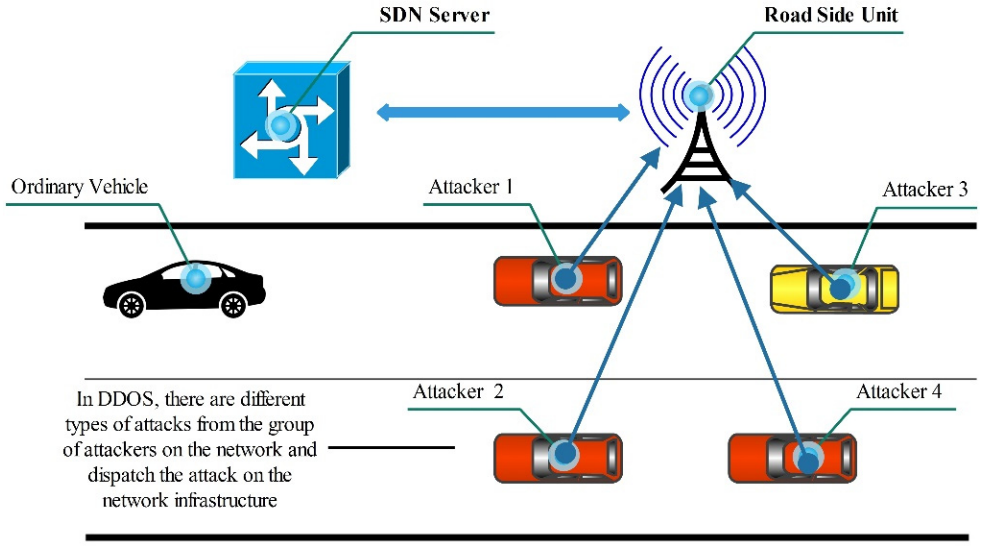

Figure 13. Distributed denial of service (DDoS) attack in SDN-based VANETs.

5.6. Rule Conflicts

The rule conflicts could have frightful attacks in the OpenFlow programs and applications. For example, a few principles can be devoted to isolate the servers which are superseded by a heap of adjusting applications and programs which may establish that the focus is on least-stacked servers [81]. Potential quick assistance could be received to settle the standard clashes in the SDN-based programs and applications. For example, the FortNOX [82] recognizes classes that disregard current security strategies, and suggests approval authorizations in controllers bit. One may introduce FortNOX in the RSU controllers in SDN-based VANET models.

5.7. Privacy Attack

In SDN-based models, different client connection data must be secured, for example, the tag, location, and driver's name, and the specialists ought to have the option to uncover their characters if a mishap or a question should arise [83]. Contingent protection saving components in the vehicular interchanges can be adjusted to the vehicular programming structures. Lin et al. [84], developed the well-designed group signature and identity based signature (GSIS), an answer which coordinates the gathering based marks and identity based marks, and offers security and protection saving systems between various OBUs, and among OBUs and RSUs. Zhang et la. [85], elaborated an area security protecting verification plot dependent on daze signature. The plan ensures the area obscurity to people in general. Utilizing the proposed plan, the likelihood of following a vehicle's course is little. In addition, the absence of secure correspondence channels among the control and information layer, and divulgence on organization assets removed at the SDN or RSU controllers can reveal the VANET clients to different protection vulnerabilities.

5.8. Forgery Attack

This type of attack comprises molding and transmitting bogus admonition messages, so as to taint enormous bits of the roads [86]. For example, the attacker can communicate a fashioned Global Positioning System (GPS)-based signal so as to deceive vehicles to receive off-base area data. Instances of conventional quick assistance against this attacker guarantees the secured confinement. In a study by Abu-Ghazaleh et al. [87], the authors define the triangulation method to decide the situation of a vehicle. Utilizing this procedure, assailants cannot diminish the separation between two neighboring vehicles. In another study by Capkun et al. [88], the authors developed the unquestionable multilateration so as to decide the situation of the vehicle from the lot of reference focuses whose locations are identified

ahead of time. Independent position confirmation [89,90] is a system to distinguish the effect of misrepresented position data specifically for location based directing conventions at the VANETs. It depends on different ideas, for example, the greatest thickness limit and position guarantee catching. Jaballah et al. [90] proposed a protected appropriated area check to distinguish vehicles cheating about their positions. The discovery component does not depend on extra equipment yet just on communitarian neighbors.

5.9. Tampering Attack

A vehicle that goes about as a transfer can disturb correspondences of different vehicles, in this way prompting alterations in travel. Henceforth, the vehicle can drop or alter or degenerate communication. The OBU altering utilizes the information layer degree of based designs made through various vehicles. Specifically, the aggressor might change information, messing with the on-board detecting. So as to distinguish altered information bundles, the approaches depend on irregularity location practices. For example, Li et al. [91] proposed a self-ruling guard dog development to guarantee that guard dog hubs screen the practices of the handing-off hubs.

5.10. Jamming Attack

In this type of attack, an aggressor can parcel the system even without trading off cryptographic components [55]. Due to the communicative idea of remote correspondence, an assailant can stick the system by utilizing an amazing transmitter. This type of attack can prompt a counteract by gathering detected information if there should be an occurrence of a brilliant stopping application. In addition, the RSU controller will not have the option to direct the vehicles. In based structures, this type of attack can be relieved. The RSU assembles and screens the nature of the channel, and afterward sends the report to the controller. After that it selects the rundown of a poor channel and requests that the RSU sends this rundown to the all conveyed sensors [55]. The jamming attack is well elaborated in Figure 14.

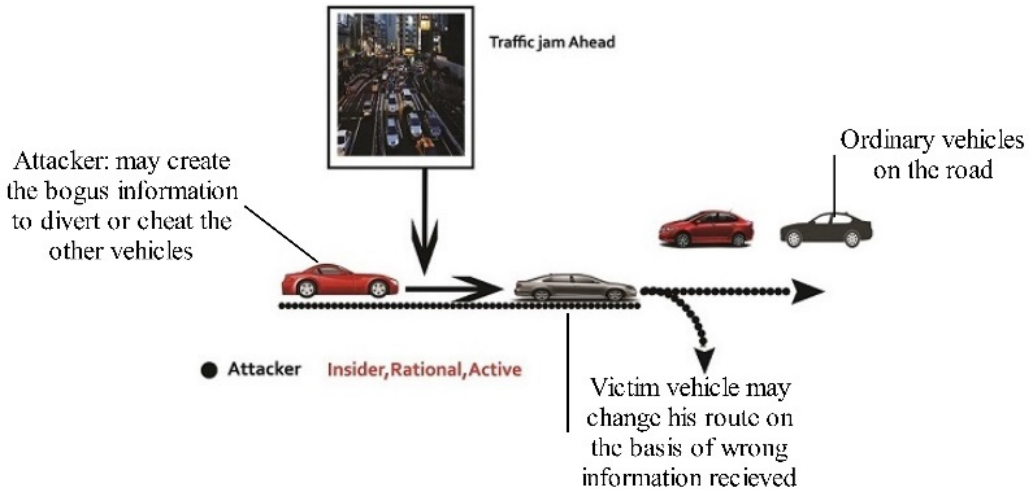

Figure 14. Jamming attack in SDN-based VANETs.

5.11. Impersonation Attack

In this kind of attack, an adversary can take on the appearance of the police so as to deceive different vehicles to back off or alter course [55]. An aggressor can similarly parody positive messages or administration commercials, and afterwards imitate RSU controllers. In addition, an aggressor can impact the course of its surrounding vehicles in the network by the distribution of inaccurate data related to the road conditions. Various methodologies has been developed so as to recognize pantomime attacks [55] in vehicular networks. Porras et al. [82] developed an appropriated methodology where

each vehicle can check the guaranteed places of nearby vehicles so as to distinguish troublemaking vehicles. The proposed methodology depends on measurement calculations to improve the exactness of position confirmation. The identification of tricking hubs is affirmed while watching the sign quality dissemination of a speculate vehicle over some stretch of time. The impersonation attack is presented in Figure 15.

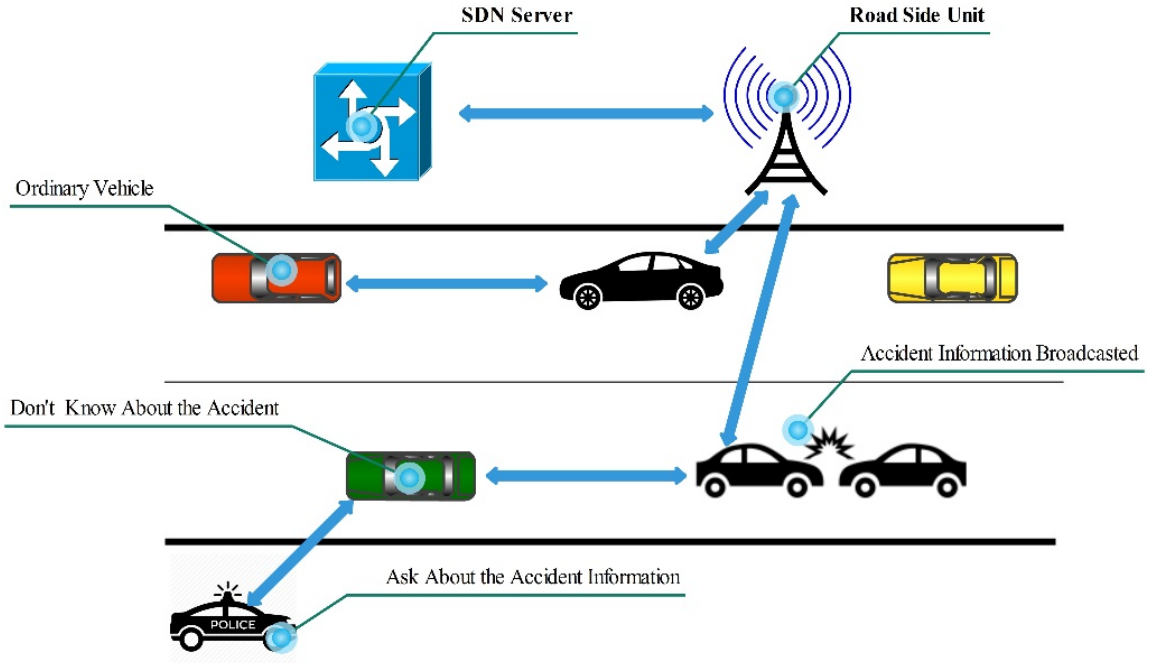

Figure 15. Impersonation attack in SDN-based VANETs.

5.12. Black Hole and Gray Hole Attacks

Another risky attack that particularly influences security applications is the black hole attack [55] (shown in Figure 16), where vehicle assailants connect with different vehicles by guaranteeing that they have the best course to the goal or have the best position to advance the bundle. After different vehicles send their bundle to aggressors, the pernicious vehicle disposes of all parcels from the system which causes it to lose colossal bundles including basic data and security messages. In addition, pernicious vehicles go about as dark hubs and misinforming bundles, sifting them per their advantages. A solitary malevolent hub or many malignant hubs chose a few bundles to advance and drops others [55].

More or less, a name-based sending plan is used to advance solicitations and convey information back to buyers. Illuminating the black hole attacks can be accomplished either by verifying the sending plane itself or by utilizing secure name spaces to advance name-prefixes that do not exist in the forwarding information based (FIB) table. Furthermore, as the based sending plane advances Interest/Data packets without realizing who is mentioned or who will serve, these types of attacks may not influence SDN-based VANETs even by reporting that they have the best course. In any case, as the based sending plane uses various leveled names to distinguish substances and administrations, a malevolent hub can, without much of a stretch, screen the sending framework and channel dependent on content names the permitted and denied parcels, which make these types of attacks hard to tackle in such cases particularly when a gathering of pernicious vehicles dispatches the attacks [92,93].

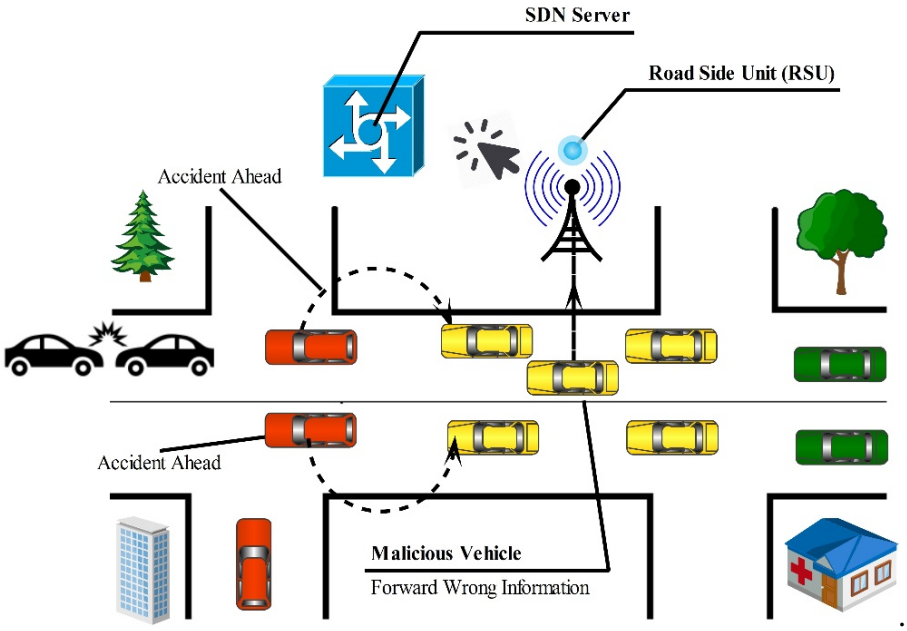

Figure 16. Black hole attack in SDN-based VANETs.

5.13. Wormhole Attack

The wormhole attack comprises of making a passage between at least two community oriented malevolent vehicles, intending to record and transmit information bundles between them. Thus, in order to attack, malevolent vehicles draw in other neighbor vehicles about the connection between them as the best way to get the information as opposed to utilizing the first trusted way. After malignant vehicles get parcels from unfortunate casualty vehicles (Figure 17), they epitomize and pass on to another pernicious vehicles, where the last one opens the embodied bundles and spreads them in the system [55].

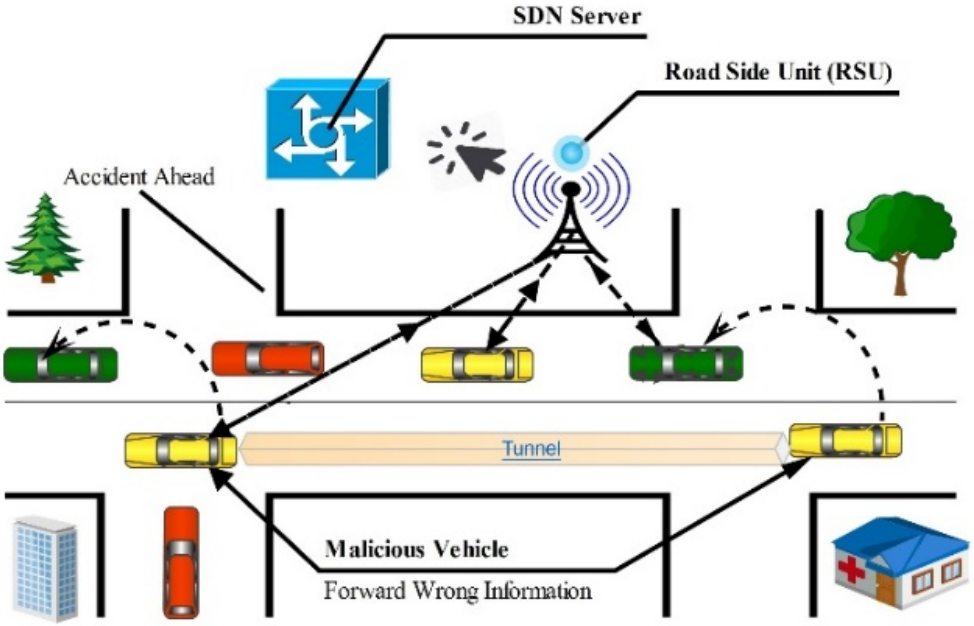

Figure 17. Wormhole attack in SDN-based VANETs.

The principle target of this type of attack is to change the system legitimate topology and remove the significant data sent through the passage, just like making a private system among the malignant

vehicles. In an IP-based system, assailants utilize their IP deliveries to make the passage. Due to the utilization of names rather than locations and sending bundles without the need to realize who is mentioning and to whom ought to advance, wormhole attacks may not be effectively executed in based systems [44,94,95].

5.14. Man-in-the-Middle Attack (MiMA)

In MiMA, a noxious vehicle in the correspondence way holds all navigated data and injects bogus data between vehicles. This type of attack, as shown in Figure 18, effectively affects the security applications particularly if the injected data are about mishaps that may cause life-jeopardizing mishaps. On account of the substance based security, all data are marked by the first maker during creation, and any adjustments in the information payload during the correspondence is presented as changes in the first marks [55,96].

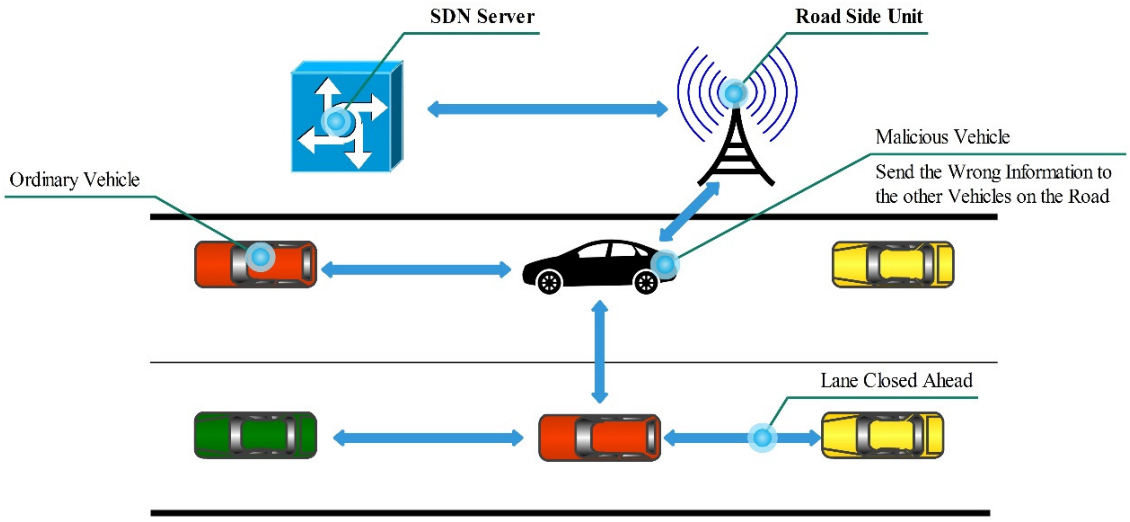

Figure 18. Man-in-the-middle attack (MiMA) in SDN-based VANETs.

5.15. Bogus Information

In this kind of attack, a pernicious vehicle may create bogus or wrong data and send it to the system so as to control different vehicles. We find that different types of attacks can be delegated as false data attacks, for example:

5.15.1. False Position Information

The vast majority of security applications depend on the specific position, where broadcasting bogus position data are a hard and basic issue in SDN-based VANETs. A solid trust and approval model is expected to anticipate such bogus data.

5.15.2. GPS Spoofing

A malicious hub uses the Global Positioning System (GPS) satellite test system to deliver signals which are more grounded than the real satellite sign and have a tendency to misdirect vehicles to acknowledge the bogus position data. This kind of attack is identified with physical gadgets. Therefore, SDN-based VANETs should manage trust in such information engendering, where community oriented vehicles may identify this data and stop it [55,96].

5.15.3. Illusion Attack

The attackers scatter wrong messages to deceive vehicles by abusing the flow street conditions, similar to a gathering of autos that moves gradually so as to trick drivers into putting stock in this

off-base data. This type of attack is difficult to identify as the physical vehicle's sensors are utilized to make and spread inappropriate traffic data. Counterfeit data attacks are generally connected with verification security conditions, which are simple undertakings to manage SDN-based VANETs, as the substance is ensured and confirmed at the parcel level with a safe substance name official in systems dependent on hashing procedures and open private keys [96].

5.16. Replay Attack

In the replay attack, a malignant vehicle spares a duplicate of the message and resends it later in the system so as to delude different vehicles, causing superfluous halting. As SDN-based VANETs are a reserve based system, this sort of attack can be overwhelmed by utilizing the substance name and checking the lifetime esteem in data parcels to know the information freshness in contrast to the mentioned substance [55]. The replay attack is presented in Figure 19.

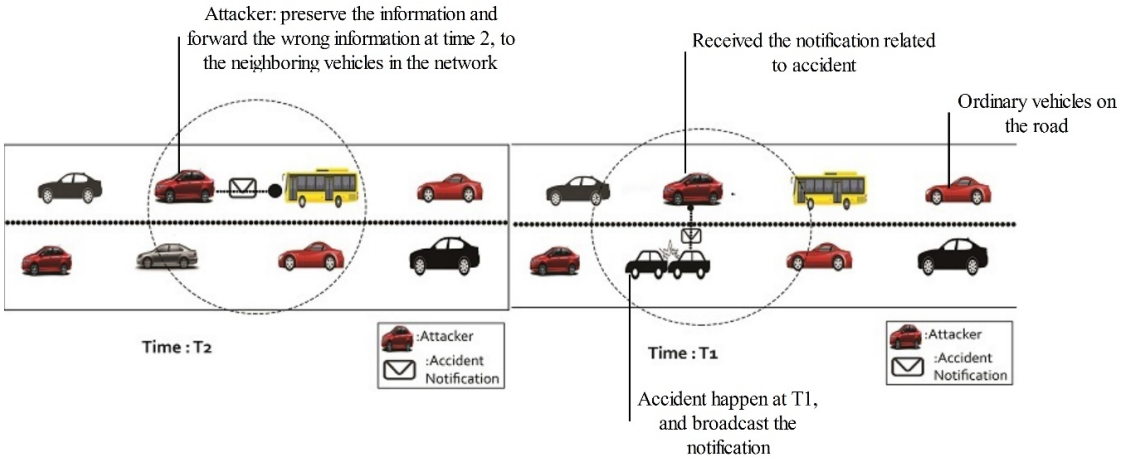

Figure 19. Replay attack in SDN-based VANETs.

5.17. Sybil and Masquerade Attacks

The sybil attacks are considered as one of the most perilous attacks in the SDN-based VANETs, where the malevolent vehicle acts that it is in excess of a hundred vehicles by causing confusion and countless pseudonyms (Figure 20). The objective of this conduct is to mislead dissimilar vehicles and ask them to change their routes. In actuality, as the name shows, in disguise attacks, a noxious vehicle changes its personality [55] to be another vehicle, attempting to deliver various messages, modify, and replay with data to bamboozle different vehicles [97].

For instance, a malevolent vehicle can change its personality to be a rescue vehicle and power different vehicles to back off or change their courses. Previous studies [98,99] proposed a trust model dependent on SDN-based VANETs for self-sufficient vehicular applications so as to counteract bugged data and vehicle following. The authors structured a progressive naming plan made out of four levels: independent vehicle, producers, vehicles, and information. They utilized an intermediary pseudonym based plan so as to make it hard for aggressors to follow vehicles. SDN-based VANETs tie content names utilizing cryptography calculations; for example, open private keys that may verify the official and exceed these issues. In addition, circulated arrangements, such as square chain, can be applied to implement the substance name authoritative and save substance and client security.

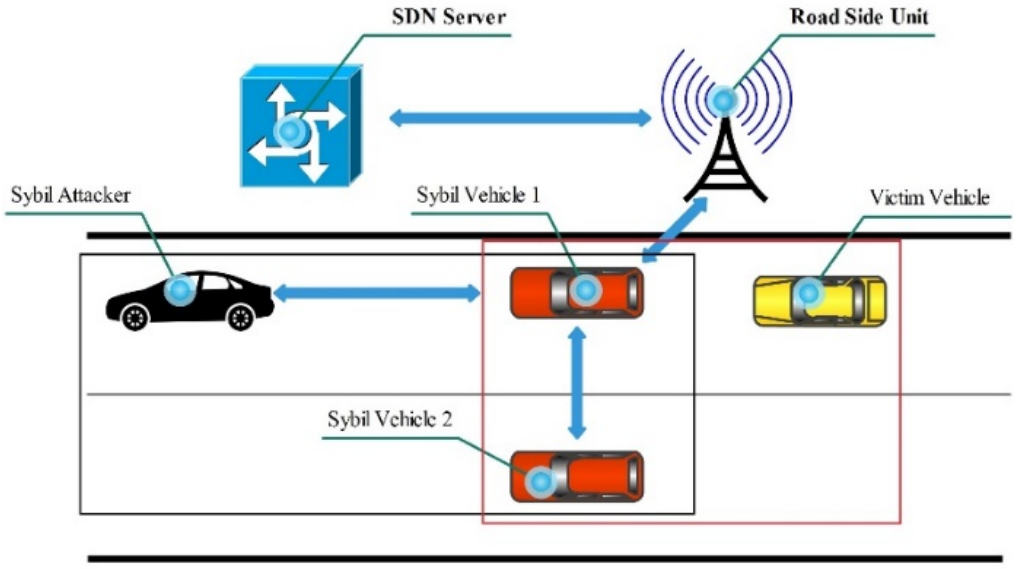

Figure 20. Sybil attack in SDN-based VANETs.

5.18. Timing Attack

In the timing attack, the malevolent vehicles do not advance the crisis messages and data at the ideal time as shown in Figure 21. The attacker in the timing attack creates correspondence delay and adds schedule vacancies to the received messages. Their neighbor's vehicles get these messages past the point of no return after the time they need it. The timing attack is a basic issue, particularly when managing time-limited applications [55].

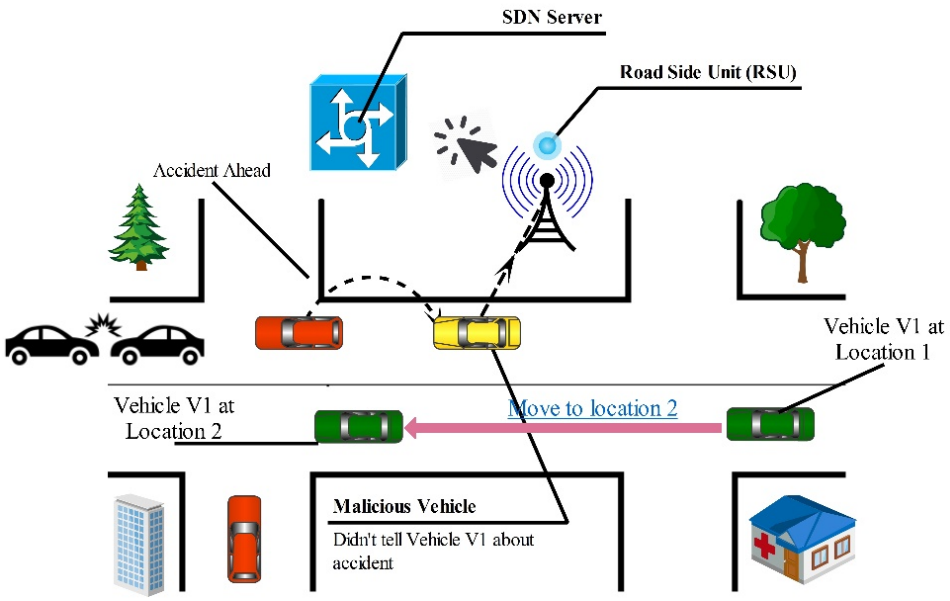

Figure 21. Timing attack in SDN-based VANETs.

5.19. Snooping Attack

Snooping is an isolated attack, where the noxious vehicle gets to the substance and data that cross it, so as to utilize it for its advantages without alteration. In any case, as the substance is secure and marked, and utilizes cryptographic hashing strategies when it has been made, just real clients can get to it. Thus, snooping attacks might not affect SDN-based VANETs [55]. At the end of this section we

categorize the attacks with respect to the infotainment and security. The taxonomy of the attacks with respect to these categories are listed in Figure 22.

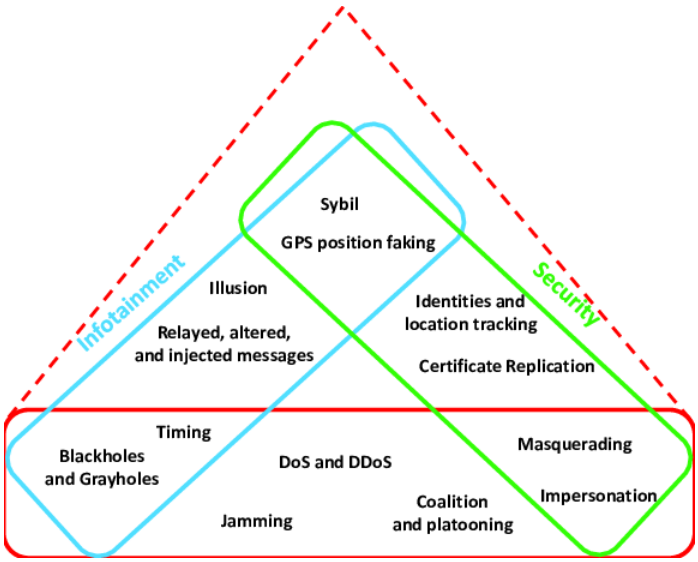

Figure 22. Taxonomy of attacks with respect to security and infotainment applications.

6. Challenges in SDN-based VANETs

Despite the fact that based is quickly developing, there are many more challenges related to the effectiveness, versatility, and unwavering quality (acceptance) of it. These difficulties might choose the upcoming heading in the advancement of the based. The closeness and decentralization of the SDN-based VANETs give various advantages to systems, like low idleness, proficient vitality use, and more prominent throughput. The most recent vehicles in VANETs are being installed through various sensors for handling and remote correspondence abilities. This has empowered numerous potential advantages to be misused, for example, safety, proficiency, and solace while they are out and about. The SDN-based VANETs provide some benefits, but still some challenges are available which are listed below in greater detail.

6.1. Mobility of the Vehicles

Conventional models of sensor systems think about a static domain. Likewise, specially appointed systems additionally center around constrained versatility dependent on workstations and hand-held gadgets conveyed by the clients. In any case, portability is a standard for vehicular systems. The examples of portability for vehicles has a robust connection. All vehicles out and about have an always altering arrangement of neighbors, few of them have certainly not gone over and it is very improbable to have a connection later on [100]. This regularly altering environment of vehicular elements could obstruct the utilization of the notoriety based plans. To rate various vehicles dependent on unwavering quality of reports is questionable to demonstrate value such that a particular vehicle might not get adequate data from a similar vehicle to settle on its choice related to that vehicle. Furthermore, as the two vehicles are likely to correspondence for a couple of moments, we cannot think about conventions, which require a connection among sender and collector [101].

An updated portability model is required to provide information identified with the exact vehicular behaviors, such as vehicular speed, expectation of vehicular notoriety, and conveyances. Specifically, we built up a progressively intricate portability model which examines the versatility designs precisely and exactly for various conditions that are valuable for functional applications. Information on common vehicular practices and versatility examples can assist with bettering correspondence and computational asset use. Along these lines, adaptability among the edge hubs and among edge

and the cloud could likewise be contemplated. In spite of ordinary server farms, edge gadgets are geologically conveyed over heterogeneous platforms. The QoS crosswise over stages should likewise be advanced [102].

6.2. Switching, Routing, and Forwarding

On account of directing and sending, numerous inquiries emerge like the exchanging of SDN servers and their administrations from source to goal as indicated by the development of the vehicle.

6.2.1. SDN Server Switching

Vehicles for the most part settle on choices of their best course of action in a limited ability to focus time as the vehicles are continually moving at a blasting velocity. In this manner, it is hard to foresee that specific vehicles are going to get administrations from BS or SDN servers, in view of traffic and open transportations data making progress examples of the vehicles movement for anticipating the vehicles in the next area. In spite of the way that numerous methods have been applied to decide the issue, this is still an open research issue and much work need to be completed [103,104].

6.2.2. Service Switching

As discussed above, when the vehicles fluctuate their situation starting with one SDN server, then the next, the administrations which utilize from the previous SDN server, should be moved to another SDN server. In a study by Stolyarova et al. [96], a calculation to foresee the QoS for administration proposals was developed. In spite of the fact that this calculation works effectively for the portable client, it may not be very proficient in a vehicular situation. This is an exceptionally muddled and sensitive undertaking to acquire opportune and dependable assistance transmission among vehicles and edge servers so as to keep up the QoS in a vehicular domain [104].

6.2.3. Content Caching

Content storing, for example, before bringing and helpful reserving, can be executed in SDN-based VANETs. The storing substance can likewise incorporate those components which the vehicles have not mentioned, however, they acquire those substance over the remote association. It might be valuable for vehicles to spare and advance those unmentioned substances (e.g., cautions created in a tough situation). What is more, there are still holes in storing strategies that make the best fleeting and spatial extent of the vehicular substance [105]. By storing in substances which are out of the spatial degree, and furthermore reserving out of the old substances (an hour prior to traffic congestion data on an interstate), a few additionally consuming specialized ramifications are developed as follows:

- In spite of the fact that vehicle-to-vehicle correspondence can improve the limit of the system regarding content reserving, they are not yet ready to approve a dependable and highest-rate information administration for vehicles because of the amazingly powerful and unsure system topologies and severe channels conditions.
- Since the SDN-RSUs are sent in various areas and diverse system administrators possess them, the participation of the SDN-RSUs to give substance to the vehicles must be considered as far as the valuing model.
- A reserving plan should be created to improve the content hit rates by the base handovers cost by recognizing store size parting, predominant substance refreshes, and guaranteeing portability mindful reserving for the smooth handover even with the highest versatility of vehicles. In addition, these vehicular storing frameworks require such procedures, which by considering the geologies and system setups effectively investigate the points of interest.

6.3. Need to Deploy Network Elements

An adequate number of system components upgrade the system's presentation on a huge scale. Since the organization of the system gear brings about a significant expense, it is fundamental to ideally introduce a fitting number of system components [43]. The significant apprehension is to locate a reasonable area so the effectiveness of the vehicular systems can be amplified. Moreover, the cost should essentially be upgraded and furthermore the SDN servers and the SDN-RSUs ought to be conveyed at such points where accessible assets can be overseen ideally. Due to differing traffic dispersion in the city condition, additional servers are sent in the congested zones. As servers assume an imperative job in distribution traffic communication, the SDN-RSUs represented by the SDN servers influence the traffic bundles to move in the foundation with no requirement for multi jump correspondences [43].

Through the foundation, these bundles are moved to different hubs in the system. Getting through the framework with less bounces lessens the accepting time of the SDN servers which forward the communication to the next vehicles. Consequently, it is at last compulsory to build up an ideal system that gauges the base need of the SDN servers just as the SDN-RSUs to be conveyed so as to limit the organization cost and to boost QoS [43,106].

6.4. Ubiquitous and Network Connectivity

The prime goal of heterogeneous vehicle systems administration is to ensure a consistent, universal, and undistinguishable system availability to guarantee the rigorous QoS and the quality of experience (QoE) of different vehicles' security and the non-safety applications, programs, and the passengers, separately. Without a doubt, two vehicles and vehicular clients ought to consistently be associated with the ideal radio connection innovations that guarantee ultra-lowest start to finish delay (inertness), highest transfer speed, upgraded information rates, and cost-efficiency [107]. However, the heterogeneity of assorted radio access innovations is a challenging errand to handle, and in this way, insightful vertical handovers choices are compulsory to guarantee consistent versatility. In the distributed vehicular systems administration condition, vehicles either cross along the geological areas of covering radio connection advances or diverse topographical districts with particular radio access advances [108]. In addition, inferable from the profoundly unique conduct of vehicles, they are required to perform visit handover. By the by, too many visit handovers waste valuable system assets and should be relieved. Moreover, for the vertical handovers to unfold effectively, three vertical handover choice systems ought to be executed with a negligible conceivable postponement [29]:

- For the available networks, it is necessary to determine the need of the handover.
- The target selection of handover is the best network among the all available networks.
- Handover-activating conditions approximate in deciding the exact time to trigger the handover for the chosen system. Since the unified SDN-based controller in a distributed system has a 10,000 foot perspective on the whole fundamental design, it can meet the consistent, omnipresent, and undistinguishable system networks.

Since the SDN-based controllers have worldwide information on the accessible physical radio assets of each radio connection to BS/RSUs along a vehicle's foreseen voyage, smart vertical handovers plans could be likewise utilized for exchanging determinations.

6.5. Heterogeneous Multi-Hop Routing

Vehicles regularly scatter basic data to different vehicles in their quick region by means of multi-jump V2V correspondence or by transferring the communication by the RSUs, all with an alternate radio connection innovation. All things considered, this basic communication may get lost if the available connection comes up short or the next jump becomes inaccessible (particularly in inadequate rush hour gridlock conditions), therefore bringing about a correspondence breakdown and wastage of valuable system assets, which may prompt deadly mishaps on the streets. In addition,

a portion of these radio connection advances are nearly more costly as compared to others (i.e., the LTE is genuinely more costly as opposed to WiFi and dedicated short-range communication (DSRC) [29]).

Along these lines, an exceptionally solid and cost-viable correspondence through multi-jump directing is fundamental in a VANET setting. It is likewise vital in reestablishing the system availability, particularly on the off chance that the serving radio access innovation comes up short, yet a covering radio access innovation is open. In a similar manner, on account of vehicles outside the inclusion scope of the available RSUs, the system bundles can be imparted by the multi-hop V2I and V2V correspondence by the vehicles related with RSUs; brought together by SDN-based controllers with a worldwide perspective on the basic system can delineate the most limited, yet ideal multi-hope courses for this reason [29].

6.6. Broadcast Storm Mitigation and Network Slicing

The absolute increment in accessibility of on-board sensors and the edge correspondence stages encourage vehicles to scatter basic messages to different vehicles and people on foot in their region. Such messages are incredibly basic in nature and ordinarily incorporate, however are not restricted to, crisis vehicle admonitions, forward impact alerts, overwhelm crossing point alerts, powerless passerby admonitions, daze bend alerts, and line alerts. Spreading these bundles in a simultaneous way or to vehicles not requiring similar outcomes in parcel crash, gagging the whole system, and impressively deferring the bundle conveyance timetables may prompt various grave results inside the setting of vehicular systems [29,67].

This sensation is alluded to as communicate raging where a sheer measure of traffic is communicated, thus devouring the valuable system assets and deserting less assets to move ordinary traffic. Communicate tempest could likewise be activated by a vindictive substance, and the security of the system is additionally vital so as to guarantee that such elements are not permitted to enter the system in the principal occurrence, yet in the event that they do as such, proper recuperation components ought to be set up to track and accordingly destroy them from the system [67,109].

6.7. Dynamic Network Topology

The highest vehicle portability effects the quick fluctuations in SDN-based VANET topologies and variances in radio correspondence channels. The continuous topology fluctuations additionally impede the constant assortment of systems administration information that is obligatory at the controller level to keep up a present perspective on the information layer assets. The deferred or off base worldwide point of view drives the controller to encounter delays in conveying directions to organize components [110]. In this way, to help the fast reception of SDN globally in the VANETs, it is obligatory to create components which deal with higher system versatility the executive issues in target SDN-based VANETs. To this end, there hardly exist any methods (e.g., utilization of fog registering and nearby controller at organize edge computing) that attempt to limit the impact of system versatility in the VANETs. These procedures are not in propelled phases and therefore cannot be ported legitimately (i.e., with no improvements) in SDN-based VANETs [111].

Currently, the best answers to deal with the adaptability affected problems in SDN-based VANETs are the ones wherein the vehicles' future bearings are anticipated by depending on various measurements (e.g., speed, previous driving examples, and the GPS area) by relating AI apparatuses. Although, a correct and legitimate execution of such arrangements is trying because of the protection concerns and high organization multifaceted nature [111].

6.8. Broader Flow Rule Definitions and Policies

In the SDN, the switches preserve sending tables that contains the following three items:

- Information sending rules
- The actions list for the communication rules

- A counter list to measure the communication

Nonetheless, the current stream decides the arrangements that administer the information; correspondence in SDN organization should be upgraded to deal with the basic requests of a wide scope of novel VANET applications and programs. For instance, the SDN-based controller can offload a portion of the assignments to RSUs/BSs that go about as neighborhood (or the lowest level) controllers by forwarding the general stream rules or arrangements rather than explicit principles related with an information stream. Lastly, these neighborhood controllers could give or introduce information stream specific standards and arrangements relying upon their nearby information on the system. Additionally, the RSUs and BSs could process the gathered systems administration data locally for settling on a portion of the choices, and furthermore send similar data to cloud server farms and SDN controllers by means of a southbound interface for worldwide, long-haul use [112].

6.9. Security and Privacy Considerations

In SDN-based VANETs, the SDN-based controller oversees organized assets and furthermore controls different system administrations (security, traffic, the board, and QoS administrations); in this way it is essential to shield the SDN controllers from various digital attacks. The proliferation of vindictive data to the controller from enemies can prompt serious mishaps. For instance, DoS attacks can be propelled to incapacitate the tasks of the controllers which could be undermined by the internal attacks [55]. Thus, the security of the SDN-based controller turns into a need as it is concentrated basic leadership element in SDN-based VANETs. Moreover, the new security vulnerabilities that may happen because of the coordination of the VANETs and SDN or different innovations with SDN-based VANETs should be examined before the organization of such half breed structures [112].

6.10. Interworking Gaps Among Heterogeneous Networks

The conjunction of the heterogeneous V2X systems necessitate proficient interworking instruments that permit productive correspondence between these systems. Additionally, the current SDN-based VANET designs are missing institutionalized NBI/SBI APIs and northbound APIs for vehicular programs and applications [113].

6.11. Misbehavior of Elements from Different Technologies

The utilization of different advances and structures in understanding the new VANET applications also builds its attacks vectors. It is on the grounds that getting out of hand or powerlessness in any of the incorporated innovations may influence the tasks of the entire VANET. For example, we talked about how utilization of the SDN-based controller includes another arrangement of the security susceptibilities in a system [114]. Essentially, the downsides in other incorporating advances (e.g., 5G, ICN, Fog/Edge/Cloud) can altogether expand the dangers in the coordinated system. Gao et al. [48] elaborated on general security susceptibilities and attacks for SDN-based VANETs. The work talks about the security ramifications of SDN-based VANET models at every plane. The planes (application, control, and information planes) of SDN-based VANETs are essentially verified such that the security arrangements address cross-layer dangers which view that security breaks relating to one layer could hurt different layers as the layers are intensely reliant on one another [115,116].

6.12. Highly Dynamic and Distributed Behaviour of Vehicles

The enormous difficulties for SDN-based VANETs is the profoundly unique and disseminated conduct of the vehicles which makes it amazingly hard for the SDN control layer to keep up the running time places of vehicles and anticipated traveling directions. This, accordingly, prompts organization of the board overhead and considerable measure of start to finish delays for security basic and non-wellbeing vehicular programs and applications. Without a doubt, dynamic portability and dispersed conduct of the vehicles, that are in actuality the underlying drivers for all vehicular

systems administration difficulties, require cautious consideration [117]. Moreover, it is vital to spread system parcels relying upon the geological situation of vehicles rather than their IP addresses, and exceptionally smart and productive confinement and direction expectation components should be planned so as to handle such a test. This necessitates that knowledge is passed to the edge of the system. Moreover, various confinement strategies have been proposed in the exploration writing for versatile specially appointed systems, and the equivalent could be investigated and hence advanced for SDN-based VANETs [118,119].

6.13. Mobility-Aware Edge Caching

The other critical test in SDN-based VANETs is to figure an ideal edge reserving approach; for a specified anticipated vehicle (or the vehicle passenger) request, it is basic to figure out which vehicular programs, applications, administrations, and additionally substances ought to be set in each edge store to limit the normal deferral for such demands. Assuming such, or comparable, solicitations are not being taken into account through the edge-based stores, getting them from remote back-end servers should actuate an essentially bigger postponement, which turns out to be very basic particularly with regards to vehicular safety applications. A few analysts in the scholarly community and industry have just proposed various approaches, including, yet not restricted to, leaving duplicate down, leaving duplicate somewhere else, haphazardly duplicate one, probabilistic reserving, dormancy mindful reserving, clog mindful storing and search, and PopCache [120]. Moreover, reserve removal techniques are vital as they figure out which passages should be ousted from the store so as to make adequate space for the new sections and regularly remember first-in first-out, least as of late utilized, least habitually utilized, and random plans. All things considered, since vehicles navigate at extremely high speeds and substance ubiquity accordingly fluctuations at a unique jump, it is very hard to assess the substance fame at some random time and area on a prompt premise, and in this manner, keen powerful edge-based reserving calculations should be formulated in such a manner [121].

In SDN-based VANETs, the SDN controller has adequate information on a vehicle's available edge hub (EN) and the time it proceeds to navigate by the inclusion of the particular EN alongside the foreseen directions and grouping of the ENs in forecast directions of vehicles. This encourages the SDN controller to send the imperative substance ahead of time on ENs in the foreseen directions of vehicles. In addition, it is suggested that the substance ought to be put away on ENs where vehicles have the genuine opportunity to gain them, for example, on moderate traffic areas or clogged street convergences. In this way, wise versatility mindful edge reserving models could guarantee ultra-solid and low-idleness correspondence, in this way, not only gathering the stringent QoS of assorted vehicular security basic and non-safety applications, but also ensuring the QoE of the vehicular clients [121]. The taxonomy of the mobility management in the SDN-based VANETs is shown in Figure 23.

6.14. Management of Rapidly Changing SDN-based VANETs

Highest adaptability of hubs (vehicles) makes quick and unusual changes in the system topology of SDN-based VANETs. It is difficult for the SDN-based controllers or the RSUs to control the vehicles in the network and provide the facility for direct communication. As the DSRC or the wireless access for vehicular environment (WAVE) availability are not ready to endure huge variances among the speeds in the V2V foundation, there are greater odds of broken connections. However, this procedure can be dealt with by some productive steering calculation and adjustments in the framework; yet this turns out to be expensive [13,122].

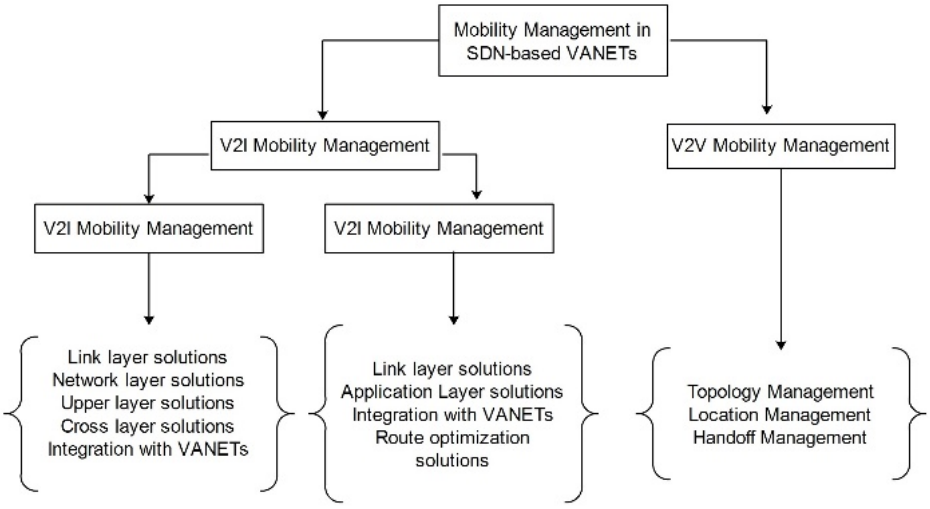

Figure 23. Mobility management in SDN-based VANETs.

6.15. Security of SDN-based VANETs

Security is as yet the significant dread that is preventing SDN-based VANETs from becoming generally adequate. A considerable amount of SDN-based VANET applications pursue a brought together method where SDN-based controllers are the fundamental units which are answerable for the working of the entire system. It is anything but difficult to attack an individual controller to shut the entire system down. A vindictive client could hide intrude into the framework and take choices rather than the controllers. By such invasions, systems could be controlled or clients' security could be put in jeopardy [12,40]. Moreover, DDoS attacks can flood the stream table with counterfeit passages, which shut the system down and make it inaccessible for genuine clients. Thus, it is fundamental to ensure controllers. Hasrouny et al. recorded numerous kinds of attacks in the four principle classifications. First is dangers to remote interface, for example, area following, DDoS, Sybil attack, malware attack, spam attack, MiMA, savage power attacks, and black hole. Second is equipment and programming parts of the design, for example, injection of the wrong communication (fake data), communication concealment or adjustment, usurpation of personality of a hub (satirizing or pantomime or disguise), altering equipment, directing system, GPS mocking, burrowing, and black hole [11]. The third is the threat to the equipment, for example, sensors and the handsets of vehicles. Illusion attack and the jamming attacks are in the rundown of the third classification. The forth is threats to framework, for example, sessions hijacking, renouncement (loss of occasion detectability), and unapproved get to [56].

6.16. Latency Control in SDN-based VANETs

In SDN-based VANETs, inertness is a truly erratic imperative. As it is remote assistance, one cannot guarantee what time information is received. In any case, dormancy control can be accomplished by streamlining a few or various parts of system execution by assessing the board [110]. The dormancy control is straightforwardly reliable on streamlining of assets. These days, distributed computing approaches are inclining as they are more enhanced. In addition, the expense of utilizing distributed computations in VANETs is costly as the quantity of the vehicles begins developing exponentially [123]. The explanations for the expenses are activities, for example, passing client data to cloud database, gathering client data with respect to channel conditions, computational outstanding task at hand in the cloud, QoS necessities, area following, giving the ideal asset access to clients, and so forth. These all presents idleness in the system. In this way, dormancy control ought to be a significantly engaged subject for new systems [47].

6.17. Scalability of Architecture

Adaptability of the existing SDN-based VANETs are the key components as the auto portable industry is congesting. The odds of unforeseen obstacles and unexpected fluctuations are erratic although voyaging. There are numerous elements, for example, specialized up-degree, complex roads topologies, framework harm, and so forth, which can influence the presentation of SDN-based VANETs [68]. The expanding number of the vehicles pursued through an expanded number of interchanges can likewise debase the presentation of the lowest adaptable SDN-based VANETs. In addition, design ought to have the option to determine the requested administrations and differing climate conditions. This results in wasteful asset management and degrades system efficiency. One more thought is calamity of the board. At the point when some messed up frameworks in view of the catastrophe are not fit for transmitting bundles, then the SDN controller ought to keenly allot different functionalities to help and maintain the QoS limitations [124].

6.18. Heterogeneous Network

The other difficult undertaking for the SDN-based VANETs is interworking holes between the diverse systems as the eventual fate of SDN-based VANETs is not constrained to correspondence among the vehicles. It will stretch out to novel innovations and gadgets having numerous highlights from various producers. Consequently, the issue of shared selectiveness happens, and correspondence between vehicles can come up short. The institutionalization of advancements is a way to conquer this issue. As a result of an enormous number of vehicles, some normal issues, for example, crash, long postponements, expanded parcel misfortune rates, impedance, and commotions, can happen [125]. Along these lines, existing heterogeneous V2X systems require effective interworking instruments. According to this present reality situation, the plan of SDN-based VANET design can be dependent on heterogeneity of the RSUs. For instance, in city conditions where forceful rush hour gridlock is normal, SDN-based VANET design requires numerous novelizations of the system topology. Along these lines, the producing limit of system topologies must be improved. For the use of SDN-based VANET usage, topology forecast is not basic errands for RSUs as the system topology does not vary a great deal. In urban areas, where there are less vehicles, the RSU controllers can decrease their capacity of registering multi-hope communication [126].

6.19. Trustworthiness Evaluation, Misbehavior Detection, and Revocation Process

Reliability assessment of interest hubs in VANETs is an open issue. Any off-base advance in assessing a vehicle can place the lives of clients in harm's way. Henceforth, solid parameters for choosing the trusted vehicles in a network are needed. Analysts have proposed a technique for troublemaking identification, yet no methodologies are available for using these data [127]. The penalties are not well characterized for malignant vehicles. There is no work available for an actualized repudiation procedure to be attempted if any hub is getting out of hand in the system. Certificate Revocation List (CRL) based solutions are as of yet experiencing an improvement stage. Utilizing the constrained time testaments for the CRL and endorsements alteration, procedures that are not yet characterized are helpless under no framework for the CRL. The endorsement confirmation and disavowal are no longer handled. Along these lines, options ought to be found. Numerous analysts in past investigations have proposed ways to deal with supplanting the CRL [55,128].

6.20. Demarcation of SDN into VANETs

The strategy of characterizing the limits to the degree wherein one could coordinate the SDN into VANETs is still not characterized. Just altering the wired portion is not a correct incorporation. Despite what might be expected, changing over VANETs into a SDN-based system is anything but a shrewd choice. There are higher odds of powerlessness when any SDN-based VANET is designed by all planes of the SDN [1]. Such frameworks can present individual purpose of disappointment and

programming susceptibilities. For the most part, the foundation layer in the VANETs comprises a huge number of vehicles. Along these lines, this will affect the solicitation numbers from the foundation layer to the control layer and these circumstances can affect execution issues. As an attack of partition among the framework and the control layer in the SDN, structuring a decent reaction system is conceivable [129].

SDN-based VANETs could offer a channel assignment and psychological radio approach that allows highest transmission capacity and the lowest inertness correspondence. Usage of the SBI ought to be institutionalized and merchant skeptic since it is significant how the foundation layer corresponds with the control layer. An undeniable evaluation of the vehicular system can recognize which part of the control layer can be excluded from the foundation layer to get full points of interest of the SDN-based VANETs. However, the lack of such certifiable executions and reproduction apparatuses block such an assessment. Later, genuine consideration specified to the advancement of true usage and recreation apparatuses for exhibition assessment of the vehicles under the SDN-based VANETs to figure out which segment of the control layer ought to be decoupled from the foundation layer [130,131]. All the challenges are listed in Figure 24.

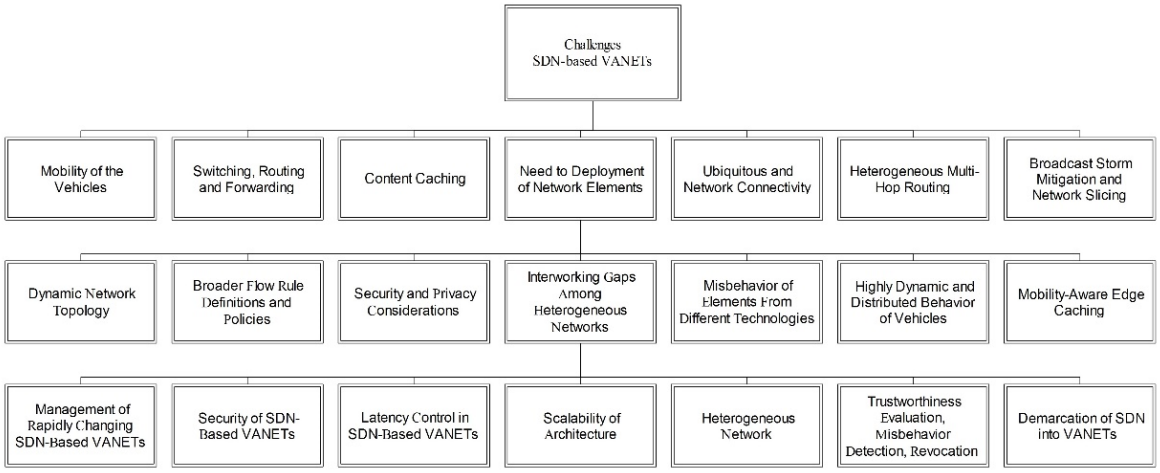

Figure 24. The taxonomy of the SDN-based VANET challenges.

7. Applications in SDN-based VANETs

7.1. Remote Video Analysis and Initial Assessment

The conventional rescue approach sends a crisis vehicle at whatever point a guide demand is received with no first appraisal of the mishap scene. The crisis vehicles attempt to land at the mishap point within the shortest time possible. Conventional salvage approaches do not consider any examination and exhortation of a location to see how basic is the mishap, which does not maintain a strategic distance from more harms and impacts, and furthermore for expelling the harmed people from the vehicle appropriately [132]. It is sensible to use sensors accessible in the vehicle to accumulate mishap related data and forward it to the closest salvage focus. In addition, a continuous video can be recovered and spread to the salvage focus, which can have precise direct data to assess the mishap dependent on visual data. Along these lines, it is conceivable to set up an effective salvage, and tell the appropriate specialists and gadgets to advance treatment [133].

7.2. Accident Notification and Congestion Avoidance

Since vehicles close by do not think about the car crash, traffic blockage may emerge at the mishap area. The expansion of blockage is on the grounds that the vehicles will go into a blocked street without knowing it, and subsequently stall out in the road. These conceivably obstructs the entrance of the crisis vehicles to the mishap area. However, a haze hub near the mishap area can characterize

a blockage shirking zone and spread it to caution vehicles going towards the mishap area. When a vehicle goes into a blockage shirking territory, it is informed to maintain a strategic distance from the mishap spot to forestall a traffic jam and postpone the salvage movement [134].

7.3. Fast Rescue Route and Emergency Traffic Prioritization

A strategy to organize crisis traffic can be characterized by staying away from delay in the salvage movement brought about by the traffic jam. In this sense, a salvage course is set, and the vehicles checking such a strategy will prepare for the crisis vehicles. Additionally, each haze hub that covers the salvage course can caution vehicles about the salvage action, thus diminishing the ideal time [132].

7.4. Efficient Data Dissemination

Profoundly modified information spread of SDN-based VANETs is a striking highlight. The information dispersal gives a take-off to numerous administrations, for example, crisis communicate administrations, versatile communicate interim time, security of clients, and so on. Nguyen et al. [118] built up a versatile signal-based information spread convention which scatters the admonition messages to vehicles close by when a risky circumstance happens without tossing an additional heap on the channel. The data dissemination depends on the safe and measured public key infrastructure (PKI), vehicular gatherings, the hybrid trust model, the CRL, and the board framework [110].

7.5. Applications-based Safety Services

The functionalities of the SDN in the VANETs upgrade the roads' wellbeing by utilizing V2I, V2V, and V2H correspondences. The SDN-based VANETs can verify or limit specific frequencies or channels for later usage. Emergency traffic or other special exercises could be used to save the frequencies [55]. The principle bit of leeway of SDN-based VANETs over regular emergency channels is that the description of repetition should be possible progressively. The SDN-based controller could hold the channels for the emergency administrations dependent on traffic situations, programs, and application needs. Essentially, these channels could be used to oblige different applications or administrations. Emergency communication, helpful for concentrated communication, can profit from the advantages of this. Different protection plans can likewise be executed to improve two security administrations, namely, path change cautioning and forward impact [40,106]. The taxonomy of the safety services are listed in Figure 25.

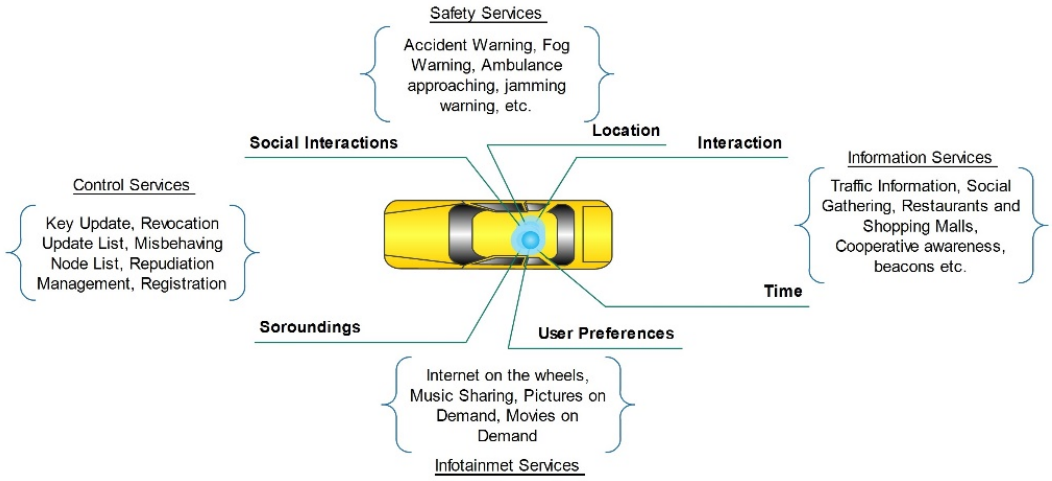

Figure 25. Taxonomy of safety services in SDN-based VANETs.

7.6. On Demand Reconnaissance Service

On-request reconnaissance is another help which is made accessible for the approved customer of a SDN-based VANET. This administration can be utilized in a crisis or examination situation. To utilize this administration, an approved hub (e.g., a squad car) must send an observation demand. The controller benefits from this solicitation. In answer to this solicitation, the controller implants the stream rules for the observation information to arrive at the requesters. When there is more than one solicitation for the indistinguishable data, for example, numerous requester hubs demand for video observation feed, the controller makes passages of rules in the stream table with the goal that a similar duplicate is sent to numerous requesters. This is likewise appropriate for infotainment administrations like video spilling, video conferencing, and media sharing [135,136].

7.7. Virtualization of Wireless Network

System virtualization administrations hope to provide theoretical and enlightening virtual systems over mutual physical system resources. The server farms use SDN-based VANETs to organize virtualized administrations, and such a thought could likewise be assigned to SDN-based VANETs. At the point when the individual system has utilized particular frequencies, singular systems traffic is isolated from one another. Creator attempted to adequately hack the system into system sections and made virtual remote systems [137]. By progressively gathering a remote hub for the RSUs, overhead was diminished. Presently, every RSU just engenders traffic from the gathering. A SDN-based controller administers the system and timespan of its individual radio edge/recurrence, which dispenses the system traffic in a programmable way. Moreover, the controllers have the organization of the setting input channels over remote hubs, and those hubs acknowledge the traffic as a contribution for that they are permitted. The fundamental utilization of information examining stops impedance among the two administrations [138–140]. The visualization of wireless networks and its characteristics are shown in Figure 26.

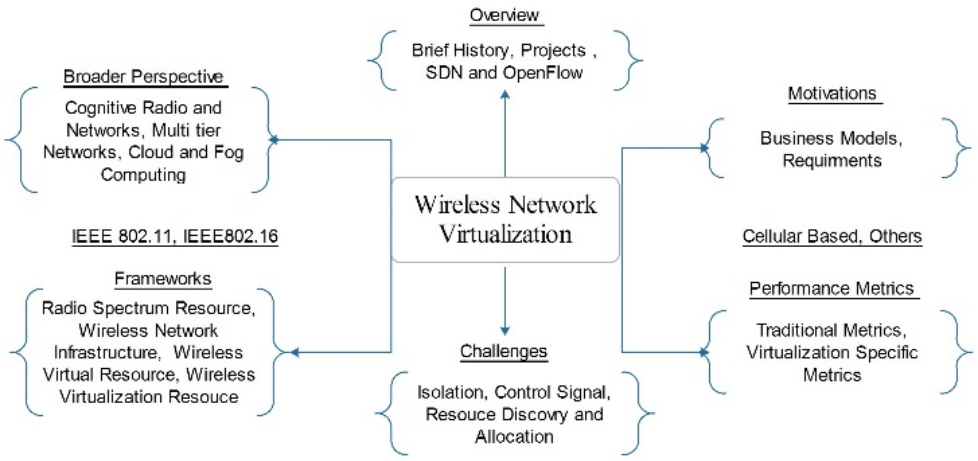

Figure 26. Wireless network virtualization.

7.8. Dynamic Air Quality Monitoring

Through the quickly developing auto portable enterprises, contamination noticeable by the discharge of gases is expanding. The Air Quality Index (AQI) is the estimation of the dirtied air. In certain nations, governments or autonomous organizations are estimating the AQI for different commitments. The vehicular wireless sensor network (VWSN) is actualized to screen the AQI. To make it more arrangement situated, sending IoT-based vehicles contamination checking framework is trending, yet despite everything it does not have a global point of view and few edge functionalities [12]. This can be overwhelmed by sending SDN-based RSUs in the VANETs. A SDN-based RSU is utilized to give focal access to crude information gathered by all SDN-based RSUs. All the SDN-based RSUs can

function as instructed by the focal controllers. The crude information assembled can additionally be prepared utilizing different information investigative strategies. The yield from prepared information can profit the wellbeing segment, condition part, framework division, and so forth [141–143].

7.9. Heterogeneous Support

In the VANET-based correspondences framework, heterogeneity is a regular thing. Although the VANETs utilizing IEEE 802.11p (WiFi) and cell correspondence rely upon either V2V or V2I. Novel VANET applications require increasingly productive and savvy correspondence advances to decrease correspondence cost. The known and financially cheap innovation is the DSRC, but it is not appropriate for the V2I interchanges as its remote range for communication is short. Then again, for long-extended correspondences, 4G/5G cell systems are utilized at the same time and they are exorbitant. Others such as Wireless Access in Vehicular Environments (WAVE), Universal Mobile Telecommunication Service (UMTS), and Worldwide Interoperability for Microwave Access (Wi-MAX), are additionally accessible. In the SDN-based VANETs scientists are allowed to pick access innovations for the various layers of SDN-based VANETs, which empowers heterogeneous accessibility and enhances the utilization of transfer speed and the channel [43,144,145].

7.10. Intersection Collision Avoidance

Intersection collision avoidance is utilized to support the driver or the vehicle for basic leadership, although crossing a convergence; this framework utilizes the correspondence medium of the V2I correspondence. RSUs accumulate information from the vehicles moving close to it and process that information. If there is any likelihood of caution or any sort of mishap, a notice information is forwarded to the vehicles that are close to the notice region so they can decide to stay away from it. It has various applications and programs in impact avoidance [11].

7.11. Warning in Case of Violating Stop Signal

These applications are utilized to forward ready information to drivers in the event of damaging the farthest point of a stop signboard. The framework will forward a most extreme speeds expected alarm to forestall emergency breaking. This prompts anticipation of any perilous circumstance.

7.12. Stop Movement Signal Assistant

These types of programs and applications are utilized to caution drivers to not cross any crossing point or generally to prevent any hazardous circumstance from happening. It includes the correspondence among the vehicular sensors and the SDN-RSUs. This type of application advises the driver that different vehicles are closer to the crossing point, so he or she needs to sit tight for quite a while. After the other vehicles cross the junction, the vehicle gets a green signal to cross the junction.

7.13. Left/Right Turn Assistant

The left/right turn assistant is utilized to assist the driver with making the choice to turn left/right if there should be an occurrence of safe circumstance. It assembles the data related the left half of the roads by forwarding a solicitation information to the SDN-based RSUs; the RSUs will send back the information when it is safe to go across the roads.

7.14. Latency-based Routing

SDN-based VANETs adequately acknowledge the inactivity when the blockage on specific routes increase. In such events, various conventional steering conventions (i.e., Border Gateway Protocol (BGP), Interior Gateway Routing Protocol (IGRP), and Routing Information Protocol (RIP)) are pointless as they are not prepared to provide directing choices successfully and rapidly to evolving topologies. This novel SDN-based VANET globally reacts to inertness and lining delay.

On account of the voice traffic, security associated or ongoing programs and applications, which cannot endure postponements and jitter are upheld utilizing the least dormant way [146].

7.15. Lane Change Assistance

Without safety applications and programs like path alteration cautioning, changing of the path might bring about dangerous mishaps. A current path changing framework needs to include numerous difficulties such as the bearing and speed of the vehicles, roads situations, and traffic density. This is not possible for multi-hop path alteration tasks. The SDN-based controller could tackle this issue due to the global point of view about the road organization. The SDN-based controller directs the RSUs to assemble data, for example, the speed of vehicles, thickness, guide, and path direction. At the point when path alteration is mentioned by the vehicle, the controller makes a choice by relying upon the data assembled by the RSUs. DSRC is likewise a basic innovation for utilization of path change help [147].

7.16. Traffic Accident Detection

Based on the velocities and directions of vehicles, the information is gathered from the SDN-based VANETs. Since the accessible information is as indicated by speed and organization of each vehicle, artificial intelligence (AI) computations are utilized to break down the vehicle's conduct and anticipate the mishap that will undoubtedly occur. The Artificial Neural Network (ANN), Support Vector Machine (SVM), and arbitrary backwoods are calculations utilized on the informational index acquired to recognize the typical case from the clumsy case [12].

7.17. Bandwidth Management

Radical augmentation in the utilizations of SDN-based VANETs expands the interest of data transfer capacity necessity. The current system's engineering and highlights do not bolster the dynamic data transfer capacity request. SDN worldview makes accessible the practical transfer speed on-request bandwidth on demand (BWoD) in the profoundly altering condition of the SDN-based VANETs. The OpenFlow based SDN enables buyers to profit the data transmission on-request benefits enabling vehicles to determine their transfer speed prerequisites powerfully. This adaptiveness can be executed utilizing system gadgets, for example, RSUs, switches, and data transmission scheduler introduced on an SDN controller. However, effective designation of data transfer capacity is likewise a test [148].

7.18. Smart Grid Application

SDN-based VANETs can be utilized where the information plane incorporates electric vehicles (EVs) and electrical vehicle supply equipment (EVSE). Attacks on the keen matrix incorporate the system overflowing, the topology harming, and the transmission sticking. At the point when the electric vehicles are essentials to associate with the EVSE, information is forwarded to the SDN controllers so as to follow the flow arranged topology and status of the system. The SDN controller can introduce sending rules, and identify the attacks inferred by abnormal practices in the keen framework application [12].

7.19. Warning in Case of Blind Merge

This component of the application is utilized to forward alerts to vehicles and drivers of the vehicles at the union of roads where perceivability is not great. It is utilized to gather information at the convergence point and produce an outcome on the off chance that it is perilous and the drive needs to be cautioned [11].

7.20. Crossing Road Warning

This component of the programs and applications is utilized to forward the stop signal to the vehicles' drivers if a person on foot is going across the street in the interim. The SDN-based RSUs gather the data from vehicles that are close to the passerby crossing line and confirm if the signal is with a stop sign and the vehicle is moving; it produces admonition information and alarms the vehicle driver to break the vehicle on the grounds that a person on foot is going across the road.

7.21. Emergency Vehicle is Approaching Warning

The focus on this program is to caution the driver of the vehicle if any crisis vehicle is drawing close. This framework includes V2I and V2V correspondence. It cautions the driver of the vehicle on a similar path as the crisis vehicle to clear that road.

7.22. Emergency Vehicle Signal Pre-emption

This application is utilized deliberately to turn the signal light of the particular RSUs to a green light and to turn the other traffic signs to red. This component is used to diminish the waiting time of emergency vehicles at the red light sign.

7.23. Post-Crash Warning

This application highlight is utilized to forward a notice information to every one of the vehicles' drivers in foggy climate on the grounds that there might be an opportunity of a mishap because of substantial mist. This application will communicate something specific containing the most extreme speed limit and the path appropriate for driving the vehicle. This framework utilizes both the V2V and V2I correspondences.

7.24. Sign Extension

This application is utilized to cause the vehicle driver to drive mindfully and confirms the signs that are set on the roadsides. These programs and applications are utilized to supply/delivery some information within the range of approximately 150 to 250 m. These programs and applications are additionally arranged into various classifications.

7.25. Cooperative Forward Collision Warning

This application is utilized to help drivers of vehicles evade mishaps with different vehicles which are going ahead. This type of application includes the V2I and V2V types of correspondence. In the outcome structure, it gives the threat levels ahead.

7.26. Road Condition Warning

Although sensors are utilized to gather the data related to the roads' circumstances, the OBUs evaluate the information received through the sensors and forward the investigation results to the SDN-based RSUs. The SDN-based RSUs forward the ready information to all the vehicles that are in the communication range of the RSUs. This program application shields vehicles from the crisis parts of mishaps that are being brought about by applying the crisis breakdowns of the vehicle. All the SDN-based VANET applications are listed in Figure 27.

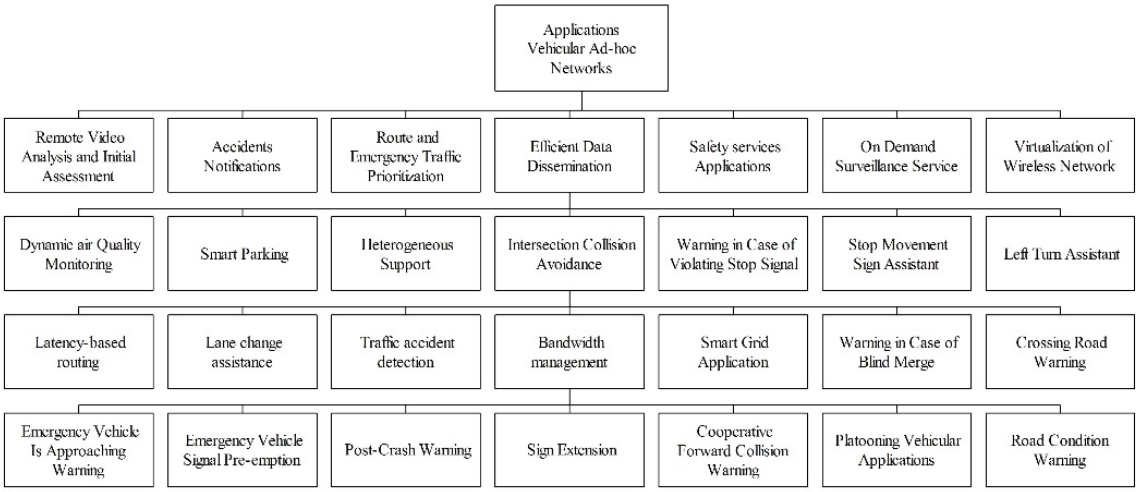

Figure 27. The taxonomy of the SDN-based VANET applications.

8. Future Directions

In virtualized conditions, vehicles will require to communicate with the framework so as to give administrations, for example, traffic the executives, impact shirking, internet gaming, and so on. Thus, this will lead to explicit virtual network functions (VNFs) custom-fitted for systems (as the self-mending virtual capacities: self-association, terminal self-revelation, and portability of the executives) and virtual capacities for the intra and inter vehicle regions (e.g., the virtual OBU work). Then again, so as to screen traffic and stay away from security attacks, organized administrators need to indicate additional security capacities, such as virtual interruption recognition framework, virtual Firewalls, virtual intrusions protection framework, and the DDoS. Various occupants may have distinctive security prerequisites for the streams by considering the security works their streams shall cruise by. Consequently, one ought to think about the arrangement and requesting of these VNFs. In previous studies [80,81], the authors designed various ways to deal with a secured VNF situation in particular to their requesting and launch in rush hour gridlock. This position of the secure capacities all through stream traffic of inhabitants ought to be dynamic so as to adapt to the portability of vehicles and various administrations that they give, and explain the security dangers with respect to the organization and usage of virtual system capacities.

Mobile edge computing (MEC) [149] depends on a virtualization stage and empowers the application to execute at the edge of the system. The environment of the MEC is portrayed through low inactivity, closeness, huge data transfer capacity, and area mindfulness. MEC opens up administrations to buyers and ventures to convey their crucial application. The vehicular system could benefit through edge computing with the goal, for example, to expand vehicular cloud computing (VCC) into a dispersed versatile condition. MEC empowers information and the application to be put near vehicles. In safety applications related to the vehicles, the MEC applications can get information from the applications in the vehicles or RSUs. At that point, this type of application examines the information and spreads alarm cautioning alerts about the roads' environments to vehicles close by on the roads. Utilizing the MEC applications, information is quickly received, enabling the vehicles or drivers to respond right away. MEC can have distinctive VNFs, so as to permit secure interchanges of administrations between vehicles or vehicles to foundations.

Initially, the integrated computer network (ICN) was imagined to tackle the squeezing necessities (e.g., gadget versatility, organize adaptability, access to data, and appropriated content generation) of the present Internet. Notwithstanding, because of its novel preferences that suit the different necessities of various system designs, along with the SDN [59], 5G, and VANETs [55], the utilization of the ICN worldview is imagined in models too. In this perspective, there are a few starter arrangements (i.e., the ICN empowered the SDN-based VANETs) that have been proposed by utilizing a broadly

known ICN occasion, specifically SDN-based VANETs. The correspondence model of SDN-based VANETs replaces the conventional host-driven worldview to another data-driven one [58]. Due to the different advantages that the ICN gives, specialists have researched its use for tending to various VANET problems [55]. For example, Khan et al. [150] proposed a V2I correspondence design that endeavors to convey an RSU foundation for content recovery in SDN-based VANETs. The authors elaborate that the utilization of SDN-based VANETs can give enhancements in VANETs concerning portability of executives, asset utilization, and quicker substance recovery. We accept that the utilization of the SDN in SDN-based VANETs can possibly improve the VANETs, but these areas are still profoundly under-researched and additional studies are needed. Specifically, the new issues and difficulties that emerged from the mix of these three advancements should be completely comprehended and satisfactory answers for the recognized issues ought to be imagined [22].

Giving effective portability for the executives in SDN-based VANETs is imperative to keep a reliable and exact worldwide topology for the SDN controller, which is expected to accurately empower different system administration functions (e.g., directing, security administrations, traffic the board and system virtualization) in the system. In spite of the fact that the SDN gives control which is adaptable and programmable, its relevance to portable systems, (for example, VANETs and 5G) is still in the early stages. Along these lines, new portability strategies, for example, proactive versatility for board calculation usage, and half-and-half control plane changes that the controller can delegate a fractional burden for versatility are required [151]. In SDN-based VANETs, right off the bat the accessibility of the systems' wider topologies at SDN-based controller can anticipate precise versatility of vehicles through novel AI methods like ANN. Furthermore, these forecast outcomes can be utilized by RSUs and base stations over high versatility occasions to gauge the exact estimated communication counts likelihood and start to finish postponement of every vehicle solicitation. Another alternative is to utilize the ICN worldview that bolsters effective information recovery in high versatility situations. ICN handles versatility issues since it encourages information recovery which is autonomous to the real area of the source or maker of the information; consequently, it can be the key empowering influence for the future IoV [152]. However, the ICN engineering likewise exhibits security vulnerabilities, for example, switch reserve harming, Interest flooding, and protection infringement attacks; these dangers should be appropriately examined before its utilization in SDN-based VANETs.

Security is one of the most basic concerns in a vehicular system's administration condition. Throughout the years, various security arrangements have been conceived for VANETs, that principally depend on customary cryptographic plans using open key frameworks and endorsements [55]. By and by, cryptologic-based arrangements are not attainable for vehicular systems since the vehicles are profoundly unique in the environment and disseminated all through the system, the accessibility of a system's administration framework cannot be ensured consistently, and customary cryptography-based arrangements are likewise helpless against insider attacks. Subsequently, trust has been as of late presented as an option for guaranteeing security in vehicular systems [55].

At the point when an attacks focuses on the product characterized systems, it for the most part impacts the SDN-based VANET structures, for example, control plane asset utilization, system topology harming, and rule clashes [153]. In addition, the majority of attacks that are custom fitted against vehicular networks are assiduous on the SDN-based VANET structures; for example, on-board altering, sticking, and application and program based attacks. The attacks as the replay, denial of service (DoS), the Sybil, the sink-gap, the malware injection, security infringement, falsification, and conveyed DoS are persevered in the SDN, VANETs, and SDN-based VANETs, yet with various prerequisites and effect on every innovation [92]. A few threats bargain sending, control, and application layers [58]. Man-in-the-middle attacks between a switch and the controller are brought about by the absence of transport-layer security [59]. Such types of attacks can be moderated by reinforcing a physical system security. Refusal of administration attacks could soak stream tables and cushions. Such attacks are brought about by the inclusion of receptive principles as opposed to embracing a proactive methodology. They can be averted by utilizing different controllers. Different threats may originate

from disseminated multi-controllers, applications, unlawful access, or clashes of security rules or arrangements. In spite of existing arrangements, high portability requires security components that can perform continuous validation. In addition, dormancy can cause traffic jams that hinder the acknowledgment of SDN-based VANETs. This ongoing element builds trouble in fortifying security [59,60].

The attacks, for example, evolving path, merger, rushing or braking, diverting traffic or altering course could be done. In SDN-based VANET models, the controller can introduce the suitable principles identified with the increasing speed/deceleration, merger/parting, and changing path considering contributions from traffic conditions and occasions in the streets. At that point a controller could gather data on the roads' status and bizarre vehicle conduct by utilizing traded information. Specifically, components, for example, the ones conveyed in another study [84] can be effective to distinguish a rowdiness in platooning SDN-based VANET applications. So as to guarantee better system usage, the RSU controllers in the SDN-based VANET applications and programs have the job to educate the detachment chief to set various limitations. These limitations incorporate the booking approach of information, increasing speed, or braking. Moreover, SDN-based RSU controllers could recognize the attacks, for example, sticking, replay, or the attacks focusing on the administration conventions. These types of the attacks instigate moves, for example, parting, consolidating, or path evolving. In SDN-based VANET based structures, an attacker could noxiously inject a product that imitates itself by the various SDN-based controllers and vehicles and the switches. The remote attacker by Bluetooth or cell correspondences enables the aggressor to assume responsibility for the vehicle. One of the weakness disorders lives on the absence of the information verification of the controller region position.

The versatility the executives in VANETs builds the delay in disseminating the information where the handover techniques are not appropriately actualized. To this, SDN-based VANETs with haze figuring would permit competition of the prerequisites of the lowest information dissemination delays by receiving a cross breed handover conspire, improving radio asset distribution by Markov choice procedure [154]. However, wasteful controls for the highest portability that matter, flimsy remote channels for SDN put together VANETs, and inactivity with respect to the appropriation of directions from the controllers and the interworking break by the heterogeneous systems between continuous VANETs make it difficult to fight through SDN-based VANETs. Furthermore, arrange edge computing and NFV [155] in SDN-based VANETs present potential research openings. Indeed, SDN permits employable system edge computing in unique topologies. NFV by the utilization of the hypervisor has the assignment of altering OpenFlow rules in the manner to empower the heterogeneous system interworking. The framework investigation of SDN-based VANET systems distinguishes parts, structures, and conventions straightforwardly connected to the SDN-based VANET. There are six design frameworks of SDN-based IoV developed in writing: SDN-based VANETs [22], SDN-based directing [156], SDN-based VANETs [157], SDN-based cloud-fog/versatile (fog/edge) processing, and programming characterized VANETs [158]. A complete investigation of SDN-based VANETs, its advantages and administrations are depicted elsewhere [59]. Albeit six frameworks of SDN-based VANET designs are as of now executed and recreated, framework examination gives bits of knowledge to important parts, structures, conventions, and reenactment devices to be considered before giving an answer model to VANET challenges.

Indeed, we can list a couple of SDN-based VANET frameworks' examination as discussed above: the situation of the SDN controller, correspondence controls VANETs or mobile network based, nearby information on encompassing hubs by means of reference point or geo-communicate messages [39,42], arrange test system devices, for example, Mininet-WiFi, hint of overhead communication among the vehicles, and the SDN-based controllers. Far reaching reviews [41,43] do not have similar reports on the framework examination of the existing SDN-based VANETs to call attention to SDN-based VANET parts, designs, and calculations explored to handle SDN-based VANET downsides. Arif et al. [23] explored SDN-based VANET designs to distinguish their advantages and difficulties against the VANETs with respect to correspondence [58] and security [22]. Inside the current SDN-based VANET

arrangements, innovation for the SDN-based controllers and execution device for OpenFlow rules convention have been developed, yet a far reaching study on SDN put together VANET designs will give the necessary bits of knowledge on the parts required for further improvements. Since the framework examination of SDN-based VANET frameworks give key empowering innovations to exploring SDN-based VANET problems and issues, the arrangement models developed in the execution based framework investigation in SDN-based VANETs represents potential research openings towards proficient SDN-based VANETs that could permit an enormous number of new VANET applications. As affirmed by the huge research output which we talked about in our paper, the academia and the industry world are moving forward to build the structure and setup of the new SDN-based VANET designs. The quick push toward this path is after the effect of rising and creative applications (5G, IoV, ITS) of VANETs which have stringent prerequisites about power, adaptability, inertness (i.e., time imperatives for basic continuous basic leadership), security, and protection. Scientists' imagine the effective arrangement of these applications by utilizing the SDN-based VANETs combined with other new innovations, for example, versatile edge/haze registering, SDN-based VANETs, and NFV.

Although different designs are developed in the literature to enhance the correspondence of unwavering quality and security in the VANETs, thorough examination to assess the adequacy of the structures remains a popular issue. Specifically, the novel privacy and security susceptibilities that emerge because of the joining of the novel innovations, (e.g., NFV, SDN, and cloud/fog and the edge processing) by the current VANETs ought to be painstakingly contemplated. For example, scientists ought not just to provide the advantages of utilizing SDNs to enhance the VANETs design, however, the novel problems (e.g., administration inertness, versatility, and verifying the SDN-based controller) which are inalienable to the SDN and currently disappoint the presentation of the SDN-based VANETs, ought to likewise be researched and talked about. In addition, it is essential to take a gander at how unique, continuous change, fast on-request development (adaptability), and joining of administration setting will assume key jobs in empowering fruitful arrangement and maintaining a strategic distance from execution permeability holes in SDN-based VANETs. In the ongoing future, VANETs engineering will continually be developing to fulfil the quickly developing prerequisites of its new applications. Along these lines, we currently present hardly any exploration bearings that could be abused toward this path.

SDN and car frameworks are key empowering influences for 5G frameworks. This will obstruct the applications described by the individual or multi-occupancy. The deviating 5G and V2X administrations range from a solitary mechanized vehicle in smart cities, to upgraded constant route frameworks ready. In conventional systems, various administrations can be bolstered in similar engineering and worked without versatility as a main priority. In addition, these administrations share similar assets and are prepared by a similar system component. The idea of system cuts has risen as a novel innovation that segregates arrange capacities and assets. The SDN-based controller arranges the distinctive VNF and the physical systems works in a single cut. Due to the highlights of V2V or V2I, edge computing could be used for vehicular applications, self-driving, security and privacy, and for efficient information for drivers without delays. In addition, an adversary may acquire abilities to dispatch the attacks to changes in data so as to adjust the setup of other clients' change occurrence, trading off a system work, or even end a change. Consequently, this will uncover the administrations and systems to expose and remove. We distinguish here the necessity to explore the security necessities and the security answers for arrange V2X edge computing. We should also make reference to which significant endeavors are as yet required from scientists and businesses to plan a total way to deal with empowered secure edge computing in 5G vertical areas, for example, car frameworks.

9. Conclusions

The connected vehicles in the IoV are advancing in a highly powerful and complex condition that provides driver choices in basic circumstances. Specifically, VANETs are generally acknowledged as a foundation for enabling the security, privacy, safety, traffic, and infotainment based services

and applications for drivers, travelers, and people walking on the roads in the IoV. In reality, these profoundly portable systems are relied upon to add to road security and safety by giving the appropriate data to the drivers on the potential threats inside their environment. In any case, a VANET is certainly not a benign domain, inferable from its immense working region and the hidden advancements used to convey basic data. As far as growing the vehicles on the roads, it is difficult to manage the data and the security threats produced by the vehicles and the adversaries by the traditional VANETs, so there is a need for a platform that manages all the difficulties in the traditional VANETS. The best solution is to utilize the SDN in the VANETs.

The SDN-based VANETs are a system innovation dependent on the partition of information and control and application planes. This paper for the most part centers around examining certain literature that focuses on characterizing existing SDN-based VANETs dependent on their demonstration and execution. We additionally discuss the SDN-based ITS, and SDN-based VANETs in detail. Security is one of the basic concerns in a vehicular system. Throughout the years, various security arrangements has been conceived for VANETs that principally depend on customary cryptographic plans using open key frameworks and endorsements. Eventually, cryptologic based solutions are not attainable for the vehicular systems since the vehicles are profoundly unique in their environment and are disseminated all through the system. The accessibility of a systems administration framework cannot be ensured consistently, and customary cryptography-based arrangements are likewise helpless against insider attacks.

Subsequently, trust has been as of late presented as an option for guaranteeing security in the vehicular systems. We furthermore examined the security attacks alongside the taxonomy of the security measure in the SDN, and every single imaginable attack with models that would occur in SDN-based VANETs. What is more, this work gives a brief overview of the present investigations available in the literature on applications in support of SDN-based VANETs. The key thoughts of SDN-based VANETs and their administrations and applications were likewise presented. We also discussed the overview of the challenges that are available in the SDN-based VANET literature. In this paper we explain the details of the security attacks in future SDN-based VANETs. Where SDN-based VANETs provide some benefits in terms of applications and services, some SDN-based VANETs have important challenges which need to be solved. In this study we discuss and elaborate the challenges, along with the applications. At the end, we also discussed some guidelines for future research directions.

Author Contributions: M.A., writing, original draft preparation, designing, analysis, editing. O.G., A.B., and P.T., review, editing, investigation. V.E.B., help in methodology investigation, and content verification. G.W., supervision, review, content verification, editing, resources and funding acquisition. J.C., review and editing the content. All the authors also contributed in writing, reviewing, and structured the work. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Natural Science Foundation of China under Grant 61632009 and Grant 61472451, in part by the Guangdong Provincial Natural Science Foundation under Grant 2017A030308006, and in part by the High-Level Talents Program of Higher Education in Guangdong Province under Grant 2016ZJ01.

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

References

1. Pérez, M.Á.B.; Losada, N.Y.S.; Sánchez, E.R.; Gaona, G.M. State of the art in Software Defined Networking (SDN). *Visión Electrónica* **2019**, *13*, 178–194. [CrossRef]
2. Schafer, V.; Cooper, S.; Paloque-Bergès, C. Back to the roots of ARPANET and Internet history with Alexandre Serres. *Internet Hist.* **2019**, *3*, 51–67. [CrossRef]
3. Karmakar, K.K.; Varadharajan, V.; Tupakula, U. Mitigating attacks in software defined networks. *Clust. Comput.* **2019**, *22*, 1143–1157. [CrossRef]
4. Balmakhtar, M.; Rajagopal, A.; Persson, C.J. Software Defined Network (SDN) Proxy Correlation Index (PCI) Information Distribution across an SDN Data-Plane. U.S. Patent 10,313,193, 4 June 2019.

5. Hoang, H.D.; Pham, V.-H. A Security-Enhanced Monitoring System for Northbound Interface in SDN using Blockchain. In Proceedings of the Tenth International Symposium on Information and Communication Technology (SoICT), Hanoi-Ha long Bay, Veitnam, 4–6 December 2019; pp. 197–204.
6. Sen, S.; Gupta, K.D.; Ahsan, M.M. Leveraging Machine Learning Approach to Setup Software-Defined Network (SDN) Controller Rules during DDoS Attack. In Proceedings of the International Joint Conference on Computational Intelligence, Singapore, 4 July 2019; pp. 49–60.
7. Bhatia, J.; Dave, R.; Bhayani, H.; Tanwar, S.; Nayyar, A. SDN based real-time urban traffic analysis in VANET environment. *Comput. Commun.* **2020**, *149*, 162–175. [CrossRef]
8. You, Z.; Cheng, G.; Wang, Y.; Chen, P.; Chen, S. Cross-Layer and SDN Based Routing Scheme for P2P Communication in Vehicular Ad-Hoc Networks. *Appl. Sci.* **2019**, *9*, 4734. [CrossRef]
9. Srinivasagopalan, P. *Fernweh Travelogues in a Self-Driving Car*; State University of New York at Buffalo: Buffalo, NY, USA, 2017.
10. Nehra, A.; Tripathi, M.; Gaur, M.S. 'Global view' in SDN: Existing implementation, vulnerabilities & threats. In Proceedings of the 10th International Conference on Security of Information and Networks, Jaipur, India, 13–15 October 2017; pp. 303–306.
11. Shafiq, H.; Rehman, R.A.; Kim, B.-S. Services and security threats in sdn based VANETs: A survey. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 1–14. [CrossRef]
12. Di Maio, A.; Palattella, M.; Soua, R.; Lamorte, L.; Vilajosana, X.; Alonso-Zarate, J.; Engel, T. Enabling SDN in VANETs: What is the impact on security? *Sensors* **2016**, *16*, 2077. [CrossRef]
13. Truong, N.B.; Lee, G.M.; Ghamri-Doudane, Y. Software defined networking-based vehicular adhoc network with fog computing. In Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), Ottawa, ON, Canada, 11–15 May 2015; pp. 1202–1207.
14. Chahal, M.; Harit, S.; Mishra, K.K.; Sangaiah, A.K.; Zheng, Z. A survey on software-defined networking in vehicular ad hoc networks: Challenges, applications and use cases. *Sustain. Cities Soc.* **2017**, *35*, 830–840. [CrossRef]
15. Boucetta, S.I.; Johanyák, C.; Pokorádi, L.K. Survey on software defined VANETs. *Gradus* **2017**, *4*, 272–283.
16. Barakabitze, A.A.; Ahmad, A.; Mijumbi, R.; Hines, A. 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges. *Comput. Netw.* **2020**, *167*, 106984. [CrossRef]
17. Papavassiliou, S. Software Defined Networking (SDN) and Network Function Virtualization (NFV). *Future Internet* **2020**, *12*, 7. [CrossRef]
18. Qu, K.; Zhuang, W.; Ye, Q.; Shen, X.; Li, X.; Rao, J. Dynamic Flow Migration for Embedded Services in SDN/NFV-Enabled 5G Core Networks. *IEEE Trans. Commun.* **2020**, *68*, 2393–2408. [CrossRef]
19. Kazmi, A.; Khan, M.A.; Bashir, F.; Saqib, N.A.; Alam, M.; Alam, M. Model Driven Architecture for Decentralized Software Defined VANETs. In Proceedings of the International Conference on Future Intelligent Vehicular Technologies, Porto, Portugal, 15 September 2016; pp. 46–56.
20. Soua, A.; Tohme, S. Multi-level SDN with vehicles as fog computing infrastructures: A new integrated architecture for 5G-VANETs. In Proceedings of the 2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), Paris, France, 19–22 February 2018; pp. 1–8.
21. Kalinin, M.; Krundyshev, V.; Zegzhda, P.; Belenko, V. Network security architectures for VANET. In Proceedings of the 10th International Conference on Security of Information and Networks, Jaipur, India, 13–15 October 2017; pp. 73–79.
22. Arif, M.; Wang, G.; Wang, T.; Peng, T. SDN based secure VANETs communication with fog computing. In Proceedings of the International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, Melbourne, NSW, Australia, 11 September 2018; pp. 46–59.
23. Gaur, K.; Grover, J. Exploring VANET Using Edge Computing and SDN. In Proceedings of the 2019 Second International Conference on Advanced Computational and Communication Paradigms (ICACCP), Gangtok, India, 25 February 2019; pp. 1–4.
24. Trivedi, H.; Tanwar, S.; Thakkar, P. Software Defined Network-Based Vehicular Adhoc Networks for Intelligent Transportation System: Recent Advances and Future Challenges. In Proceedings of the International Conference on Futuristic Trends in Network and Communication Technologies, Chandigarh, India, 22 November 2019; pp. 325–337.

25. Din, S.; Paul, A.; Ahmad, A.; Ahmed, S.H.; Jeon, G.; Rawat, D.B. Hierarchical architecture for 5g based software-defined intelligent transportation system. In Proceedings of the IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Honolulu, HI, USA, 15 April 2018; pp. 462–467.
26. Hasan, K.F.; Kaur, T.; Hasan, M.; Feng, Y. Cognitive Internet of Vehicles: Motivation, Layered Architecture and Security Issues. *arXiv* **2019**, arXiv:1912.03356.
27. Dai, P.; Liu, K.; Wu, X.; Yu, Z.; Xing, H.; Lee, V.C.S. Cooperative Temporal Data Dissemination in SDN Based Heterogeneous Vehicular Networks. *IEEE Internet Things J.* **2018**, *6*, 72–83. [CrossRef]
28. Sheikh, M.S.; Liang, J.; Wang, W. A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs). *Sensors* **2019**, *19*, 3589. [CrossRef] [PubMed]
29. Mahmood, A.; Zhang, W.E.; Sheng, Q.Z. Software-Defined Heterogeneous Vehicular Networking: The Architectural Design and Open Challenges. *Future Internet* **2019**, *11*, 70. [CrossRef]
30. Rezaee, M.; Moghaddam, M.H.Y. SDN based Quality of Service Networking for Wide Area Measurement System. *IEEE Trans. Ind. Inform.* **2019**, *16*, 3018–3028. [CrossRef]
31. Tello-Oquendo, L.; Akyildiz, I.F.; Lin, S.-C.; Pla, V. Sdn based architecture for providing reliable internet of things connectivity in 5g systems. In Proceedings of the 2018 17th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net), Capri, Italy, 22 June 2018; pp. 1–8.
32. Raza, N.; Jabbar, S.; Han, J.; Han, K. Social Vehicle-to-Everything (V2X) communication model for intelligent transportation systems based on 5G scenario. In Proceedings of the 2nd International Conference on Future Networks and Distributed Systems (ICFNDS), Amman, Jordan, 26–27 June 2018; pp. 1–8.
33. Li, B.; Zhao, X.; Han, S.; Chen, Z. New sdn based architecture for integrated vehicular cloud computing networking. In Proceedings of the 2018 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT), Tangier, Morocco, 20 June 2018; pp. 1–4.
34. Han, R.; Shi, J.; Banoori, F.; Shen, W. A Novel Next-Hop Selection Scheme Based on GPSR in VANETs. In Proceedings of the International Conference on Internet of Things as a Service, Xian, China, 16 November 2019; pp. 101–110.
35. Buinevich, M.; Vladyko, A. Forecasting Issues of Wireless Communication Networks Cyber Resilience for an Intelligent Transportation System: An Overview of Cyber Attacks. *Information* **2019**, *10*, 27. [CrossRef]
36. Cho, W.; Han, K.-S.; Choi, H.K.; Oh, H.S. Realization of anti-collision warning application using V2V communication. In Proceedings of the 2009 IEEE Vehicular Networking Conference (VNC), Tokyo, Japan, 28 October 2009; pp. 1–5.
37. Yousefi, S.; Mousavi, M.S.; Fathy, M. Vehicular ad hoc networks (VANETs): Challenges and perspectives. In Proceedings of the 2006 6th International Conference on ITS Telecommunications, Chengdu, China, 21 June 2006; pp. 761–766.
38. Arif, M.; Wang, G.; Peng, T. Track me if you can? Query Based Dual Location Privacy in VANETs for V2V and V2I. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1 August 2018; pp. 1091–1096.
39. Arif, M.; Alam, K.A.; Hussain, M. Crime Mining: A Comprehensive Survey. *Int. J. u- e-Serv. Sci. Technol.* **2015**, *8*, 357–364. [CrossRef]
40. Ku, I.; Lu, Y.; Gerla, M.; Gomes, R.L.; Ongaro, F.; Cerqueira, E. Towards software-defined VANET: Architecture and services. In Proceedings of the Med-Hoc-Net, Piran, Slovenia, 2 June 2014; pp. 103–110.
41. Liu, Y.-C.; Chen, C.; Chakraborty, S. A software defined network architecture for geobroadcast in VANETs. In Proceedings of the 2015 IEEE International Conference on Communications (ICC), London, UK, 2 June 2015; pp. 6559–6564.
42. Kazmi, A.; Khan, M.A.; Akram, M.U. DeVANET: Decentralized software-defined VANET architecture. In Proceedings of the 2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW), Berlin, Germany, 4 April 2016; pp. 42–47.
43. Soua, R.; Kalogeiton, E.; Manzo, G.; Duarte, J.M.; Palattella, M.R.; Di Maio, A.; Braun, T.; Engel, T.; Villas, L.A.; Rizzo, G.A. SDN coordination for CCN and FC content dissemination in VANETs. In *Ad Hoc Networks*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 221–233.
44. Todorova, M.S.; Todorova, S.T. DDoS Attack Detection in SDN based VANET Architectures. Master's Thesis, Aalborg University, Aalborg, Denmark, 2016.

45. Venkatramana, D.K.N.; Srikantaiah, S.B.; Moodabidri, J. SCGRP: SDN-enabled connectivity-aware geographical routing protocol of VANETs for urban environment. *IET Netw.* **2017**, *6*, 102–111. [CrossRef]
46. Thun, S.; Saivichit, C. Performance improvement of vehicular ad hoc network environment by cooperation between sdn/openflow controller and ieee 802.11 p. *J. Telecommun. Electron. Comput. Eng. (JTEC)* **2017**, *9*, 95–99.
47. Borcoci, E.; Ambarus, T.; Vochin, M. Distributed control plane optimization in sdn-fog vanet. *ICN* **2017**, *2017*, 135.
48. Gao, J.; Agyekum, K.O.-B.O.; Sifah, E.B.; Acheampong, K.N.; Xia, Q.; Du, X.; Guizani, M.; Xia, H. A Blockchain-SDN enabled Internet of Vehicles Environment for Fog Computing and 5G Networks. *IEEE Internet Things J.* **2019**. [CrossRef]
49. Duan, X. Software-defined Networking Enabled Resource Management and Security Provisioning in 5G Heterogeneous Networks. Ph.D. Thesis, The University of Western Ontario, Ontario, ON, Canada, 2017.
50. Cox, J.H.; Chung, J.; Donovan, S.; Ivey, J.; Clark, R.J.; Riley, G.; Owen, H.L. Advancing software-defined networks: A survey. *IEEE Access* **2017**, *5*, 25487–25526. [CrossRef]
51. Peng, H.; Ye, Q.; Shen, X.S. SDN based resource management for autonomous vehicular networks: A multi-access edge computing approach. *IEEE Wirel. Commun.* **2019**, *26*, 156–162. [CrossRef]
52. Camacho, F.; Cárdenas, C.; Muñoz, D. Emerging technologies and research challenges for intelligent transportation systems: 5G, HetNets, and SDN. *Int. J. Interact. Des. Manuf. (IJIDeM)* **2018**, *12*, 327–335. [CrossRef]
53. Chekired, D.A.; Togou, M.A.; Khoukhi, L.; Ksentini, A. 5G-slicing-enabled scalable SDN core network: Toward an ultra-low latency of autonomous driving service. *IEEE J. Sel. Areas Commun.* **2019**, *37*, 1769–1782. [CrossRef]
54. Simsek, M.; Aijaz, A.; Dohler, M.; Sachs, J.; Fettweis, G. The 5g-enabled tactile internet: Applications, requirements, and architecture. In Proceedings of the 2016 IEEE Wireless Communications and Networking Conference, Doha, Qatar, 3 April 2016; pp. 1–6.
55. Arif, M.; Wang, G.; Bhuiyan, M.Z.A.; Wang, T.; Chen, J. A survey on security attacks in VANETs: Communication, applications and challenges. *Veh. Commun.* **2019**, *19*, 100179. [CrossRef]
56. Hussein, A.; Elhajj, I.H.; Chehab, A.; Kayssi, A. SDN VANETs in 5G: An architecture for resilient security services. In Proceedings of the 2017 Fourth International Conference on Software Defined Systems (SDS), Valencia, Spain, 8 May 2017; pp. 67–74.
57. Arif, M.; Dar, A.R. Survey on Fraud Detection Techniques Using Data Mining. *Int. J. u- e-Serv. Sci. Technol.* **2015**, *8*, 165–170. [CrossRef]
58. Arif, M.; Wang, G.; Balas, V.E. Secure VANETs: Trusted communication scheme between vehicles and infrastructure based on fog computing. *Stud. Inform. Control* **2018**, *27*, 235–246. [CrossRef]
59. Jaballah, W.B.; Conti, M.; Lal, C. A Survey on Software-Defined VANETs: Benefits, Challenges, and Future Directions. *arXiv* **2019**, arXiv:1904.04577.
60. Arif, M.; Wang, G.; Chen, S. Deep learning with non-parametric regression model for traffic flow prediction. In Proceedings of the 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), Athens, Greece, 12 August 2018; pp. 681–688.
61. Yan, Q.; Yu, F.R.; Gong, Q.; Li, J. Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. *IEEE Commun. Surv. Tutor.* **2015**, *18*, 602–622. [CrossRef]
62. Shin, S.W.; Gu, G. Attacking software-defined networks: A first feasibility study. In Proceedings of the ACM SIGCOMM workshop on Hot topics in software defined networking, Hong Kong, China, 16 August 2013; pp. 165–166.
63. Cabaj, K.; Wytrebowicz, J.; Kuklinski, S.; Radziszewski, P.; Dinh, K.T. SDN Architecture Impact on Network Security. In Proceedings of the FedCSIS position papers, Warsaw, Poland, 7 September 2014; pp. 143–148.
64. Hizver, J. Taxonomic modeling of security threats in software defined networking. In Proceedings of the BlackHat Conference, Las Vegas, NV, USA, 5 August 2015; pp. 1–16.
65. Ulema, M. Vulnerabilities and opportunities in SDN, NFV, and NGSON. *IEEE CQR* **2014**, *2014*, 24.

66. Arbettu, R.K.; Khondoker, R.; Bayarou, K.; Weber, F. Security analysis of OpenDaylight, ONOS, Rosemary and Ryu SDN controllers. In Proceedings of the 2016 17th International telecommunications network strategy and planning symposium (Networks), Montreal, QC, Canada, 26 September 2016; pp. 37–44.
67. He, Z.; Cao, J.; Liu, X. SDVN: Enabling rapid network innovation for heterogeneous vehicular communication. *IEEE Netw.* **2016**, *30*, 10–15. [CrossRef]
68. Correia, S.; Boukerche, A.; Meneguette, R.I. An architecture for hierarchical software-defined vehicular networks. *IEEE Commun. Mag.* **2017**, *55*, 80–86. [CrossRef]
69. Lai, C.-F.; Chang, Y.-C.; Chao, H.-C.; Hossain, M.S.; Ghoneim, A. A buffer-aware QoS streaming approach for SDN-enabled 5G vehicular networks. *IEEE Commun. Mag.* **2017**, *55*, 68–73. [CrossRef]
70. Khan, A.A.; Abolhasan, M.; Ni, W. 5G next generation VANETs using SDN and fog computing framework. In Proceedings of the 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 12 January 2018; pp. 1–6.
71. Wang, H.; Xu, L.; Gu, G. Floodguard: A dos attack prevention extension in software-defined networks. In Proceedings of the 2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Rio de Janeiro, Brazil, 22 June 2015; pp. 239–250.
72. Wei, L.; Fung, C. FlowRanger: A request prioritizing algorithm for controller DoS attacks in Software Defined Networks. In Proceedings of the 2015 IEEE International Conference on Communications (ICC), London, UK, 8 June 2015; pp. 5254–5259.
73. Ambrosin, M.; Conti, M.; De Gaspari, F.; Poovendran, R. Lineswitch: Tackling control plane saturation attacks in software-defined networking. *IEEE/ACM Trans. Netw.* **2016**, *25*, 1206–1219. [CrossRef]
74. Shang, G.; Zhe, P.; Bin, X.; Aiqun, H.; Kui, R. FloodDefender: Protecting data and control plane resources under SDN-aimed DoS attacks. In Proceedings of the IEEE Conference on Computer Communications (INFOCOM), Atlanta, GA, USA, 1 May 2017; pp. 1–9.
75. Hong, S.; Xu, L.; Wang, H.; Gu, G. Poisoning Network Visibility in Software-Defined Networks: New Attacks and Countermeasures. In Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, 8 November 2015; pp. 8–11.
76. Aujla, G.S.; Chaudhary, R.; Kumar, N.; Rodrigues, J.J.; Vinel, A. Data offloading in 5g-enabled software-defined vehicular networks: A stackelberg-game-based approach. *IEEE Commun. Mag.* **2017**, *55*, 100–108. [CrossRef]
77. Dhawan, M.; Poddar, R.; Mahajan, K.; Mann, V. SPHINX: Detecting Security Attacks in Software-Defined Networks. In Proceedings of the Network and Distributed System Security (NDSS), San Diego, CA, USA, 8 November 2015; pp. 8–11.
78. Khelifi, H.; Luo, S.; Nour, B.; Shah, S.C. Security and Privacy Issues in Vehicular Named Data Networks: An Overview. *Mob. Inf. Syst.* **2018**, *2018*, 1–11. [CrossRef]
79. Alrehan, A.M.; Alhaidari, F.A. Machine Learning Techniques to Detect DDoS Attacks on VANET System: A Survey. In Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 1 May 2019; pp. 1–6.
80. Hussain, R.; Hussain, F.; Zeadally, S. Integration of VANET and 5G Security: A review of design and implementation issues. *Future Gener. Comput. Syst.* **2019**, *101*, 843–864. [CrossRef]
81. Shin, S.W.; Porras, P.; Yegneswara, V.; Fong, M.; Gu, G.; Tyson, M. Fresco: Modular composable security services for software-defined networks. In Proceedings of the 20th Annual Network and Distributed System Security (NDSS), San Diego, CA, USA, 24 February 2013; pp. 1–16.
82. Porras, P.; Shin, S.; Yegneswaran, V.; Fong, M.; Tyson, M.; Gu, G. A security enforcement kernel for OpenFlow networks. In Proceedings of the first workshop on Hot topics in software defined networks, Helsinki, Finland, 13–17 August 2012; pp. 121–126.
83. He, D.; Zeadally, S.; Xu, B.; Huang, X. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2681–2691. [CrossRef]
84. Lin, X.; Sun, X.; Ho, P.-H.; Shen, X. GSIS: A secure and privacy-preserving protocol for vehicular communications. *IEEE Trans. Veh. Technol.* **2007**, *56*, 3442–3456.
85. Zhang, C.; Lu, R.; Ho, P.-H.; Chen, A. A location privacy preserving authentication scheme in vehicular networks. In Proceedings of the 2008 IEEE Wireless Communications and Networking Conference, Las Vegas, NV, USA, 31 March 2008; pp. 2543–2548.

86. Wu, Z.; Wei, Q.; Ren, K.; Wang, Q. A Dynamic Defense Using Client Puzzle for Identity-Forgery Attack on the South-Bound of Software Defined Networks. *KSII Trans. Internet Inf. Syst.* **2017**, *11*, 846–864.
87. Abu-Ghazaleh, N.; Kang, K.-D.; Liu, K. Towards resilient geographic routing in wsns. In Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks, Montreal, QC, Canada, October 2005; pp. 71–78.
88. Capkun, S.; Hubaux, J.-P. Secure positioning in wireless networks. *IEEE J. Sel. Areas Commun.* **2006**, *24*, 221–232. [CrossRef]
89. Leinmüller, T.; Maihöfer, C.; Schoch, E.; Kargl, F. Improved security in geographic ad hoc routing through autonomous position verification. In Proceedings of the third international workshop on Vehicular ad hoc networks, Los Angeles, CA, USA, 29 September 2006; pp. 57–66.
90. Jaballah, W.B.; Conti, M.; Mosbah, M.; Palazzi, C.E. Fast and secure multihop broadcast solutions for intervehicular communication. *IEEE Trans. Intell. Transp. Syst.* **2013**, *15*, 433–450. [CrossRef]
91. Li, Z.; Chigan, C.; Wong, D. AWF-NA: A complete solution for tampered packet detection in VANETs. In Proceedings of the IEEE GLOBECOM 2008IEEE Global Telecommunications Conference, New Orleans, LO, USA, 30 November 2008; pp. 1–6.
92. Kalinin, M.O.; Krundyshev, V.; Semianov, P. Architectures for building secure vehicular networks based on SDN technology. *Autom. Control Comput. Sci.* **2017**, *51*, 907–914. [CrossRef]
93. Waraich, P.S.; Batra, N. Prevention of denial of service attack over vehicle ad hoc networks using quick response table. In Proceedings of the 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, India, 21 September 2017; pp. 586–591.
94. Nikam, A.S.; Sarawagi, A. Security over Wormhole Attack in VANET Network System. *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* **2017**, *7*, 196–200. [CrossRef]
95. Garg, S.; Kaur, K.; Kaddoum, G.; Ahmed, S.H.; Jayakody, D.N.K. SDN based Secure and Privacy-preserving Scheme for Vehicular Networks: A 5G Perspective. *IEEE Trans. Veh. Technol.* **2019**, *68*, 8421–8434. [CrossRef]
96. Stolyarova, E.S.; Shiryaev, D.M.; Vladyko, A.G.; Buinevich, M.V. VANET/ITS cybersecurity threats: Analysis, categorization and forecasting. In Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow, Russia, 29 January 2018; pp. 136–141.
97. Al-Kahtani, M.S. Survey on security attacks in Vehicular Ad hoc Networks (VANETs). In Proceedings of the 2012 6th International Conference on Signal Processing and Communication Systems, Gold Coast, Australia, 12 December 2012; pp. 1–9.
98. Chowdhury, M.; Gawande, A.; Wang, L. Anonymous authentication and pseudonym-renewal for VANET in NDN. In Proceedings of the 4th ACM Conference on Information-Centric Networking, Berlin, Germany, 26–28 September 2017; pp. 222–223.
99. Chowdhury, M.; Gawande, A.; Wang, L. Secure information sharing among autonomous vehicles in NDN. In Proceedings of the 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI), Pittsburgh, PA, USA, 18 April 2018; pp. 15–26.
100. Bechler, M.; Wolf, L. Mobility management for vehicular ad hoc networks. In Proceedings of the 2005 IEEE 61st Vehicular Technology Conference, Stockholm, Sweden, 30 May 2005; pp. 2294–2298.
101. Lee, J.M.; Yu, M.J.; Yoo, Y.H.; Choi, S.G. A new scheme of global mobility management for inter-VANETs handover of vehicles in V2V/V2I network environments. In Proceedings of the 2008 Fourth International Conference on Networked Computing and Advanced Information Management, Gyeongju, Korea, 2 September 2008; pp. 114–119.
102. Meneguette, R.I.; Bittencourt, L.F.; Madeira, E.R.M. A seamless flow mobility management architecture for vehicular communication networks. *J. Commun. Netw.* **2013**, *15*, 207–216. [CrossRef]
103. Heinonen, J.; Partti, T.; Kallio, M.; Lappalainen, K.; Flinck, H.; Hillo, J. Dynamic tunnel switching for SDN based cellular core networks. In Proceedings of the 4th workshop on All things cellular: Operations, applications, & challenges, Chicago, IL, USA, 22 August 2014; pp. 27–32.
104. Yoshida, Y.; Maruta, A.; Kitayama, K.-i.; Nishihara, M.; Tanaka, T.; Takahara, T.; Rasmussen, J.C.; Yoshikane, N.; Tsuritani, T.; Morita, I. SDN based network orchestration of variable-capacity optical packet switching network over programmable flexi-grid elastic optical path network. *J. Lightwave Technol.* **2014**, *33*, 609–617. [CrossRef]

105. Liu, J.; Xu, X.; Chen, W.; Hou, Y. QoS guaranteed resource allocation with content caching in SDN enabled mobile networks. In Proceedings of the 2016 IEEE/CIC International Conference on Communications in China (ICCC Workshops), Chengdu, China, 27 July 2017; pp. 1–6.
106. Rizzo, G.; Palattella, M.R.; Braun, T.; Engel, T. Content and context aware strategies for QoS support in VANETs. In Proceedings of the 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), Crans-Montana, Switzerland, 25 March 2016; pp. 717–723.
107. Kirichek, R.; Vladyko, A.; Paramonov, A.; Koucheryavy, A. Software-defined architecture for flying ubiquitous sensor networking. In Proceedings of the 2017 19th International Conference on Advanced Communication Technology (ICACT), Bongpyeong, Korea, 19 February 2017; pp. 158–162.
108. Lee, C.S.; Lee, G.M.; Rhee, W.S. Standardization and challenges of smart ubiquitous networks in ITU-T. *IEEE Commun. Mag.* **2013**, *51*, 102–110. [CrossRef]
109. Lacoste, M.; Armand, D.; L'Hereec, F.; Prévost, F.; Rafflée, Y.; Roché, S. Software-Defined Vehicular Networking Security: Threats and Security Opportunities for 5G. Available online: https://www.cesar-conference.org/wp-content/uploads/2019/10/20191119_J1_090_M-LACOSTE_Software_Defined_Vehicular_Network.pdf (accessed on 5 May 2020).
110. Zhu, M.; Cao, J.; Pang, D.; He, Z.; Xu, M. SDN based routing for efficient message propagation in VANET. In Proceedings of the International Conference on Wireless Algorithms, Systems, and Applications, Honolulu, HI, USA, 24 June 2019; pp. 788–797.
111. Dong, B.; Wu, W.; Yang, Z.; Li, J. Software defined networking based on-demand routing protocol in vehicle ad hoc networks. In Proceedings of the 2016 12th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN), Hefei, China, 16 December 2016; pp. 207–213.
112. Kalinin, M.; Zegzhda, P.; Zegzhda, D.; Vasiliev, Y.; Belenko, V. Software defined security for vehicular ad hoc networks. In Proceedings of the 2016 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea, 19–21 October 2016; pp. 533–537.
113. Imran, M.A.; Sambo, Y.A.; Abbasi, Q.H. Future Perspectives. In *Enabling 5G Communication Systems to Support Vertical Industries*; John Wiley & Sons, Incorporated: Hoboken, NI, USA, 2019.
114. Rivas, D.A.; Barceló-Ordinas, J.M.; Zapata, M.G.; Morillo-Pozo, J.D. Security on VANETs: Privacy, misbehaving nodes, false information and secure data aggregation. *J. Netw. Comput. Appl.* **2011**, *34*, 1942–1955. [CrossRef]
115. Kim, C.-H.; Bae, I.-H. A misbehavior-based reputation management system for VANETs. In *Embedded and Multimedia Computing Technology and Service*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 441–450.
116. Pathan, A.-S.K. *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*; CRC Press: Boca Raton, FL, USA, 2016.
117. Maglaras, L.A.; Al-Bayatti, A.H.; He, Y.; Wagner, I.; Janicke, H. Social internet of vehicles for smart cities. *J. Sens. Actuator Netw.* **2016**, *5*, 3. [CrossRef]
118. 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 April 2018; pp. 93–99.
119. Abolhasan, M.; Lipman, J.; Ni, W.; Hagelstein, B. Software-defined wireless networking: Centralized, distributed, or hybrid? *IEEE Netw.* **2015**, *29*, 32–38. [CrossRef]
120. Zhang, K.; Leng, S.; He, Y.; Maharjan, S.; Zhang, Y. Cooperative content caching in 5G networks with mobile edge computing. *IEEE Wirel. Commun.* **2018**, *25*, 80–87. [CrossRef]
121. Garg, S.; Kaur, K.; Ahmed, S.H.; Bradai, A.; Kaddoum, G.; Atiquzzaman, M. MobQoS: Mobility-Aware and QoS-Driven SDN Framework for Autonomous Vehicles. *IEEE Wirel. Commun.* **2019**, *26*, 12–20. [CrossRef]
122. Lazar, S.-A.; Stefan, C.-E. Future vehicular networks: What control technologies? In Proceedings of the 2016 International Conference on Communications (COMM), Bucharest, Romania, 9 June 2016; pp. 337–340.
123. Li, H.; Dong, M.; Ota, K. Control plane optimization in software-defined vehicular ad hoc networks. *IEEE Trans. Veh. Technol.* **2016**, *65*, 7895–7904. [CrossRef]
124. Bhatia, A.; Haribabu, K.; Gupta, K.; Sahu, A. Realization of flexible and scalable VANETs through SDN and virtualization. In Proceedings of the 2018 International Conference on Information Networking (ICOIN), Chiang Mai, Thailand, 10 January 2018; pp. 280–282.

125. Huang, C.-M.; Chiang, M.-S.; Dao, D.-T.; Pai, H.-M.; Xu, S.; Zhou, H. Vehicle-to-Infrastructure (V2I) offloading from cellular network to 802.11 p Wi-fi network based on the Software-Defined Network (SDN) architecture. *Veh. Commun.* **2017**, *9*, 288–300.
126. Zhang, D.; Yu, F.R.; Wei, Z.; Boukerche, A. Software-defined vehicular ad hoc networks with trust management. In Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications, Malta, Malta, 13–17 November 2016; pp. 41–49.
127. Bhatia, J.; Modi, Y.; Tanwar, S.; Bhavsar, M. Software defined vehicular networks: A comprehensive review. *Int. J. Commun. Syst.* **2019**, *32*, e4005. [CrossRef]
128. Raza, S.; Wang, S.; Ahmed, M.; Anwar, M.R. A Survey on Vehicular Edge Computing: Architecture, Applications, Technical Issues, and Future Directions. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 1–19. [CrossRef]
129. Rak, J.; Papadimitriou, D.; Niedermayer, H.; Romero, P. Information-driven network resilience: Research challenges and perspectives. *Opt. Switch. Netw.* **2017**, *23*, 156–178. [CrossRef]
130. Chiu, K.L.; Hwang, R.H.; Chen, Y.S. Cross-layer design vehicle-aided handover scheme in VANETs. *Wirel. Commun. Mob. Com.* **2011**, *11*, 916–928. [CrossRef]
131. Moreira, E. An evaluation of reputation with regard to the opportunistic forwarding of messages in VANETs. *EURASIP J. Wirel. Commun. Netw.* **2019**, *2019*, 204.
132. Nobre, J.C.; de Souza, A.M.; Rosario, D.; Both, C.; Villas, L.A.; Cerqueira, E.; Braun, T.; Gerla, M. Vehicular software-defined networking and fog computing: Integration and design principles. *Ad Hoc Netw.* **2019**, *82*, 172–181. [CrossRef]
133. Liu, J.; Wan, J.; Jia, D.; Zeng, B.; Li, D.; Hsu, C.-H.; Chen, H. High-efficiency urban-traffic management in context-aware computing and 5G communication. *IEEE Commun. Mag.* **2017**, *55*, 34–40. [CrossRef]
134. Ullah, A.; Yaqoob, S.; Imran, M.; Ning, H. Emergency message dissemination schemes based on congestion avoidance in VANET and vehicular FoG computing. *IEEE Access* **2018**, *7*, 1570–1585. [CrossRef]
135. Fan, Y.; Zhang, N. A Survey on Software-defined Vehicular Networks. *J. Comput.* **2017**, *28*, 236–244.
136. Zhou, Y.; Zheng, K.; Ni, W.; Liu, R.P. Elastic switch migration for control plane load balancing in SDN. *IEEE Access* **2018**, *6*, 3909–3919. [CrossRef]
137. Li, M.; Yu, F.R.; Si, P.; Sun, E.; Zhang, Y. Random access optimization for M2M communications in vanet with wireless network virtualization. In Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications, Valleta, Malta, 13–17 November 2016; pp. 1–7.
138. Li, H.; Ota, K.; Dong, M. Network virtualization optimization in software defined vehicular ad-hoc networks. In Proceedings of the 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall), Montreal, QC, Canada, 18 September 2016; pp. 1–5.
139. Bizanis, N.; Kuipers, F.A. SDN and virtualization solutions for the Internet of Things: A survey. *IEEE Access* **2016**, *4*, 5591–5606. [CrossRef]
140. Arif, M.; Shakeel, H. Virtualization security: Analysis and open challenges. *Int. J. Hybrid Inf. Technol.* **2015**, *8*, 237–246. [CrossRef]
141. Qafzezi, E.; Bylykbashi, K.; Spaho, E.; Barolli, L. A New Fuzzy-Based Resource Management System for SDN-VANETs. *Int. J. Mob. Comput. Multimed. Commun. (IJMCMC)* **2019**, *10*, 1–12. [CrossRef]
142. Arif, M.; Mahmood, T. Cloud computing and its environmental effects. *Int. J. Grid Distrib. Comput.* **2015**, *8*, 279–286. [CrossRef]
143. Geman, O.; Chiuchisan, I.; Ungurean, I.; Hagan, M.; Arif, M. Ubiquitous Healthcare System Based on the Sensors Network and Android Internet of Things Gateway. In Proceedings of the 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Guangzhou, China, 8 October 2018; pp. 1390–1395.
144. Duarte, J.M.; Kalogeiton, E.; Soua, R.; Manzo, G.; Palattella, M.R.; Di Maio, A.; Braun, T.; Engel, T.; Villas, L.A.; Rizzo, G.A. A multi-pronged approach to adaptive and context aware content dissemination in VANETs. *Mob. Netw. Appl.* **2018**, *23*, 1247–1259. [CrossRef]
145. Arif, M.; Alam, K.A.; Hussain, M. Application of data mining using artificial neural network: Survey. *Int. J. Database Theory Appl.* **2015**, *8*, 245–270. [CrossRef]
146. Das, T.; Sridharan, V.; Gurusamy, M. A Survey on Controller Placement in SDN. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 472–503. [CrossRef]

147. Ji, X.; Yu, H.; Fan, G.; Fu, W. SDGR: An SDN based geographic routing protocol for VANET. In Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, China, 15 December 2016; pp. 276–281.
148. Secinti, G.; Canberk, B.; Duong, T.Q.; Shu, L. Software defined architecture for VANET: A testbed implementation with wireless access management. *IEEE Commun. Mag.* **2017**, *55*, 135–141. [CrossRef]
149. Huang, C.-M.; Chiang, M.-S.; Dao, D.-T.; Su, W.-L.; Xu, S.; Zhou, H. V2V data offloading for cellular network based on the Software Defined Network (SDN) inside Mobile Edge Computing (MEC) architecture. *IEEE Access* **2018**, *6*, 17741–17755. [CrossRef]
150. Khan, A.A. Optimized Communication in 5G-Driven Vehicular Ad-Hoc Networks (VANETs). Ph.D. Thesis, University of Technology Sydney, Ultimo, Australia, 2019.
151. Xie, L.; Ding, Y.; Yang, H.; Wang, X. Blockchain-Based Secure and Trustworthy Internet of Things in SDN-Enabled 5G-VANETs. *IEEE Access* **2019**, *7*, 56656–56666. [CrossRef]
152. Zhuang, W.; Ye, Q.; Lyu, F.; Cheng, N.; Ren, J. SDN/NFV-Empowered Future IoV With Enhanced Communication, Computing, and Caching. *Proc. IEEE* **2020**, *108*, 274–291. [CrossRef]
153. Iwendi, C.; Uddin, M.; Ansere, J.A.; Nkurunziza, P.; Anajemba, J.H.; Bashir, A.K. On detection of sybil attack in large-scale VANETs using spider-monkey technique. *IEEE Access* **2018**, *6*, 47258–47267. [CrossRef]
154. Chahal, M.; Harit, S. Network Selection and Data Dissemination in Heterogeneous Software-defined Vehicular Network. *Comput. Netw.* **2019**, *161*, 32–44. [CrossRef]
155. Shahzad, M.; Antoniou, J. Quality of User Experience in 5G-VANET. In Proceedings of the 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Limassol, Cyprus, 11 September 2019; pp. 1–6.
156. Singh, P.K.; Sharma, S.; Nandi, S.K.; Nandi, S. Multipath TCP for V2I communication in SDN controlled small cell deployment of smart city. *Veh. Commun.* **2019**, *15*, 1–15. [CrossRef]
157. Vladyko, A.; Khakimov, A.; Muthanna, A.; Ateya, A.A.; Koucheryavy, A. Distributed Edge Computing to Assist Ultra-Low-Latency VANET Applications. *Future Internet* **2019**, *11*, 128. [CrossRef]
158. Xiao, K.; Liu, K.; Xu, X.; Zhou, Y.; Feng, L. Efficient fog-assisted heterogeneous data services in software defined VANETs. *J. Ambient Intell. Humaniz. Comput.* **2019**, 1–13. [CrossRef]