The Journal of Supercomputing (2023) 79:8368–8400
https://doi.org/10.1007/s11227-022-05008-y

A survey on software-defined vehicular networks (SDVNs): a security perspective

Rohit Kumar[1] · **Neha Agrawal**[2]

Accepted: 4 December 2022 / Published online: 17 December 2022

Abstract

Smart transportation systems have been the focus of research due to the development of smart cities. However, existing vehicular networks are not sufficient enough to fulfill the vision of futuristic smart cities due to limited flexibility, scalability, poor connection, and insufficient intelligence. These technological hurdles make the role of Software-Defined Networking (SDN) very important to improve the overall performance of the existing vehicular networks considering the unique properties of SDN such as Decoupling of network planes and Real-time network programming. This leads to the development of Software-Defined Vehicular Networks (SDVNs). SDVNs help to realize the development of smart transportation systems which further helps to optimize the vision of truly smart cities. However, the security remains a consistent concern due to the increased mobility, larger attack surface, and improvised future attack vector. This work includes the different design components, and offers a detailed survey to understand different security issues including the architectural and functional ones. Additionally, multiple security solutions are discussed including Service-based, Infrastructure-based, and Application-based solutions. Furthermore, the work also covers the possible challenges in the development of SDVNs based on Improved Architectural Development, Holistic Integration, Effective Orchestration, Environmental Volatility Handling, Global Network Management, Efficient Components/Technologies Integration, Diverse Security Offerings, and Design Issues' Maintenance. Lastly, the work highlights the resultant opportunities based on Application, Open Research, Network Management, Device Configuration, Traffic Management, QoS, and Efficient Routing.

Keywords Internet of Things (IoT) · Software-defined networks (SDNs) · Software-defined vehicular networks (SDVNs) · Vehicular ad hoc network (VANET) · Security issues

✉ Neha Agrawal
nehaiiitm345@gmail.com

Extended author information available on the last page of the article

Abbreviations

SDN	Software-defined networking
SDVNs	Software-defined vehicular networks
QoS	Quality of service
ITS	Intelligent transportation system
VANET	Vehicular ad hoc network
IDT	Intelligent digital twin
RSUs	Road side units
5G	Fifth generation
VN	Vehicular network
IIoT	Industrial internet of things
RGA	RSU-based group authentication
p-CIDS	In private-collaborative intrusion detection system
5G-SDVN	5G-enabled SDVN
SD-DSD	Software-defined dynamic security defense
VSNs	Vehicular sensor networks
V2X	Vehicle to everything
NR	New radio
VNG	Vehicular neighbor groups
IoE	Internet of everything
CPS	Cyber physical system
V2V	Vehicle-to-vehicle
V2I	Vehicle-to-infrastructure

1 Introduction

Vehicular networks are the backbone of any smart city transportation system. In future generation smart cities, the role of vehicular networks has been of prominent importance [1, 2]. Despite the huge significance of vehicular networks in smart cities, there are multiple challenges present in vehicular networks [3, 4]. Some of the major challenges are global monitoring, real-time routing, and accurate route cost estimation [5]. Software-Defined Networking (SDN) [6] is a future generation networking technology as the technology is under active exploration and research and can be used to improve multiple functional aspects of vehicular networks. SDN presents different unique features, e.g., agile network programming, global network state collection, and real-time topology update [7]. Multiple existing literary works have discussed the role of SDN to counter the challenges of modern vehicular networks [8]. In this way, the concept of Software-Defined Vehicular Networks (SDVNs) [9] gets evolved, which is the new generation vehicular technology.

SDVN offers all benefits of SDN to the vehicular systems. There are multiple challenges in vehicular networks such as network congestion, traffic management, accidents' probability calculation, and so on. The traditional vehicular networks might suffer from different attacks, inefficient traffic monitoring, congestion issues, reliability concerns, and ineffective network heuristics. The SDN functionality helps to counter these issues in a suitable way as it offers the proper architectural and

functional support for IDS/IPS, Traffic monitoring and filtering, Congestion control, Blockchain, and Machine learning technologies.

In addition to this, multiple other security issues have also been the serious concerns including authentication, privacy, availability, and mobility [10]. SDN helps to counter these network challenges and security issues, and extends the benefits like flexible network management, improved service capability, higher data rate, less delay, sustainable Quality of Service (QoS) [11]. This study comprises several design elements and provides a thorough analysis to comprehend various security challenges, including architectural and functional ones. Additionally, the work discusses a variety of security solutions including application-, infrastructure-, and service-based solutions. The work also highlights potential obstacles to SDVN development based on improved architectural development, holistic integration, effective orchestration, handling environmental volatility, managing a global network, integrating components/technologies efficiently, providing a variety of security options, and maintaining design issues. Furthermore, the study focuses on the opportunities that arise as a result of Application, Open Research, Network Management, Device Configuration, Traffic Management, QoS, and Efficient Routing. Figure 1 exhibits

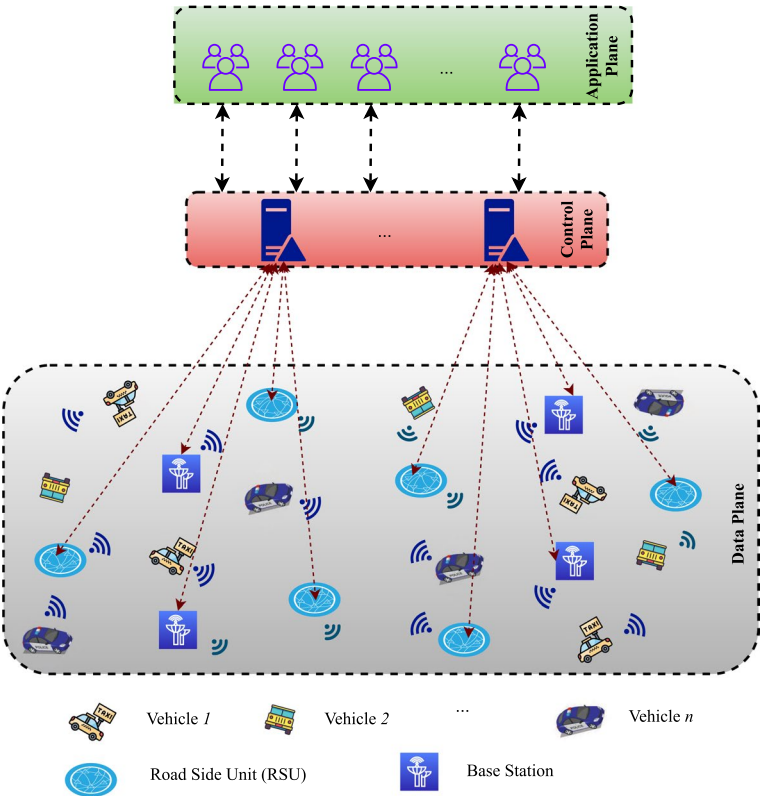


Fig. 1 Conceptual functional architecture of SDVNs

the architecture of a general SDVN. In addition to this, the common functional modules of SDVNs are also listed down in Fig. 2.

1.1 Motivation

When telecommunication and vehicular networks are combined to produce a heterogeneous vehicular network, the network suffers from heterogeneity and flexibility concerns. SDN allows for the separation of the data plane and the control plane in this scenario. This distinguishing characteristic of SDN enables an abstraction of heterogeneity in vehicular networks, which simplifies network management and setup by offering a common interface to various network components. Given the dynamic nature of vehicle networks, the control plane enables quick configuration management and efficiently combines numerous network technologies. There have been multiple works offering SDVN architectures and related issues; however, the security aspects in SDVNs have not been explored well enough. Furthermore, the existing solutions lack a work offering a dedicated survey on the Security issues, Security solutions, Security challenges, and various Opportunities in SDVNs.

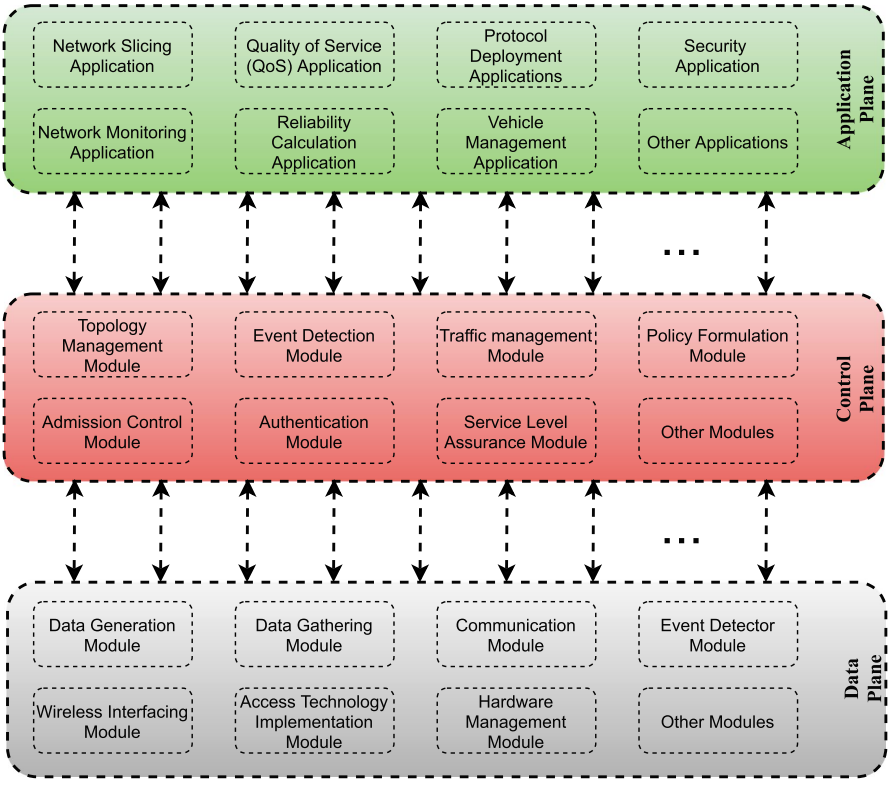


Fig. 2 Common functional modules of SDVNs

Table 1 summarizes a comparative analysis of the recent relevant surveys [9, 12–19]. It is clear from Table 1 that multiple security concerns are not addressed in existing surveys. Although the goal is stated, the classification criteria and taxonomy details are not sufficiently articulated. The goal of this survey is to alleviate these constraints by conducting a thorough survey of various security elements and concerns w.r.t. SDVNs.

1.2 Major contributions

This work discusses the various security aspects of the SDVNs. The work involves multiple existing SDVN surveys and tutorials. Based on the motivation detailed in the above subsection, some of the major contributions of the presented work are listed below.

- It offers a survey covering a variety of SDVN works. It helps to understand the different design components including the System Components, Architectural Components, Operational Modes, Access Technologies, and Services. Furthermore, the work highlights the state-of-the-art of the SDVNs based on Architecture, Service, and Security.
- It details the Security issues in SDVNs including the Architectural and Functional issues like Network congestion, Access control, Periodic updates, Authentication, Authorization, etc.
- It highlights various security solutions in SDVNs including Service-based, Infrastructure-based, Application-based solutions. Additionally, the work compares them based on the Secure design, Audit, Policies, and Analysis.
- It also exhibits the Security challenges in SDVNs based on Improved Architectural Development, Holistic Integration, Effective Orchestration, Environmental Volatility Handling, Global Network Management, Efficient Components/Technologies Integration, Diverse Security Offerings, and Design Issues' Maintenance. The existing works are compared against some common security challenges including Network management, Interoperability, Protocol standardization, Scalability, etc.
- Finally, the paper offers various opportunities in the field of SDVNs based on Application, Open Research, Network Management, Device Configuration, Traffic Management, QoS, and Efficient Routing. It also details various possibilities ranging from Global network monitoring, Agile network management, Real-time programming, etc.

1.3 Use cases

Use cases are beneficial since they aid in describing how a system ought to operate and aid in generating ideas for potential problems. Their list of objectives may be used to determine the system's cost and complexity. Furthermore, the existing use-cases work like a dummy model and foundation stone for the futuristic use-cases. There are multiple use cases related to SDVNs including Efficient data

Table 1 Comparative analysis of this survey with the existing-related surveys

S. No.	References	Objective	IDDC	SI	SS	SC	Op
1.	Cardona et al. [9]	To perform a systematic review of SDVN-related techniques	✓	×	×	✓	✓
2.	Bhatia et al. [12]	To offer summary of the SDVN studies and components	✓	✓	×	✓	✓
3.	Ben et al. [13]	To study the state-of-the-art SDVN architectures	×	✓	×	✓	×
4.	Akhunzada et al. [14]	To present a systematic top-down approach against security vulnerabilities, attacks, and challenges	×	✓	×	✓	×
5.	Islam et al. [15]	To offer a taxonomy of SDVN architecture-based on its modes of operation	×	×	×	✓	×
6.	Lacoste et al. [16]	To discuss the overview of the SDVN approaches and architectures	×	✓	×	✓	✓
7.	Sultana et al. [17]	To encompass a comprehensive review of the security solutions for SDVNs	×	✓	✓	✓	×
8.	Wang et al. [18]	To discuss the architectures of cloud-enabled SDVN	×	×	×	✓	✓
9.	Arif et al. [19]	To elaborate the challenges, along with the applications, and the future directions	✓	×	×	✓	✓
10.	This Survey	To provide the security issues, solutions, challenges, opportunities, and related coverage in SDVNs	✓	✓	✓	✓	✓

In-detail description is offered in Sects. 2, 4, 5, 6, and 7, respectively

***IDDC** In-Detail Design Components, *SI* Security Issues, *SS* Security Solutions, *SC* Security Challenges, *Op* Opportunities

dissemination, On demand surveillance service, Virtualization of wireless network, Dynamic air quality monitoring, Smart parking, Latency-based routing, Lane change assistance, Traffic accident detection, and so on. However, the common use case of security w.r.t. SDVNs is to improve the safety services, e.g., road safety by allowing V2V and V2I communication [12]. The SDN might encrypt or limit specific frequencies or channels. The allocated frequencies might be used for emergency traffic or other privileged operations. The key benefit of SDN-enabled VANET over traditional emergency channels is the ability to dynamically allocate frequencies. Based on traffic circumstances and application requirements, the SDN controller can reserve channels for emergency services. These channels can also be used to accommodate a variety of applications or services. This restricted frequency can be used for emergency alerts such as cooperative awareness messaging. Various privacy strategies can also be used to improve the two safety features including lane change warning and front collision.

1.4 Outline of the paper

This work is divided into eight sections. Section 1 offers the basic introduction to the vehicular networks and SDN technologies. The basic design components of SDVNs are discussed in Sect. 2. The state-of-the-art SDVN works are covered in Sect. 3. Section 4 details the various security issues. The related SDVN security solutions are discussed in Sect. 5. Section 6 highlights the multiple challenges present in SDVNs. The possible opportunities in SDVNs are covered in Sect. 7. Finally, Sect. 8 concludes the work with respective future possibilities. The overall workflow of this paper is depicted in Fig. 3.

2 SDVN basic design components

There are different design components that constitute the SDVNs. Some of the major component categories are discussed herewith in detail [9–12, 20].

2.1 System components

The system components of SDVNs include—(a) Application plane, (b) Control plane, (c) Data plane, and (d) Communication interfaces. The respective details are provided below.

- *Application Plane* The application plane contains applications that rely on the network to offer services to end users and processes. The application plane does not include applications that directly (or mostly) support the operation of the forwarding plane (such as routing procedures within the control plane).
- *Control Plane* The control plane makes choices about network device packet forwarding and provides packet forwarding rules to network switches and rout-

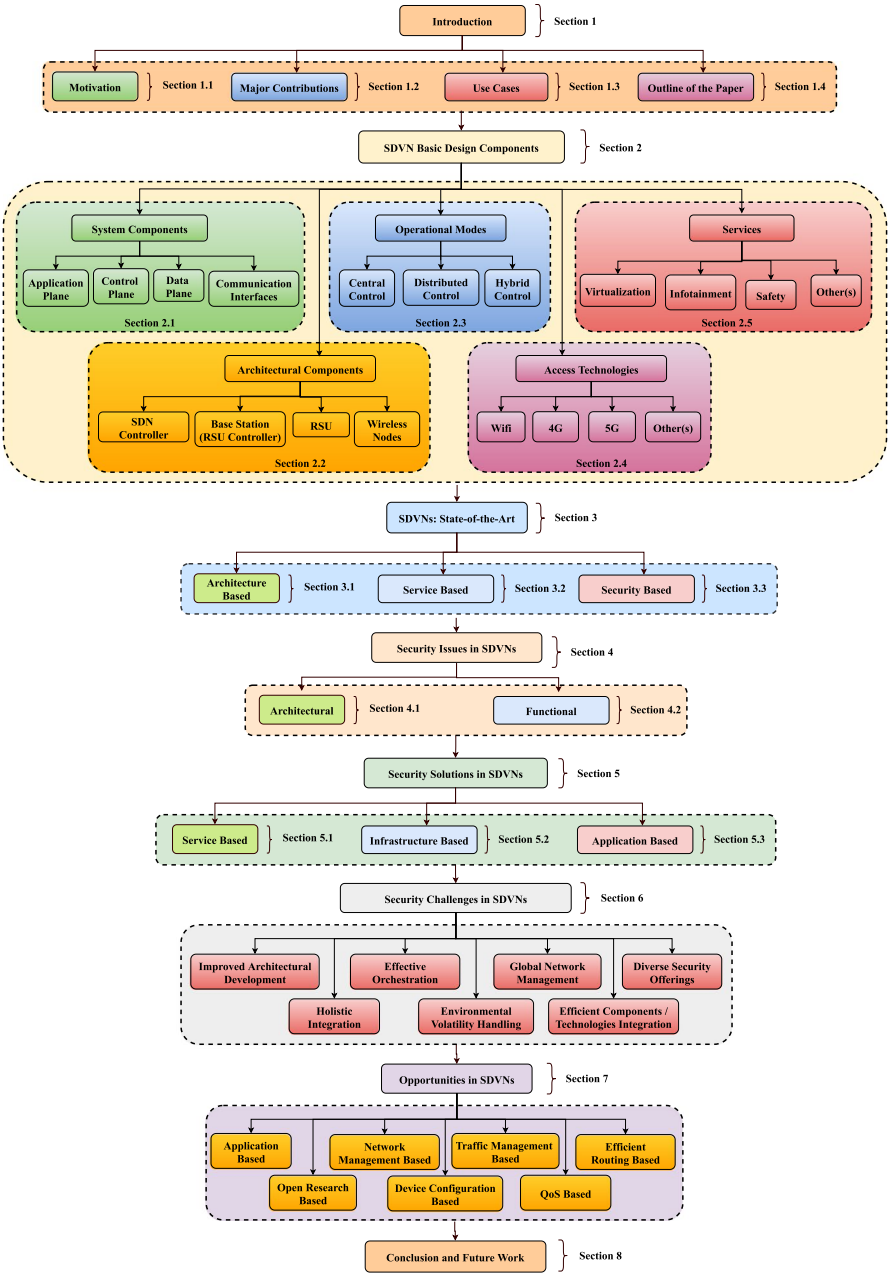


Fig. 3 Workflow of the paper

ers for implementation. Given the network design, the control plane is primarily responsible for updating the forwarding table, which is located on the data plane.
- *Data Plane* The data plane processes packets in-line with the control plane's directives. The data plane's duties include, but are not limited to, altering, discarding, and forwarding packets. In addition, the data plane includes forwarding resources such as classifiers. As a result, it is also known as the forwarding plane.
- *Communication Interfaces* There are two types of communication interfaces in the SDVN architecture: (a) northbound interfaces and (b) southbound interfaces. The northbound interface allows the control plane and management plane to communicate with the application plane, whereas the southbound interface allows the control plane and management plane to communicate with the network device.

2.2 Architectural components

SDVNs include four major network architecture components: (a) the SDN controller, (b) SDN wireless nodes, (c) SDN Road Side Units (RSUs), and (d) the SDN RSU controller.

- *SDN Controller* The SDN controller is an important component of SDN-based vehicular networks. It is in charge of the overall network's behavior. It also manages the flow of data to routers/switches via southbound interfaces and applications via northbound interfaces.
- *Base Station (RSU Controller)* The SDN RSU controller manages a group of RSUs that are linked to it over a broadband link. This controller is an OpenFlow-based infrastructure that is in charge of data forwarding, emergency services, and local data storage.
- *RSU* In SDN-based vehicular networks, RSUs are stationary structures. RSUs are installed along roadsides and are controlled by the SDN controller. An RSU is crucial for gathering and evaluating traffic data produced by smart cars within their coverage area. RSUs can also act as entry points to other communication networks, such as the Internet.
- *Wireless Nodes* In SDN-based vehicular networks, SDN wireless nodes are the cars that carry out operations depending on control messages received from the SDN controller. They are the mobile data plane pieces that the SDN controller manages.

2.3 Operational modes

An operational mode of a system is defined as the operational configuration or the way of functioning of the system. It is characterized by its active functions. The system may carry out particular operational tasks while being in a particular operational mode, which activates the associated functionality. Similarly, the operational mode in SDVNs defines the operational/functional control of the overall network. There are three main

operational modes for SDVNs namely, (a) Central, (b) Distributed, and (c) Hybrid. The respective details are given below.

- *Central Control* The flow rules for traffic management are enforced using the SDN controller in central control mode. The SDN controller oversees all operations done by SDN wireless nodes, SDN RSUs, and the SDN RSU controller in this mode.
- *Distributed Control* Since single controller represents a single point of failure in the network, relying only on it may not be feasible. It could develop into a performance snag. As a result, it becomes necessary to divide network control. SDN wireless nodes and SDN RSUs are not led by the SDN controller while in dispersed control mode. This style of control is similar to that seen in classic distributed self-organizing networks.
- *Hybrid Control* The SDN controller does not entirely control SDN wireless nodes and SDN RSUs in hybrid control mode. Instead, it simply describes the overall policy principles, not all of the flow rules. To route packets and perform flow-level processing, SDN data elements, SDN wireless nodes, and SDN RSUs use their own intelligence.

2.4 Access technologies

Multiple access technologies are used in SDVNs. Some of the major ones are discussed below.

- *Wi-Fi* The DSRC working group has been actively creating a standard for wireless access in vehicle contexts, where communication is based on the IEEE 802.11p standard, an upgraded version of the IEEE 802.11 Wi-Fi standard.
- *4G* 4G is a vehicle access technology that is utilized in SDVNs. Commercially, two 4G potential standards are in use: (a) LTE and (b) Mobile WiMAX. In SDVNs, LTE can be utilized to meet the needs for delay-sensitive applications. Mobile WiMAX is suited for vehicle network applications since it provides high-speed mobility and has a large coverage; as a result, network disturbances are minimized.
- *5G* 5G-based vehicle networks are capable of supporting a wide range of applications and enabling vehicular networking for traditional multimedia applications.
- *Other(s)* TV white spaces are also employed to increase efficiency by vehicle networks equipped with cognitive radio technology. Users of vehicular networks employ available spectrum in TV bands to meet application quality-of-service needs.

2.5 Services

SDVNs offer a variety of critical services, such as SDN-assisted safety services, network virtualization services, on-demand surveillance services, infotainment services, and so on. A brief description of these services is provided below.

- *Virtualization* The notion of wireless network virtualization is the virtualization of network resources or data routes in order to achieve tenant or application segregation. Typically, such segregation is necessary for a variety of reasons, including fault isolation, network abstraction, scalability, and security.
- *Infotainment* Advertisements, tourist information, traffic information, and parking guidance are examples of infotainment services. These services are predicted to attract a large mass market in vehicle networks. The usage of SDN aids in the effective implementation of these services by isolating control traffic from real service data flow.
- *Safety* Safety services are supplied by dynamically setting flow rules and allocating them to switches while taking into account network circumstances and application needs.
- *Surveillance* An SDN controller is used to deliver surveillance services. This controller maintains and inputs flow rules for surveillance data to reach requesting vehicular nodes. SDN's centralized controller-based architecture makes it easier for network operators to supply network traffic management services. The controller makes network-wide packet-forwarding choices based on all network information.
- *Other(s)* Smart parking and light management services may also be provided by SDVNs. Thousands of luminaires, sensors, and cameras form a network in the cloud to deliver automated parking and lighting services, boost flexibility, and give real-time information.

3 SDVNs: state-of-the-art

There have been lots of enhancements in the development process of SDVNs. The different design components and technologies have matured over the period of time. This section presents some of the recent technical advancements and related literary works to highlight the state-of-the-art. The role of SDVN as a promising technology is detailed in [21] to improve the performance of modern vehicular networks. However, existing routing protocols are not robust enough to optimize the communication in SDVNs. The work presents the routing aspects of SDVNs, and offers some design insights in SDVNs. Authors offer a comprehensive analysis to understand the key opportunities and future research issues. The work discussed in [12] talks about the recent breakthroughs in automobile and telecommunication industries with a focus on Intelligent Transportation System (ITS). The potential of SDN has been highlighted to offer extensive advanced features to the vehicular networks and develop SDVNs. This work provides a detailed compilation of the SDN-based Vehicular Ad hoc Network (VANET) systems including various opportunities, trending technologies, architectural modes, access technologies, and related protocols. Finally, the work explores the challenges, open issues, and future research directions.

The unique features of SDVN help to leverage the vehicular network to improve the performance and management of VANET [22]. This work starts with a taxonomy of SDVN architecture, the state-of-the-art SDVN routing protocols, and the challenges of current SDVNs. Authors highlight the role of Fifth Generation (5G)

networks in [13], and the functional responsibilities of SDN and VANET have also been discussed for the effective development of next generation intelligent vehicular networks. The work details the benefits of software-defined VANET services, and the deployment of novel architectural components, and possible vulnerabilities. The work surveys the state-of-the-art SDVN architectures, respective functionalities, associated benefits, and related challenges. VANETs have been the research focus since the last few years as per [9] their relation with mobile ad hoc networks has also been facilitated. The work details that the role and scope of VANETs has been extended to cyclists and pedestrians, and VANETs face numerous challenges. SDN helps to address these challenges with a focus on network control and management. The work offers a systematic review of SDN techniques in the VANET domain. Additionally, it highlights the open challenges and related research areas.

3.1 Architecture based

In [23], the Intelligent Digital Twin (IDT) idea is described in depth, and a new architecture dubbed IDT-SDVN is introduced. The project emphasizes the potential for picking up new networking techniques through observation of one's surroundings. IDT supports the networking of useful features to accomplish adaptive iterative updating of networking schemes and aids in the realization of intelligent manufacturing. The paper highlights the IDT-SDVNs' related open problems and challenges while maximizing the benefits of SDVNs. The paper presents a case study to show how employing IDT-SDVNs has significantly improved things. Due to VANET's rigid design, deploying services and protocols has proven to be a challenging undertaking [24]. On top of edge networks, the idea of a cloud radio access network has been explored in [25]. The design of software-defined radio access networks is seen as a potent paradigm for the next generation of mobile networks. The optimization of resources for mobile universal radio is facilitated by an inherent "cloud-down" architecture. To implement vehicle technologies, which might not entirely rely on wireless infrastructures to ensure driving safety, an "edge-up" architecture is preferable.

3.2 Service based

The article referenced in [26] describes the function of SDVNs for various radio access technologies in order to support the substantial application and service data. SDVNs aid in creating a global network perspective and elevate static hardware-based network device limits. However, in order to manage the rapid device mobility and increasing network density, a strong discovery protocol is required. With regard to SDVNs, the paper suggests a topology discovery technique that lessens network overhead and improves time-complexity. Authors use [27] as an example to highlight the significance of trustworthy data supply in vehicle networks. A significant problem is posed by the high-speed mobility of vehicles. A caching and routing approach for SDVNs based on time prediction is proposed in the paper. Modules for information awareness and link prediction are employed to boost the performance of the flow delivery, and the controller uses these integrated modules to forecast the

remaining link time. A mobility-aware solution to the controller placement issue at the RSUs in SDVNs is put out in [28]. The strategy assists in positioning the local controllers at appropriate RSUs to reduce operational time. The method takes the possibility of dynamic road traffic into account and effectively adjusts the controller placement. To sustain the flow of control and data packets, traffic prediction and monitoring techniques are employed.

3.3 Security based

In [14], the development of secure SDVN is underlined. Security is a genuine worry with SDVNs despite their immense potential. The logical concentration of network intelligence might result in cyber risks and assaults since security and reliability in SDNs have been overlooked in many ways. Therefore, if mismanaged, developing SDVNs might cause more severe damage. Furthermore, the innovative SDVN entities and architectural elements might result in fresh security risks. The study provides a methodical top-down strategy to address the problems and potential risks. By describing the security implications in new SDVNs, the paper strengthens its contribution. A secure SDVN's prospective requirements and key enablers are also investigated, with an emphasis on unresolved security research problems. Additionally, the security and safety of the pedestrians and travelers have been described in [15]. Although VANET is a promising technology that offers safety, there may be a number of application problems.

The in-detail comparison of above-mentioned state-of-the-art SDVNs is detailed in Table 2. The comparison is done w.r.t the objective, application area, tools/techniques used, and the derived inference.

4 Security issues in SDVNs

There are different security issues w.r.t. SDVNs. Some of the common security issues are discussed in this section with related literary works. In [29], the concepts of 5G, VANETs, and SDN have been discussed with a focus on the development of intelligent vehicular networks. Different architectures and benefits of SDVN services with new functionalities have also been discussed. Additionally, the security and robustness have been focused for effective deployment and integration of different architectural components. The work explored the state-of-the-art SDVN architectures with related networking designs, functionalities, associated benefits, and respective security challenges in the form of availability, integrity, privacy, and authentication. Additionally, the role of VANETs has been highlighted in [30] w.r.t. intelligent transportation systems to offer safety and security. However, the major concern is to maintain the sensitive information as the information leakage can degrade the overall performance. The work offers a survey including various attacks and related solutions. A taxonomy has also been provided based on various types of attacks and solutions. Finally, the work explores the emerging challenges and

Table 2 Comparative analysis of the state-of-the-art SDVN approaches

References	Objective	Application area	Tools/techniques	Remark(s)
Cardona et al. [9]	Systematic review on SDN in VANET	SDVN	Studies SDN and VANET from communication and architectural perspective	Highlights open research areas and challenges
Bhatia et al. [12]	Offers a compilation of the work on SDN-based VANET system as a whole, incorporating its architecture, use-cases, and opportunities	SDVNs	Architectural modes, protocols, access technologies, etc., based taxonomy	Presents challenges, open research issues, and future research directions w.r.t. SDVNs
Ben et al. [13]	Study of SDN-based Vehicular Ad hoc Networks (VANETs)	Software-Defined VANETs	Discussed SDVN architecture against major security threats	Presents the future research directions and applications
Akhunzada et al. [14]	Security implications of SDVN networks	SDVN	SDVN layer-based taxonomy	Discusses security vulnerabilities, attacks, and challenges for each SDVN layer
Islam et al. [15]	Provides an in-detail survey on SDVN architecture and routing	ITSs and SDVNs	Operational modes based taxonomy	Explains state-of-the-art SDVN routing protocols and relevant classification. Details different classification criteria
Zhao et al. [21]	Routing schemes for SDVN	SDVN	Classification and design principles of routing schemes for SDVN	Discusses open issues and future research direction
Zhao et al. [23]	Introduced Intelligent Digital Twin (IDT)-based SDVN	SDVNs	Graph Routing	Discussed challenges and research issues in IDT-SDVN
Deng et al. [25]	Latency control	Software-Defined Mobile-Edge Vehicular Networks	Latency control of radio access steering and processing cache at base station	Improves the overall latency
Aljeri and Boukerche [26]	Distributed topology discovery protocol for SDVN	SDVN	Nodes closeness centrality scores	Improves discovery performance in terms of time and overhead complexity
Yan et al. [27]	Improving flow delivery in SDVN	SDVN	Time prediction-based backup caching and routing scheme	Improves flow delivery performance

Table 2 (continued)

References	Objective	Application area	Tools/techniques	Remark(s)
Maity et al. [28]	Mobility-aware controller placement in SDVN	SDVN	Integer linear program and Markov model	Reduces average flow setup delay by 13.85%

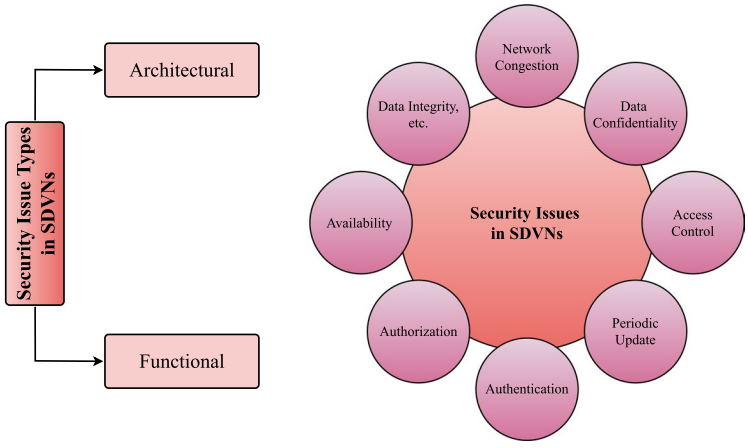
issues to motivate the research communities to counter the possible security threats in VANET.

As VANET is a superset of SDVN, many concerns also apply to SDVN. The significance of Vehicular Sensor Networks (VSNs) w.r.t. transportation technology, and its massive potential to improvise the transportation environment are discussed in [31]. The work focuses on the developments and issues in the vehicular networks, and offers some useful insights for the innovative implementation, modeling, and integration of state-of-the-art technologies such as vehicular networks. Similar issues including the security issues also get applied to the SDVNs.

Some of the common security issues are listed in the form of Fig. 4. Additionally, the in-detail comparison of some SDVN-based works w.r.t. security issues is detailed in Table 3. The analysis is done based on the network congestion, authorization, availability, etc.

4.1 Architectural

The SDVN, associated concepts, further innovation, and enhanced network programmability are documented in [14]. Traditional vehicular networks are expanded by SDN in the form of SDVNs; however, security solutions are of utmost importance. The logical concentration of network intelligence may have more disastrous repercussions than in conventional networks, raising security concerns. The new SDVN entities and components might reveal fresh security risks. In order to allow safe SDVNs, the essay discusses additional security considerations. Finally, a wide range of security concerns have been researched in order to foresee safe SDVNs. In [23] authors examine SDVN as a possible design to overcome the shortcomings of the current vehicular networks. The real-time network architecture has several difficulties due to the absence of different aspects, such as adequate data gathering, verification, and validation. The work thus debuted IDT's intelligent manufacturing



(a) Security Issues Categorization (b) Some examples of Security issues

Fig. 4 General categorization and common security issues in SDVNs

Table 3 Comparative analysis of some SDVN-based works w.r.t. security issues

References	Network congestion	Data confidentiality	Access control	Periodic update	Authen.	Authorization	Avail.	Data integrity
Akhunzada et al. 2017) [14]	×	×	✓	✓	✓	✓	✓	✓
Zhao et al. [21]	×	×	×	✓	×	×	×	×
Zhao et al. [23]	×	×	×	✓	×	×	×	×
Jaballah et al. [29]	✓	✓	×	✓	✓	✓	✓	✓
Tanwar et al. [30]	✓	✓	✓	✓	✓	✓	✓	✓
Kurugollu et al. [31]	×	×	✓	×	✓	×	×	×
Mendiboure et al. [32]	×	×	✓	✓	✓	✓	×	×
Xu et al. [33]	✓	×	×	✓	✓	✓	✓	✓
Raut and Rawat [35]	✓	✓	×	×	✓	✓	✓	✓
Raja et al. [36]	×	×	✓	✓	✓	×	×	✓
Shrestha et al. [37]	✓	✓	✓	✓	✓	✓	✓	✓

offering. Additional features aimed at implementing adaptive updates in networking are promised by IDT. The IDT-SDVN architecture was suggested in the work to maximize the benefits. The work also examined IDT-SDVNs' unresolved problems and associated difficulties. SDVNs are seen as the vehicle networks of the future, according to [32]. Large SDVNs are created as a result of the interoperability and mobility management provided by SDVNs among heterogeneous networks. Additionally, SDVNs encounter a variety of security issues, notably those related to authentication and access control. Unauthorized SDN switch-based attacks and unauthorized SDN controller-based attacks (packet redirection and packet drops) are both potential (reconnaissance attack and malicious feedback). According to the SDVN features and SDVN standards, the work recommends using Blockchain technology to resolve these authentication and access control challenges. However, the blockchain network has a significant difficulty with scalability. In order to increase performance in terms of throughput, latency, CPU use, etc., the paper suggests a scalable architecture with effective access control and authentication techniques.

The research described in [33] describes the integrated architecture of 5G-enabled SDVN (5G-SDVN), which is regarded as the new standard for the next generation of transportation systems. Low latency and high throughput are promised by 5G-SDVNs. However, given the quick vehicle movement, there are various security difficulties and problems with 5G-SDVN. Additionally, because of its capabilities like scalability and programmability, SDN may increase the attack surface. This can make it even more likely that there will be flaws and vulnerabilities. As a result, the study provides an SD-DSD (Software-Defined Dynamic Security Defense) system. The plan assists in providing security-as-a-service with regard to 5G-SDVN and carries out a security evaluation to gauge the effectiveness of the present security system. In [34], a trust framework for software-defined vehicular networks (TFMD-SDVN) misbehavior detection is designed to identify the right network events delivered by trustworthy or untrusted nodes. Recommendation, similarity, and rating all contribute to a node's trust value. The event reported by the event reporting node (ERN) is deemed to be accurate if the trust value is greater than a certain threshold.

4.2 Functional

In [35], the function of the Vehicular Network (VN) to guarantee motorist safety is covered. However, several difficult problems like security, integrity, etc., are also shown. The article also discusses the risks of potential assaults on networks with inadequate security that would deny efficiency and dependability. SDN aids in dynamic network configuration. Dealing with security concerns is still difficult. The article offers a thorough analysis of SDN security, including relevant threats and weaknesses. In [36], the function of VANETs' Industrial Internet of Things (IIoT) is described. Road transportation is made possible by VANETs and is intelligent, clever, and safe. SDN offers network programmability to further this progress. The project provides SDVN with an energy-efficient end-to-end security solution. The suggested plan demonstrates SDN's ability to provide flexible network management in addition to its part in providing green IIoT

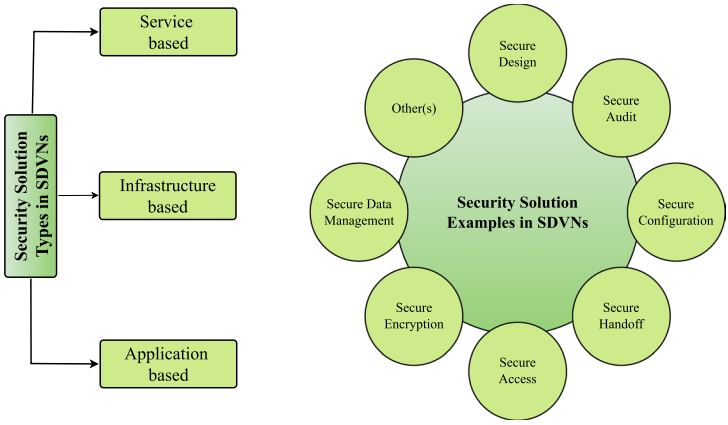
services. As a result, the suggested SDVN offers minimal end-to-end security. RSU-based Group Authentication (RGA) and a Private Collaborative Intrusion Detection System are used to manage the end-to-end security. The SDVN provides the potential intrusions while ensuring the desired privacy through collaborative learning. The idea of SDVN is described in [21] as a viable technology to enhance the conventional vehicular networks. The investigation reveals several aspects of routing performance as well as major issues and chances that are associated. Traditional and cutting-edge networks alike have long aimed to provide secure routing as a performance goal.

Similar to this, writers in [37] explore autonomous cars, intelligent autonomous vehicles, and related security challenges. The research examines Vehicle to Everything (V2X) communications in relation to real-time information, efficiency, and safety in automotive networks. Cellular 5G and New Radio (NR) technologies are being integrated into V2X communications, along with issues like security, ultra-low latency, ultra-high bandwidth, and reliability. The lack of flexibility and inadequate security, however, make the development extremely difficult. From a networking, security, and privacy perspective, blockchain aids in the creation of an environment that works well. According to [38], the characteristics of vehicle networks make security, privacy, and trust management significant tasks to manage. Blockchain is a brand-new decentralized, distributed computing platform that eliminates the need for a single reliable authority and enables resource recording and monitoring. As a result, there is a lot of room for security improvements in vehicle networks. This study's objective is to analyze, classify, and discuss several proposed models for blockchain-based vehicle networks. The authors provided concise comparisons of the different models' main traits and objectives in terms of security, privacy protection, and trust management.

Thus, multiple security-related issues such as Single point of failure, DDoS attacks, network topology poisoning, Authentication, Access control, and Controller replication remain present in SDVNs. Hence, it is suggested to counter them in a suitable way accordingly. The various security solutions have been discussed in the next section.

5 Security solutions in SDVNs

There are a variety of security solutions in the literature w.r.t. SDVNs. This section discusses some of the major security solution categories, along with relevant literary works. As per [14], SDVN helps to improve the network management and talks about security and dependability solutions. As the SDVNs' novel entities and components may have new security threats, the work offers a systematic approach to handle the potential security vulnerabilities w.r.t. each functional layer. The work highlights the security implications to devise layered taxonomies. Additionally, it describes the potential requirements of secure SDVNs. Some of the common security issues are listed in the form of Fig. 5. Additionally, the in-detail comparison of some SDVN-based works w.r.t. security solutions is detailed in Table 4.



(a) Security Solutions Categorization (b) Some examples of Security solutions

Fig. 5 General categorization and common security solutions in SDVNs

5.1 Service based

According to [29], the main concerns of SDVN designs have been security and robustness. The report underlines the potential security risks with regard to modern SDVNs. This article also discusses certain important security risks that compromise the availability, confidentiality, data integrity, and other crucial security functions. Regarding upcoming SDVN designs, the corresponding countermeasures as well as certain strict security and privacy solutions have also been outlined. The work is a thorough survey and analysis of SDVNs for networks and applications of the future (such as intelligent transportation systems and IoT-enabled advertising in VANETs). According to [32], SDVN has significant authentication and access control problems. The behavior of switches may be changed by an illegal SDN controller, which might lead to erroneous traffic redirection and packet losses. Unauthorized switches may also interfere with network operations and cause malicious feedback and/or reconnaissance attacks. Blockchain might be a productive way to address these problems. The work suggests a scalable and creative solution with effective mechanisms for cross-sub-network authentication and revocation.

In [39], authors emphasize the significance of the SDVN paradigm. Vehicle networks are discussed as an emerging technology that offers a variety of network services. However, heterogeneity presents difficulties for the efficient creation of communication protocols. SDVN aids in the creation of new adaptable protocols. The work suggests a brand-new geocast protocol called Geo-SDVN in this direction. Additionally, the work is intended to enhance general management, which could benefit security.

Table 4 Comparative analysis of some SDVN-based works w.r.t. security solutions

References	Secure design	Secure audits	Secure policies	Secure analysis	Other(s)
Akhunzada et al. [14]	✓	✓	✓	✓	Layer-wise security implications are discussed. Secure SDVN requirements are presented along with the open research issues.
Lacoste et al. [16]	✓	×	✓	×	Offers insights on the potential use of machine learning and artificial intelligence in future smart vehicular network. Discusses high mobility, strong network dynamics, security and safety, and stringent and heterogeneous QoS issues.
Jaballah et al. [29]	✓	×	✓	✓	State-of-the-art SDVN architectures are covered with positive and negative impacts. Analyzes different security vulnerabilities and attacks. Array of open security research issues is presented.
Mendiboure et al. [32]	×	×	×	×	An access privilege system for different devices is proposed. Security for cross-authentication, cross-revocation and access control in SDVN is improved.
Raut and Rawat [35]	✓	×	×	✓	Analyzes various SDVN vulnerabilities, attacks, and solutions. New methods are offered for Secure SDVN.
Raja et al. [36]	✓	×	×	✓	Security of VANET is discussed w.r.t. green IIoT. Group-id and Key pair-based RGA authentication assisted admission control is discussed.
Shrestha et al. [37]	✓	×	×	✓	Investigates the blockchain and 5G-based MEC vehicular network integration w.r.t. security, privacy protection, and content caching. Details open research challenges and future research directions.
Sousa et al. [39]	✓	×	×	✓	Improves delivery rate, transmission overhead and transmission delay. The proposed architecture does not encourage the use of roadside units.
Rahouti et al. [40]	✓	×	✓	✓	Discusses smart city communication networks to enhance resiliency and security. Offers current state-of-the-art reliable, and secure smart city communication systems.
Yu et al. [41]	✓	×	×	✓	Offers efficient and rapid detection of DDoS in SDVNs. Details the reduced attack detection and classification time with lower false alarm rate.
Huang et al. [43]	✓	×	✓	×	Improves scalability and flexibility in 5G networks. Improves resource utilization and sustainable network development.

5.2 Infrastructure based

The project presented in [40] investigates the idea of a smart city with the intention of completely overhauling the transportation and communication networks. The purpose of the work is to improve the QoS of current information technologies and maximize the sustainability of resources. It is essential to protect and transport the data effectively since some of the data from smart cities may have security requirements. SDN makes a difference, but the system still lacks cohesion. In order to assess the essential capabilities of an SDN-based secure communication infrastructure, the study focuses on security against potential risks and difficulties. To improve road safety, the development of wireless networks, vehicular networks, etc., has been the emphasis of [41]. This also contributes to reducing traffic and improving the driving experience. However, several assaults may be launched against vehicle networks. The project develops a framework to monitor potential DDoS assaults in SDN-based automotive networks and to take appropriate action. The strategy reduces the time needed to identify attacks and classify them. It also aids in reducing the incidence of false alarms. To assure driver safety, [35] discusses the idea of ITS, new protocols, architecture, etc. But problems with security, integrity, etc., must be fixed. The system's overall dependability and efficiency may be affected by new attacks brought on by the system's likely low security. The work provides an in-depth analysis of SDN security with a focus on threats and vulnerabilities.

The evolution of SDVN in the future is described in [36] together with an energy-efficient end-to-end security solution. End-to-end security is offered by the suggested method. The goal is to handle the private, collaborative intrusion detection system and RSU-based group authentication. Through the combination of privacy and homomorphic encryption techniques, the methodology offers the quick identification of possible VANET breaches. A flexible and adaptive approach is required since heterogeneity is a persistent issue in wireless networks, according to [42]. SDN provides uniform abstraction and programmability, bridging the gaps. In order to promote quick innovation and development in vehicle networks, the paper suggests an SDN-based architecture. The roadside equipment and cars are abstracted as SDN switches. The control plane assigns resources like spectrum and bandwidth, enabling more flexible setup.

5.3 Application based

Modern technologies assist the many smart city applications, such as those for energy, transportation, and health. The notion of network densification as one of the fundamental 5G technologies is explained in the study cited in [43]. The problem is managing a huge number of vehicular neighbors, despite the idea being employed for high user throughput and traffic capacity. Vehicular Neighbor Groups (VNGs), which are made up of many vehicular neighbors, are essential to improving 5G services. The approach uses mobile edge computing to increase network control while SDN aids in managing VNGs. In 5G-SDVN, programmability, flexibility, and controllability are introduced by SDN, which makes network administration easier and

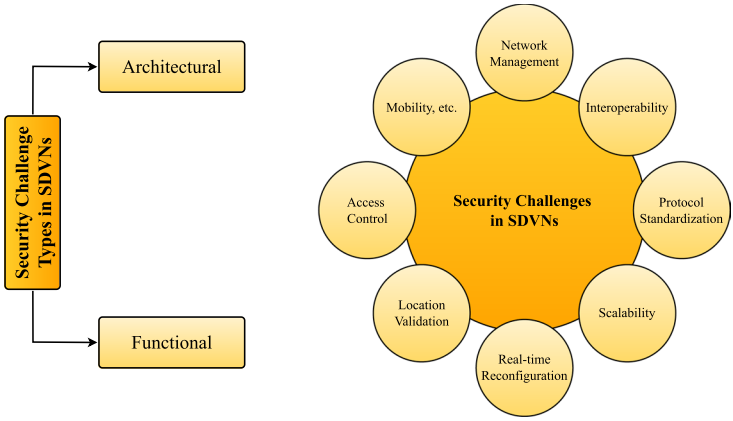
strengthens security measures in mobile edge computing. The complexity of the 5G vehicle environment is covered in the work mentioned in [16]. Numerous security calls are required due to the variety of automobile use cases. To tackle the security challenges, simple and adaptable paradigms are also required. SDVN makes use of SDN's advantages while attempting to handle the security implications for 5G automobile systems. The work describes the outcomes, security risks, and opportunities related to telcos' use of cyber-security services. 5G-based networks and important drivers like VANETs, etc., have also been described in [37] with an emphasis on some security challenges. Future SDN and VANET-based applications are the main focus of intelligent vehicular networks, and associated services are considered in order to adjust security measures.

6 Security challenges in SDVNs

As per the existing literary works, there are multiple security challenges w.rt. SDWNs. This section examines some of the common security challenges, as well as related literary works. According to [13], the main issues in software-defined VANETs have always been the deployment and integration of technology components. The study examines the most recent SDVN architectural elements and their corresponding difficulties. The primary security difficulties for preserving security services including authentication, secrecy, availability, and data integrity are highlighted in the text. Future SDVN systems' main difficulties have also included provisioning and privacy management solutions. The study examined in [44] looks into current developments in SDVN research. The study organizes and classes SDVN ideas and creates a taxonomy based on fundamental features to emphasize the function of network architectural elements, operational modes, etc. The paper also lists and describes potential future research difficulties related to SDVNs. Some of the common security challenges are listed in the form of Fig. 6. The in-detail comparison of some SDVN-based works w.r.t. security solutions are detailed in Table 5.

6.1 Architectural

Despite all the potential advantages of new SDVNs, [14] states that the main difficulties lie in realizing their full potential and handling security worries. The realistic conversion of conventional vehicle networks into cutting-edge SDVNs has also been a significant problem. Additionally, it is important to consider the security and reliability concerns in SDVNs since the centralization of network intelligence may lead to an increase in online threats and cyberattacks. Therefore, it is difficult to create new architectural elements to fend off potential security concerns. Other significant problems include developing effective and secure user interfaces, inter-layer API connections, and risk mitigation. According to [12], the unique characteristics of SDN assist to utilize the vehicular networks, however implementing flexibility, programmability, etc., in SDVNs is not a simple process. The construction of the SDN-based VANET system as a whole, combining its potential opportunities, diverse



(a) Security Challenge Categorization (b) Some examples of Security challenges

Fig. 6 General categorization and common security challenges in SDVNs

architectural components, use cases, and opportunities, has been the main problem. This is despite the fact that many previous works emphasize the SDN-based VANET designs. The paper discusses the problems and unresolved research questions as well as the taxonomy of SDVNs.

The work described in [45] emphasizes the worries for the security and safety of drivers. The standards for the safety, comfort, and entertainment services are also included in the job. High mobility, sporadic connection, heterogeneity, etc., stand out as some of the primary issues of applications since the present rigid architecture of VANETs has not been greatly changed. SDN helps to address these problems, but its effects and implementation problems are different concerns that need also be taken into account. Due to the instability of the wireless medium, the difficulties associated with VANETs have also been explored in [9]. Applications with a range of needs must be supported. The article conducts a comprehensive assessment of SDN approaches optimized for VANET systems and identifies SDN as a key solution. Focus has also been placed on current standardization initiatives, active research areas, and significant problems.

6.2 Functional

SDVNs have been the subject of research, however managing and deploying them presents several difficulties. This is brought on by the rigid architecture, inadequate scalability, limited connection, etc. Modern cutting-edge technologies, such cloud, fog, and SDN, aid in addressing these problems, according to [46]. However, a number of challenges, including effective global network management, timely distribution of safety alerts, adequate deployment of cloud-based techniques, etc., create questions as per [47]. As SDN-based VANETs are supposed to be the key enablers of 5G technology, authors highlight the roles, services, and challenges in [17]. SDN helps to enhance the efficiency of VANET, however the security remains a major

Table 5 Comparative analysis of some SDVN-based works w.r.t. security challenges

References	Network management	Interoperability	Protocol standardization	Scalability	Real-time reconfiguration	Location validation	Access control	Mobility
Cardona et al. [9]	✓	✓	✓	×	✓	×	×	✓
Ben et al. [13]	✓	×	✓	✓	✓	×	✓	✓
Akhunzada et al. [14]	✓	✓	✓	✓	×	×	✓	✓
Sultana et al. [17]	✓	✓	✓	✓	✓	×	✓	✓
Wang et al. [18]	✓	✓	×	×	✓	×	×	✓
Arif et al. [19]	×	✓	×	✓	×	×	×	✓
Raja et al. [36]	✓	×	×	✓	×	✓	×	✓
Yaqoob et al. [44]	✓	✓	✓	✓	✓	×	✓	✓
Chahal et al. [45]	✓	×	×	✓	✓	×	×	✓

issue. SDN-based VANETs introduce new security issues such as effective integration of new components and technologies, and improved and secured architectural design of the network. The work discussed in [18] highlights the significance of vehicular networks in the realization of Internet of Everything (IoE). The work details the need of emerging applications in vehicular networks in the form of rich resources and flexible management. Cloud computing and SDN help to solve these problems. The work discussed in [20] provides an in-depth analysis of the issues related with the use of machine learning in vehicular networks. Furthermore, the authors discuss several possible security risks linked with the use of ML approaches, and focus on adversarial ML attacks against CAVs in particular. In addition to this, the authors also present a strategy to protect against adversarial assaults in a variety of network scenarios. Based on the research mentioned in [19], security has grown to be a significant issue in SDN-based VANETs. Concerns are raised by the impact of both conventional and new attacks, potential dangers, and vulnerabilities. The article discusses potential security breaches in upcoming SDN-based VANETs. Despite the fact that SDN-based VANETs provide unique advantages in terms of services and applications, some significant challenges, such as the proper deployment of SDN controllers, effective communication strategies, and secure data transfer, must be overcome.

Although authors emphasize roles and duties in [21], it is necessary to redefine existing vehicular routing algorithms in order to support cutting-edge communication in SDVNs. The article also describes the design-principle problems with SDVN routing systems and provides a thorough examination of routing alternatives with an emphasis on the unresolved problems. Some significant difficulties in the design of SDVNs are also highlighted in the study cited in [48]. The low latency requirement, short link duration, and massive network size are described in detail.

7 Opportunities in SDVNs

Vehicular networks may rely on a variety of heterogeneous wireless networking technologies, which can make meeting various QoS criteria for vehicular transport services difficult. Traditional vehicle networks are incapable of meeting the increasing needs of a highly dynamic network environment. SDN, on the other hand, serves the dynamic environment of automotive networks while minimizing administrative overhead due to its flexible centralized structure. An SDN-based load balancer can assist in balancing traffic load in RSUs so that available resources in SDVNs can be used more efficiently. SDN's programmability can aid in the speedy and autonomous construction of vehicle networks. Furthermore, SDN allows network service providers to install network pieces in software form.

The work discussed in [42] explores the advances in SDN-based architecture for rapid innovation in vehicular networks. The work discusses the various opportunities in SDVN such as agile configuration, heterogeneity management, adaptive protocol deployment, and multiple tenant isolation. The work also explores the opportunities in terms of feasible and effective network management. Authors details multiple opportunities w.r.t. SDVNs in [48]. Some of the common opportunities are

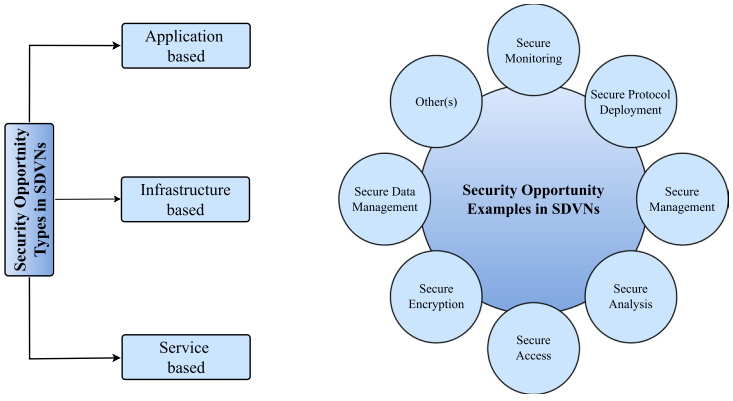
mentioned in the form of simpler network management, better network performance, and faster network innovation. Some of the common opportunities in SDVNs are listed in the form of Fig. 7. Additionally, the in-detail comparison of some SDVN based works w.r.t. security solutions are detailed in Table 6.

7.1 Application based

In [16], numerous prospects related to the 5G-SDVN applications have been highlighted. It is possible to manage the ecosystem in an easy and flexible way thanks to the variety of automotive applications and security needs. SDVNs use the SDN's ground-breaking advantages to enhance the state of the present vehicular systems. The article examines the advantages of security and the potential for cyber-security services. The work discussed in [9] describes a thorough analysis of SDN application for VANETs. The research looks on the architectural and communication potential of SDVNs. The paper highlights open research application possibilities, standardization initiatives, and adaptable architectures such as programmable network flow management.

7.2 Infrastructure based

The work illustrated in [43] examines the infrastructure technologies that will enable 5G in vehicle networks. User throughput and traffic capacity may be increased by network densification. Vehicular neighbor groups are created to improve the network services by organizing them effectively. The SDN characteristics of the 5G-SDVNs are used to dynamically manage the 5G network's vehicular neighbor groups. Mobile edge computing also contributes to improving network control. Through its excellent qualities, SDN enhances mobile edge computing and aids in streamlining network administration. In [44], SDVNs have been addressed in relation to



(a) Security opportunity Categorization (b) Some examples of Security opportunities

Fig. 7 General categorization and common security opportunities in SDVNs

Table 6 Comparative analysis of some SDVN-based works w.r.t. related opportunities

References	Global monitoring	Agile network management	Real-time programming	Flexible architecture	Other(s)
Cardona et al. [9]	✓	×	✓	×	Offers diverse control and programmability levels in data plane. Exhibits the role of SDVNs as a complementary technology in the effective implementation of MEC, VCC, and NFV
Lacoste et al. [16]	✓	×	✓	✓	Discusses issues such as mobility management, heterogeneous inter-networking, and security. Highlights the role of SDVNs in automotive cyber-security
Zhao et al. [21]	×	×	×	×	Presents design principles of routing schemes in SDVN. Explores SDVN potential w.r.t routing
He et al. [42]	✓	✓	✓	✓	Improved network resource utilization, and rapid network configuration
Huang et al. [43]	✓	×	✓	✓	Discusses efficient data sharing and ubiquitous mobile interaction. Details reliable resource cooperation
Yaqoob et al. [44]	×	×	✓	✓	Discusses flexible centralized SDN and dynamic vehicular networks with minimum management overhead
Toufga et al. [49]	✓	×	×	×	Helps in the adaptive readjustment of the number and placement of controllers. Details various challenges in the adaptive placement of controllers
Zhao et al. [50]	✓	✓	✓	×	Offers Reinforcement Learning-based insights to adjust the policies intelligently based on real-time traffic. Highlights loss-aware negative update mechanism to avoid bad policies
Ni et al. [51]	✓	×	×	×	Highlights various opportunities such as network planning and infrastructure deployment and data processing and management. Discusses optimal control algorithm design and Security and privacy issues
Sudheer et al. [52]	✓	×	×	×	Uses global network view to scrutinize the links' stability. Helps to minimize the number of exchange-messages between the control and data planes

the efficient creation of software-based configurable infrastructure. SDN provides adaptability and programmability to enhance VANET performance and network administration. Investigating recent research developments, the paper also emphasizes various access methods, network infrastructure elements, and potential. As per [49], SDVNs aid in enhancing vehicular networks' flexibility and effectiveness of administration. This makes ITSs more likely to appear. This opens the door for the successful application of IoT and Cyber Physical Systems (CPS). SDN contributes to keeping vehicle networks active. Additionally, there are better ways to deal with the rapid changes in road traffic. In [50] with regard to VANETs, the dynamic traffic information, current routing algorithms, associated concerns, local optimums, path redundancy, congestion, etc., are covered. The study examines the different benefits that SDN brings to VANETs, including a global view of traffic, effective routing table upkeep, simple data packet prioritization, etc. The paper describes connection stability difficulties as well as potential real-time routing table update opportunities with enhanced network regulations.

7.3 Service based

Data distribution is a difficult problem that has been discussed in [51] in regard to vehicle networks. The increased mobility in automobile networks makes it difficult to efficiently use the constrained wireless resources. Other unresolved challenges are diverse safety and multimedia services. The advantages of SDN and the many prospects made possible by SDVNs are highlighted in this paper. To demonstrate the benefits of the SDVN framework over conventional designs, the communication technologies for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I), as well as associated network performance and quality of service (QoS), have been examined. The authors identify different SDVN-related opportunities in [21]. The paper emphasizes the potential for effective routing protocols in SDVNs. By doing so, the performance of the network as a whole will be enhanced, and flow management problems will be reduced. In order to provide a thorough overview, the paper analyses the design concepts of SDVNs and examines their potential. The discussion of increased QoS, scalability, flexibility, and administration potential in SDVNs concludes the paper. The article cited as [52] discusses the effective data transfer in SDVNs. Links grow weak as a result of the data transmission's intrinsic dynamic nature. Conventional VANET protocols suffer in these circumstances, whereas SDN supports improved routing by effectively monitoring the network traffic. Examining the dynamic nature of wireless networks is made possible by the suggested packet routing system. The work emphasizes the stability of the routes in addition to determining the quickest path.

Finally, it can be concluded from the above discussion, that there are some open research challenges in the current state-of-the-art. Some of them are [29]: (1) Due to privacy issues and significant deployment complexity, implementing machine learning based systems correctly and effectively is difficult to manage the mobility related issues; (2) Maintaining constant connectivity with the controller is a challenging task in addition to mobility management in SDVNs; (3) To meet the critical needs

of the wide range of new VANET applications, the flow rules and policies that now control data transfer in the SDN network must be improved; (4) Additionally, different attacks can be conducted to stop controllers from operating. Since the controller is the main decision-making unit in SDVNs, its security becomes a concern; (5) Considerably in SDN-only networks, optimizing controller placement is a difficult issue. Furthermore, it is even more difficult in SDVNs because of the extra VANET components and features. All these factors must be taken into account while designing a suitable controller placement scheme.

8 Conclusion and future work

Smart transportation systems have been under active exploration considering the rapid and advanced level development of smart cities. Existing transportation systems are not capable of offering the kind of support which is expected in a smart city environment. SDVNs promise that support in terms of smart transportation in a truly smart city environment. However, there have been some serious network performance-related concerns including efficient routing, authenticity, security, etc., that attract the attention of the community researchers. Among all these issues, security is of paramount importance due to the open attack surface in a digital environment of smart cities. Thus, this work tries to offer a comprehensive research survey from a security perspective on SDVNs which is expected to motivate the researchers to explore more opportunities in this domain.

The work discusses the basic design components to offer a fundamental understanding of SDVN architectures using the System components, Operational modes, Services, Architectural components, and Access Technologies. Further, the state-of-the-art is explored to state the current developments in the field including Architecture, Services, and Security. The article also highlights the security issues w.r.t. the architectural and functional designs. Thereafter, the relevant security solutions are detailed highlighting the Services, Infrastructure, and Applications. Thereafter, authors discuss the Architectural development, Orchestration, Network management, Security offerings, etc. as challenges. Lastly, the work extends further and illustrates different opportunities in the field based on Traffic management, QoS, Device configuration, Routing, etc.

Acknowledgements The authors are thankful to the peer research community for the regular suggestions and criticism.

Author contributions RK has done the conceptualization, methodology, draft writing, figures preparation, and final review. NA has done the draft writing, figures preparation, and final review.

Funding There is no funding associated with this article.

Availability of data and materials Not applicable.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

Ethics approval and consent to participate Not applicable.

Consent for publication We, the authors, give our consent for the publication of this work in The Journal of Supercomputing.

References

1. Celes C, Boukerche A, Loureiro AA (2020) From mobility traces to knowledge: design guidance for intelligent vehicular networks. IEEE Netw 34(4):227–233. https://doi.org/10.1109/MNET.011.1900499
2. Jabbarpour MR, Marefat A, Jalooli A, Zarrabi H (2019) Cloud-based vehicular networks: a taxonomy, survey, and conceptual hybrid architecture. Wirel Netw 25(1):335–354. https://doi.org/10.1007/s11276-017-1563-5
3. Menouar H, Guvenc I, Akkaya K, Uluagac AS, Kadri A, Tuncer A (2017) UAV-enabled intelligent transportation systems for the smart city: applications and challenges. IEEE Commun Mag 55(3):22–28. https://doi.org/10.1109/MCOM.2017.1600238CM
4. Lu Z, Qu G, Liu Z (2018) A survey on recent advances in vehicular network security, trust, and privacy. IEEE Trans Intell Transp Syst 20(2):760–776. https://doi.org/10.1109/TITS.2018.2818888
5. Tang F, Mao B, Kato N, Gui G (2021) Comprehensive survey on machine learning in vehicular network: technology, applications and challenges. IEEE Commun Surv Tutor 23(3):2027–2057. https://doi.org/10.1109/COMST.2021.3089688
6. Agrawal N, Tapaswi S (2021) An SDN-assisted defense mechanism for the shrew DDoS attack in a cloud computing environment. J Netw Syst Manag 29(2):1–28. https://doi.org/10.1007/s10922-020-09580-7
7. Bekri W, Jmal R, Chaari Fourati L (2020) Internet of things management based on software defined networking: a survey. Int J Wirel Inf Netw 27:385–410. https://doi.org/10.1007/s10776-020-00488-2
8. Kim S (2019) Effective crowdsensing and routing algorithms for next generation vehicular networks. Wirel Netw 25(4):1815–1827. https://doi.org/10.1007/s11276-017-1632-9
9. Cardona N, Coronado E, Latré S, Riggio R, Marquez-Barja JM (2020) Software-defined vehicular networking: opportunities and challenges. IEEE Access 8:219971–219995. https://doi.org/10.1109/ACCESS.2020.3042717
10. Ge X, Li Z, Li S (2017) 5G software defined vehicular networks. IEEE Commun Mag 55(7):87–93. https://doi.org/10.1109/MCOM.2017.1601144
11. Ferrús R, Koumaras H, Sallent O, Agapiou G, Rasheed T, Kourtis MA, Ahmed T (2016) SDN/NFV-enabled satellite communications networks: opportunities, scenarios and challenges. Phys Commun 18:95–112. https://doi.org/10.1016/j.phycom.2015.10.007
12. Bhatia J, Modi Y, Tanwar S, Bhavsar M (2019) Software defined vehicular networks: a comprehensive review. Int J Commun Syst 32(12):e4005. https://doi.org/10.1002/dac.4005
13. Ben Jaballah W, Conti M, Lal C (2019) A survey on software-defined VANETs: benefits, challenges, and future directions. arXiv e-prints, arXiv-1904
14. Akhunzada A, Khan MK (2017) Toward secure software defined vehicular networks: taxonomy, requirements, and open issues. IEEE Commun Mag 55(7):110–118. https://doi.org/10.1109/MCOM.2017.1601158
15. Islam MM, Khan MTR, Saad MM, Kim D (2021) Software-defined vehicular network (SDVN): a survey on architecture and routing. J Syst Archit. https://doi.org/10.1016/j.sysarc.2020.101961
16. Lacoste M, Armand D, L'Hereec F, Prévost F, Rafflée Y, Roché S Software-defined vehicular networking security: threats and security opportunities for 5G
17. Sultana R, Grover J, Tripathi M (2021) Security of SDN-based vehicular ad hoc networks: state-of-the-art and challenges. Veh Commun. https://doi.org/10.1016/j.vehcom.2020.100284
18. Wang Q, Gao D, Zhu W (2019) Cloud-enabled software-defined vehicular networks: architecture, applications and challenges. J Internet Technol 20(6):1819–1828
19. Arif M, Wang G, Geman O, Balas VE, Tao P, Brezulianu A, Chen J (2020) Sdn-based vanets, security attacks, applications, and challenges. Appl Sci 10(9):3217. https://doi.org/10.3390/app10093217

20. Qayyum A, Usama M, Qadir J, Al-Fuqaha A (2020) Securing connected & autonomous vehicles: challenges posed by adversarial machine learning and the way forward. IEEE Commun Surv Tutor 22(2):998–1026. https://doi.org/10.1109/COMST.2020.2975048
21. Zhao L, Al-Dubai A, Zomaya AY, Min G, Hawbani A, Li J (2020) Routing schemes in software-defined vehicular networks: design open issues and challenges. IEEE Intell Transp Syst Mag. https://doi.org/10.1109/MITS.2019.2953557
22. Sadio O, Ngom I, Lishou C (2019) Design and prototyping of a software defined vehicular networking. IEEE Trans Veh Technol 69(1):842–850. https://doi.org/10.1109/TVT.2019.2950426
23. Zhao L, Han G, Li Z, Shu L (2020) Intelligent digital twin-based software-defined vehicular networks. IEEE Netw 34(5):178–184. https://doi.org/10.1109/MNET.011.1900587
24. Cooper C, Franklin D, Ros M, Safaei F, Abolhasan M (2016) A comparative survey of VANET clustering techniques. IEEE Commun Surv Tutor 19(1):657–681. https://doi.org/10.1109/COMST.2016.2611524
25. Deng DJ, Lien SY, Lin CC, Hung SC, Chen WB (2017) Latency control in software-defined mobile-edge vehicular networking. IEEE Commun Mag 55(8):87–93. https://doi.org/10.1109/MCOM.2017.1601165
26. Aljeri N, Boukerche A (2020) A distributed topology discovery protocol for software-defined vehicular networks. In: Proceedings of the 17th ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks, pp 17–24. https://doi.org/10.1145/3416011.3424758
27. Yan X, Dong P, Du X, Zheng T, Sun J, Guizani M (2018) Improving flow delivery with link available time prediction in software-defined high-speed vehicular networks. Comput Netw 145:165–174. https://doi.org/10.1016/j.comnet.2018.08.019
28. Maity I, Dhiman R, Misra S (2021) MobiPlace: mobility-aware controller placement in software-defined vehicular networks. IEEE Trans Veh Technol 70(1):957–966. https://doi.org/10.1109/TVT.2021.3049678
29. Jaballah WB, Conti M, Lal C (2020) Security and design requirements for software-defined VANETs. Comput Netw 169:107099. https://doi.org/10.1016/j.comnet.2020.107099
30. Tanwar S, Vora J, Tyagi S, Kumar N, Obaidat MS (2018) A systematic review on security issues in vehicular ad hoc network. Secur Priv 1(5):e39. https://doi.org/10.1002/spy2.39
31. Kurugollu F, Ahmed SH, Hussain R, Ahmad F, Kerrache CA (2020) Vehicular sensor networks: applications. Adv Chall Sens 20(13):3686. https://doi.org/10.3390/s20133686
32. Mendiboure L, Chalouf MA, Krief F (2020) A scalable blockchain-based approach for authentication and access control in software defined vehicular networks. In: 2020 29th International Conference on Computer Communications and Networks (ICCCN), pp 1–11. IEEE. https://doi.org/10.1109/ICCCN49398.2020.9209661
33. Xu H, Dong M, Ota K, Wu J, Li J (2019) Toward software defined dynamic defense as a service for 5G-enabled vehicular networks. In: 2019 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), pp 880–887. IEEE. https://doi.org/10.1109/iThings/GreenCom/CPSCom/SmartData.2019.00158
34. Nayak RP, Sethi S, Bhoi SK, Mohapatra D, Sahoo RR, Sharma PK, Puthal D (2022) TFMD-SDVN: a trust framework for misbehavior detection in the edge of software-defined vehicular network. J Supercomput. https://doi.org/10.1007/s11227-021-04227-z
35. Raut UK, Rawat MK (2020) Secure software defined vehicular network (SDVN). Int J Adv Sci Technol 29(7s):5284–5292
36. Raja G, Anbalagan S, Vijayaraghavan G, Dhanasekaran P, Al-Otaibi YD, Bashir AK (2020) Energy-efficient end-to-end security for software defined vehicular networks. IEEE Trans Indus Inf. https://doi.org/10.1109/TII.2020.3012166
37. Shrestha R, Nam SY, Bajracharya R, Kim S (2020) Evolution of V2X communication and integration of blockchain for security enhancements. Electronics 9(9):1338. https://doi.org/10.3390/electronics9091338
38. Mikavica B, Kostić-Ljubisavljević A (2021) Blockchain-based solutions for security, privacy, and trust management in vehicular networks: a survey. J Supercomput 77(9):9520–9575. https://doi.org/10.1007/s11227-021-03659-x
39. de Sousa RS, da Costa FS, Soares AC, Vieira LF, Loureiro AA (2018) Geo-sdvn: a geocast protocol for software defined vehicular networks. In: 2018 IEEE International Conference on Communications (ICC), pp 1-6. IEEE. https://doi.org/10.1109/ICC.2018.8422755

40. Rahouti M, Xiong K, Xin Y (2020) Secure software-defined networking communication systems for smart cities: current status, challenges, and trends. IEEE Access 9:12083–12113. https://doi.org/10.1109/ACCESS.2020.3047996
41. Yu Y, Guo L, Liu Y, Zheng J, Zong Y (2018) An efficient SDN-based DDoS attack detection and rapid response platform in vehicular networks. IEEE Access 6:44570–44579. https://doi.org/10.1109/ACCESS.2018.2854567
42. He Z, Cao J, Liu X (2016) SDVN: Enabling rapid network innovation for heterogeneous vehicular communication. IEEE Netw 30(4):10–15. https://doi.org/10.1109/MNET.2016.7513858
43. Huang X, Yu R, Kang J, He Y, Zhang Y (2017) Exploring mobile edge computing for 5G-enabled software defined vehicular networks. IEEE Wirel Commun 24(6):55–63. https://doi.org/10.1109/MWC.2017.1600387
44. Yaqoob I, Ahmad I, Ahmed E, Gani A, Imran M, Guizani N (2017) Overcoming the key challenges to establishing vehicular communication: Is SDN the answer? IEEE Commun Mag 55(7):128–134. https://doi.org/10.1109/MCOM.2017.1601183
45. Chahal M, Harit S, Mishra KK, Sangaiah AK, Zheng Z (2017) A survey on software-defined networking in vehicular ad hoc networks: challenges, applications and use cases. Sustain Cities Soc 35:830–840. https://doi.org/10.1016/j.scs.2017.07.007
46. Agrawal N (2021) Dynamic load balancing assisted optimized access control mechanism for edge-fog-cloud network in internet of things environment. Concurr Comput Pract Exp. https://doi.org/10.1002/cpe.6440
47. Agrawal N (2021) Autonomic cloud computing based management and security solutions: state-of-the-art, challenges, and opportunities. Trans Emerg Telecommun Technol. https://doi.org/10.1002/ett.4349
48. Zhu M, Cai ZP, Xu M, Cao JN (2015) Software-defined vehicular networks: opportunities and challenges. CRC Press, Energy Science and Applied Technology, pp 247–251
49. Toufga S, Abdellatif S, Assouane HT, Owezarski P, Villemur T (2020) Towards dynamic controller placement in software defined vehicular networks. Sensors 20(6):1701. https://doi.org/10.3390/s20061701
50. Zhao L, Bi Z, Lin M, Hawbani A, Shi J, Guan Y (2021) An intelligent fuzzy-based routing scheme for software-defined vehicular networks. Comput Netw 187:107837. https://doi.org/10.1016/j.comnet.2021.107837
51. Ni Y, He J, Cai L (2017) Data dissemination in software-defined vehicular networks. In: 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall), pp 1-5. IEEE. https://doi.org/10.1109/VTCFall.2017.8288206
52. Sudheer KK, Ma M, Chong PHJ (2017) Link dynamics based packet routing framework for software defined vehicular networks. In: GLOBECOM 2017-2017 IEEE Global Communications Conference, pp 1-6. IEEE. https://doi.org/10.1109/GLOCOM.2017.8254597

Authors and Affiliations

Rohit Kumar[1] · Neha Agrawal[2]

Rohit Kumar
rohitk@srmist.edu.in

[1] SRMIST-KTR, Chennai, TN, India

[2] CSE Group, Indian Institute of Information Technology Sri City, Chittoor, AP, India