Computer Networks 169 (2020) 107099

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Security and design requirements for software-defined VANETs

Wafa Ben Jaballah [a], Mauro Conti [b], Chhagan Lal [c,d]

[a] Department of cyber security R&D lab, 17 Rue de l'Arrivée, 75015 Paris, France
[b] Department of Mathematics, University of Padua, Italy
[c] Manipal University Jaipur, Jaipur, India
[d] Department of Mathematics, University of Padua, Via Trieste, 63-35131, Padua, Italy

ARTICLE INFO

Article history:
Received 24 May 2019
Revised 3 January 2020
Accepted 3 January 2020
Available online 10 January 2020

Keywords:
Security
VANETs
Software defined networking
5G
Networking attacks
Wireless channels
Edge/Fog computing

ABSTRACT

The evolving of Fifth Generation (5G) networks is becoming more readily available as a significant driver of the growth of new applications and business models. Vehicular Ad hoc Networks (VANETs) and Software Defined Networking (SDN) represent the critical enablers of 5G technology with the development of next-generation intelligent vehicular networks and applications. In recent years, researchers have focused on the integration of SDN and VANET, and looked at different topics related to the architecture, the benefits of software-defined VANET services, and the new functionalities to adapt them. However, the security and robustness of the complete architecture is still questionable and have been largely neglected by the research community. Moreover, the deployment and integration of different entities and several architectural components drive new security threats and vulnerabilities.

In this paper, first, we survey the state-of-the-art SDN based Vehicular ad-hoc Network (SDVN) architectures for their networking infrastructure design, functionalities, benefits, and challenges. Then we discuss these architectures against major security threats that violate the key security services such as availability, privacy, authentication, and data integrity. We also discuss different countermeasures for these threats. Finally, we present the lessons learned with the directions of future research work towards provisioning stringent security solutions in new SDVN architectures. To the best of our knowledge, this is the first work that presents a comprehensive survey and security analysis on SDVN architectures, and we believe that it will help researchers to address various challenges (e.g., flexible network management, control and high resource utilization, and scalability) in vehicular communication systems which are required to improve the future Intelligent Transportation Systems (ITS).

1. Introduction

With the pervasive use of smart devices and advances in the development of wireless access technologies (e.g., DSRC, WiFi, 4G/LTE, and 5G), the VANETs have become an accessible technology for improving road safety and transportation efficiency [1]. Due to continuous advancements in VANET technologies, it is seen as a network that can provide various services like vehicular cloud computing [2], surveillance, Internet of Thing (IoT) based advertising [3], safety traffic management, to name a few. Although heterogeneous future architectures have been extensively investigated, the VANET's salient features (e.g., varying node density, high mobility) makes it challenging to efficiently coordinate services with diverse Quality of Service (QoS) requirements. Hence, programmable networking architectures are becoming critical enablers for VANETs to support inter-operation among underlying heterogeneous networks, conduct resource allocation tasks, and effectively manage a vast number of mobile users with heterogeneous smart devices.

In recent years, SDVN architectures have been emerged as a promising technology to simplify network management and enable innovation through network programmability. Thus, it gains significant attention from academia and industry. The SDN technology allows the decoupling of control and data planes in SDVNs, which provides: (i) an abstraction for VANET applications to the underlying networking infrastructure, and (ii) a logically centralized networking intelligence and network state.

The convergence of SDN with VANET is seen as an important direction that can address most of the VANET's current challenges [4]. The use of SDN's prominent features provides the needed support to VANET applications to enhance the user experience. Moreover, the SDN features can meet the advanced demands of VANETs like high throughput, high mobility, low com-

E-mail addresses: wafa.benjaballah@thalesgroup.com (W. Ben Jaballah), conti@math.unipd.it (M. Conti), chhagan@math.unipd.it (C. Lal).

https://doi.org/10.1016/j.comnet.2020.107099
1389-1286/

munication latency, heterogeneity, and scalability. In particular, the inherent features of SDN include: (i) flexibility through dynamic programmability on networking elements, (ii) support for heterogeneous applications through network virtualization, and (iii) efficient management of various services using centralized global network knowledge. These features of SDN could help to ensure secure and efficient deployment of different VANET services. For instance, multimedia streaming services could be adequately supported through SDN by dynamically adapting to topology changes, and the global topology information could help better route planning. In SDVN architecture, the controller could create the network's comprehensive view by collecting data from heterogeneous SDN-enabled VANET entities, e.g., Road Side Unit (RSU), Road Side Unit Controller (RSUC), and Base Station (BS). The network applications running on top of the SDN control plane could use global information from the controller to implement and enforce different network policies/configurations on the data plane devices. The applications communicate with the SDN controller via North-Bound Interface (NBI) protocols. To produce coordinated and optimal decisions for the vehicles, the SDN controller enforces required configurations to the data plane elements by accessing them through South-Bound Interface (SBI) protocols.

Some of the above mentioned inherent features of SDN also makes it vulnerable to different security threats, such as (i) the support for dynamic programmability and availability of global information at controller could be exploited by adversaries through NBI [5] to abuse networking resources and to perform policy manipulations at data plane elements, and (ii) the centralised nature of SDN controller increases the possibilities of single-point failure and makes it an easy target for attackers to perform traditional attacks, such as denial of service, and network resource exhaustion. Moreover, man-in-the-middle attacks could be performed through SBI communication channels due to a lack of transport layer security.

1.1. Motivation and contributions

Although there are various research efforts done to provide efficient and feasible SDVN architectures, however, exploiting the full potential of SDN technology for new VANET applications is still at its initial stages. Moreover, during the design of SDVNs, the security aspects should be considered as a critical requirement and an equally pressing issue. The full transformation of existing VANETs into SDVNs will remain uncertain as long as the SDN issues, such as security, scalability, and data communication reliability, have not been sufficiently addressed. It is because there is a high possibility that the use of virtual centralization of network logic control (or intelligence) and the rapidly increasing cyber-attacks could make the emerging SDVNs more vulnerable to threats than the current VANETs. Furthermore, the new entities and structural components that are being used in the current SDVNs might be opening a new attack surface and vulnerabilities, which are unknown at the present stage. Consequently, it is required: (i) to perform a thorough investigation of the standardization efforts, and (ii) to address challenging issues (both, old and new) in the SDVNs.

There exist few previous efforts such as [6–9], that provides a short survey on SDVNs. Authors in [6] give a brief discussion on the Software-Defined Internet of Vehicles (SD-IoV) architectures along with their challenges and possible solutions to address them. The authors mainly focus on the implementation progress of various types of networks (e.g., IoT, IoV, WSN, and cellular network) by using SDN technology. Similarly, authors in [7] provide an overview of critical challenges in vehicular communications, and they discuss the usage of SDN to address the identified problems. Authors in [8] survey the research works done on SDN-based wireless and mobile networks with a primary focus on VANETs. Authors in [9] provide a brief study on SDN-based VANETs that includes SDVNs functionality details, possible security threats to SDVNs, and benefits of SDVNs over the state-of-the-art. However, the study does not include the importance and effects of the integration of emerging technologies with SDVNs, and it also lacks to provide a complete and comprehensive view of the attack surface considering different planes of SDVNs. In particular, none of these works provides an in-depth survey on state-of-the-art SDVN architectures with a specific focus on security and reliability of the data communication system. Also, these surveys cover the research work done till mid-2017, but most of the research concerning the practical usage of SDVNs for different real-world applications has been done in recent years, which is not covered in [6–8] works. Moreover, these works do not consider the new technologies such as Blockchain [10], fog computing [11], and 5G [12] that are being used recently to improve the SDVNs overall performance and its application areas significantly.

In this paper, first, we thoroughly discuss the working methodology of state-of-the-art SDVN architectures and provide a generic design of vehicular network architecture integrated with SDN and other novel paradigms. We also investigate these architectures to identify their benefits and challenges against the traditional VANETs, mainly regarding the security and the communication reliability parameters. Then we present a set of potential requirements and primary enablers for a secure SDVN while we perform a security analysis of the existing SDVNs. Finally, an array of open research issues are presented that require the attention of the researchers and professionals to establish a way forward towards a more secure and efficient SDVN that could enable the VANET usage in next-generation VANET applications. In particular, this paper provides the following key contributions.

- We survey the state-of-the-art SDVN solutions for their benefits and challenges, mainly regarding the security and performance of data communication processes. We believe that our survey will provide the required insights that will help to the possible development of a more secure and robust SDVN architecture. To the best of our knowledge, it is the first comprehensive work that presents such a survey and analysis on SDVNs. Based on our study, we also provide a generic design of SDVN architecture.
- We present a detailed security analysis considering an array of security threats along with their existing and possible countermeasures for the current SDVN architectures. Our report includes the security threats coming from the individual technologies (i.e., SDN only or VANET only), and the threats that result from the integration of SDN and VANETs (i.e., SDVNs). Finally, we discuss the lessons learned with the directions of future research work.

1.2. Organization

The rest of our paper is organized as follows. In Section 2, we discuss the essential background overview of the VANET, SDN, and few emerging technologies that are being integrated with SDVNs to improve one or more of its functionalities. In Section 3, we provide the design of a generic SDVN architecture along with the survey of the state-of-the-art SDVN architectures. Section 4 discusses the benefits and challenges of the existing SDVN architectures. In Section 5, we present security analysis against an array of threats that could be launched on the SDVN architectures, and we discuss the current and new possible solutions to countermeasure these threats. The lessons learned and the possible directions for future work are given in Section 6. Finally, we conclude the paper in Section 7.

2. Background overview

In this section, we provide a brief overview of VANET (in Section 2.1) and SDN (in Section 2.2) technologies along with their working methodology, benefits, and challenges. Moreover, we present an overview of the emerging technologies whose integration with SDVNs is being envisioned shortly, these include 5G, edge computing, and Named Data Networking (NDN). Here, we only provide the details which are essential to understand the SDVN architectures that we survey and investigate in the later sections of this paper. The comprehensive overview of these two networking technologies is out of the scope of this paper, and we direct the interested readers to detailed surveys given in [13] and [1].

2.1. Introduction to VANETs

In this section, we briefly overview the main components of VANET architecture, the communication domains, the wireless technology, and the reference vehicular applications.

2.1.1. VANET architecture

VANET is a self-configuring network [14], which has emerged due to the new advances in network technologies. The architecture of VANET is composed of three types of elements that are the On-Board Unit (OBU), the Road-Side Unit (RSU), and the Application Unit (AU). Nodes in VANETs are vehicles equipped with OBUs, which are wireless communication devices. This element is used for exchanging information between the vehicle with RSUs or between other vehicles or OBUs [15]. This OBU device uses an interface to connect to other OBUs. The OBU provides different services, such as routing and network congestion control. The second component, i.e., RSU, is a device or infrastructure deployed along the road-side or in dedicated locations (intersections) [16]. Depending on its functionality, the RSU can be equipped with one or more network devices. For instance, an RSU can use a dedicated short-range communication based on IEEE 802.11p [17], or it provides internet connectivity to other OBUs. The third component, i.e., AU, represents a device on-boarded inside the vehicle [18]. The AU communicates with the network via the OBU. It can be connected to the OBU through a wireless or wired connection.

2.1.2. Communications in VANETs

In the literature, the communications in VANETs can be divided into three types: (i) Intra-vehicle communication, (ii) Vehicle-to-Vehicle (V2V) Communication, and (iii) Vehicle to Infrastructure (V2I) communication. Intra-vehicle communication or in-vehicle communication refers to the interconnection of sensors and devices that are within the vehicle. In the intra-vehicle communication or in-vehicle communication, vehicles are equipped with different Electronic Control Units (ECUs), sensors, and actuators [19,20]. Intra-vehicle communication protocols vary from Local Interconnect Network, the Controller Area Network, the Media Oriented System Transport, the Ethernet, and Power Line Communications. In V2V communication, a vehicle communicates with another vehicle forming one-hop communication. Otherwise, if there is no direct connection, then vehicles execute a routing protocol to forward messages from one vehicle to another until it reaches the destination vehicle. V2V communications can enable new applications such as safety and entertainment/infotainment/online gaming services [21]. Most of these VANET applications are enabled by designing different routing protocols. Routing protocols vary from broadcasting protocols [22], route-discovery protocols [22], position-based protocols [23], to clustering-based protocols [24].

The V2I communication consists of a vehicle that communicates with an RSU to process applications, such as video streaming and advertisement dissemination. Vehicles transmit parameters to the RSU infrastructure in specific messages such as their position, their speed, and their direction. After collecting this information, the RSU will process it and provide the required services (video/multimedia streaming, location information, or advertisement dissemination depending on the position of the vehicle).

Third Generation Partnership Project (3GPP) group [25] defines another form of communication called vehicle to-X (V2X) communications that includes the V2V, V2I, and also vehicle-to-pedestrians communications. V2X communication enables many applications such as road safety, vehicle traffic optimization, infotainment services, cooperative collusion warning, in-vehicle Internet access, and remote vehicle diagnostics. Two technologies support V2X communications that are the dedicated short-range communications (DSRC) [26,27], and cellular network technologies [26,28,29]. In the following, we provide a brief overview of these two leading technologies.

2.1.3. DSRC and cellular technologies to support V2X applications

DSRC is a wireless technology used for vehicular applications via a short-range exchange of messages among the OBUs and the RSUs [27]. The DSRC reserves specific radio spectrum bands and depends on different regions such as Europe, North America, and Japan. Different DSRC standards are developed by various standardization bodies such as the European Telecommunications Standards Institute (ETSI) in Europe, and the IEEE in North America. For instance, V2V and V2I communications are supported by ITS-G5 [30], and IEEE 802.11 [31]; whereas the ASTM E2158-01 [32] supports the V2X communications. The two main limitations of DSRC in supporting V2X applications are related mainly to the short-range characteristic of DSRC, and the employment of the CSMA/CA technique as a main contention-based Medium Access Control (MAC) scheme. In particular, with using DSRC, a vehicle needs to be within a small coverage area of an RSU, and this might not be very easy to achieve when vehicles are moving with high speed [26]. To extend the coverage of RSU, the routing algorithms might require the use of multi-hop communications. However, the deployment of these algorithms will be limited by the intrinsic characteristics of VANETs that are dynamic network topology and vehicle densities. Moreover, another limitation of DSRC in supporting V2X applications is inherited from the use of CSMA/CA technique in a high vehicle density scenario [26]. As a consequence, it increases the channel contention between vehicles. Thus, it increases the number of message retransmissions and collisions.

Recent research efforts include the cellular technologies to enable V2X communications [28,29]. The main advantages of cellular technologies are the high network capacity and support for high bandwidth demand, and the wide cellular covered range compared to DSRC. These cellular technologies accelerate the deployment of V2X communications by providing high network capacity, which enables the support of high bandwidth demand and wide cellular coverage range. In [26], the authors present the main differences between DSRC and cellular V2X. There is also a clear strategy for 5*G* networks to provide reliability and ultra-low latency demands of V2V, V2I, and V2X applications [29,33].

2.1.4. VANET applications

V2V and V2I communications provide a large number of applications and disseminate a range of information to drivers and passengers. In the following, we overview safety and non-safety applications, with their characteristics and requirements.

Safety applications use wireless communications between vehicles or between vehicles and the infrastructures, to improve road safety and avoid accidents [21]. The primordial requirement of safety applications is the ability to collect information through different sensors installed in the vehicle, to process and disseminate

information in safety messages to other vehicles or with the infrastructure. Various applications emerge, such as Intersection Collision avoidance that relies mainly on V2I communication and uses a minimum of the frequency of 10 Hz and using a safety message with a communication range of 200–300 m. Other applications, such as public safety applications, aim to help drivers when an accident occurs and to support emergency vehicles. The frequency used by this application is 1hz and relies mainly on V2V and V2I communication. It uses specific safety messages that are triggered only in case of danger or accident, with a communication range of 300–1000 m. Another category of application is vehicle diagnostics and maintenance that aims to send notification messages to vehicles to remind drivers about safety problems. These applications rely on V2I communication and use specific safety messages with a communication range of 400 m [21].

The lane change warning application requires information from other vehicles and rely on V2V or V2I communications. It uses a frequency of 2–50 Hz with safety messages, and this also requires a communication range of 50–400 m. Safety messages are needed to have a complete view of the neighbors of a vehicle. These messages contain the state of the sending vehicles (i.e., position, direction, and speed) and data regarding the status of the neighboring vehicles.

The infotainment applications are referred to as non-safety applications. They aim to improve the comfort for drivers and passengers, and enhance traffic efficiency [34]. These applications require V2V or V2I communications. Similar to safety applications, infotainment applications share the requirements for quick and reliable message delivery to all vehicles in an area of interest. Safety applications have to generate a little burst of traffic for a short time. However, the infotainment applications generate a continuous flow of messages [34]. In this direction, approaches have been proposed in the literature to provide an intelligent selection of message forwarders and adapt the transmission rate [35,36]. However, the main limitations in case of infotainment applications are the redundant multi-hop transmissions, and the increasing number of collisions that affects the final performance of the system [34,37].

Another application is the smart parking that aims to assist drivers in finding parking slots [21]. OBUs and RSUs enable the information collection and sharing among vehicles and RSUs. The parking slot information is continuously disseminated among vehicles, and RSUs are responsible for caching and relaying the information to other vehicles nearby. The requirement of smart parking applications is the timely sharing and dissemination of parking lot information or updates.

Researchers and developers face several challenges when developing VANET applications, protocols, and simulation tools. Some researches have investigated the communication and networking aspects of VANET and addressed the security and privacy issues [34,37–39]. Others focus on the routing protocols for VANET and their requirements to achieve better communication time with less consumption of network bandwidth [36,40,41]. Recently, some research works also investigate on providing more reliable and efficient services by integrating heterogeneous access networks such as LTE, 5G, NDN, Edge computing, and SDN [42–45].

Literature shows that several security threats exist in VANETs, and a large number of these threats have been addressed [46]. These security threats range from Denial of Service (DoS) attacks, eavesdropping, impersonation, networking, and physical attacks. These attacks can occur at different levels of the architecture: vehicles, V2V or V2I communication link, RSUs, or access networks. The DoS attack aims to bring the network down and rendering the VANET unavailable. The eavesdropping attack occurs when an attacker is located inside the vehicle or in an RSU. This attack aims to have access to sensitive data. The impersonation attack happens when an attacker usurps the identity of a vehicle or RSU to execute malicious actions. The victim node will be rated negatively by the other nodes in the network, and it could be even excluded from the vehicular network. In case of a hardware tampering attack, the attacker manipulates a vehicle physically. It can, for instance, be perpetrated by other vehicles on radar or GPS receivers.

In [47], the authors present three kinds of security threats in VANETs, including attacks on safety-related applications, attacks on payment-based applications, and attacks on privacy. They further proposed recommended mechanisms to resolve security issues in VANETs, such as setting up tamper-proof hardware vehicles and establishing public key infrastructure in the vehicular system. Moreover, in [37], the authors propose some security requirements and an architecture for securing safety applications in VANETs. In particular, the authors focus on the security of multi-hop forwarding protocols in case of an accident. In [39], the authors focus on the position of cheating attack. They determine the impact of several malicious vehicles on delaying the alert warning messages in vehicular communications. They also identify the practical strategies and positions that could be used by adversaries to maximize the delay of the alert message. In [48], the authors analyze security challenges and potential privacy threats specific to vehicular cloud, which includes the difficulty of establishing trust relationships and models among multiple actors that are due to intermittent short-range communications. For the sake of completeness, we refer the reader to survey papers focusing on security threats and countermeasures in VANETs such as [1,49].

2.2. Software defined networking

The key concept of SDN [50] is decoupling of the *control plane* and the *data plane*. At the control plane, a logically centralized entity called controller is used for monitoring and managing networking resources. The controller aims to improve the overall network performance (i.e., efficient communication and traffic control) by optimizing the usage of network resources. The data plane is a networking infrastructure, which is used for data forwarding, and it consists of forwarding devices and wired or wireless communication links. The SDN facilitates communication between devices from various vendors via standardized interfaces (e.g., OpenFlow). Thus, it provides ease in network monitoring and management, and it supports the design of programmable and flexible networking architecture.

The most commonly used programmable interface that provides communication between the entities of the two planes (i.e., control and data) is known as *OpenFlow* protocol [51], and it runs on top of the Secure Sockets Layer (SSL). Apart from data and control planes, SDN also has a third plane called *application plane*, which consists of third-party network services and applications. These SDN applications communicate with the SDN controller to express their essential requirements concerning security, QoS, or resource consumption, via an application-control interface. In particular, the SDN uses the following two primary programming interfaces for inter-layer communications: (i) Control-Data Plane Interface called southbound API (e.g., OpenFlow Cisco OpFlex, and NETCONF), and (ii) Application-Control Plane Interface called northbound API (e.g., REST API).

In a typical SDN network, each OpenFlow-enabled Switch (OF-Switch) connects to other OF-Switches and possibly to end-user devices that are the sources and destinations of traffic flows in the network. Each OF-Switch has multiple tables implemented in hardware or firmware that it uses to process (i.e., routing) the received packets. In particular, the controller modifies the content of the table called *forwarding table*. Upon reception of a packet, the OF-Switch performs a lookup in its forwarding table to find the entry, which specifies the corresponding action for the received

packet. A table-miss occurs when there is no matching entry found for the packet, and it is processed as per the actions (e.g., send it to the controller through the southbound API or drop the packet) stated in the table-miss (or default) entry. The controller manages the network behavior by sending *flowmod* packets that modify the content of the forwarding table at OF-Switches. The detailed discussion on SDN architecture and its technologies are out of the scope of this paper. For a comprehensive study on SDN, we refer the reader to [50] and [52].

2.2.1. Benefits and challenges

The SDN significantly simplifies network management by performing efficient resource usage with the help of global network information. It also eases the implementation of the networking services for SDN applications by abstracting the data plane from the applications and allowing them to enforce their dynamic requirements on data plane entities via logically centralized controller(s). Although SDN brings many benefits, the inherent characteristics (e.g., programmable SDN-based switches, the limited bandwidth of the southbound channel, and limited resources at SDN controllers) of SDN architecture also raises new security concerns. Below, we briefly summarize both the major *benefits and challenges* in the usage of SDN technologies.

- *Support for heterogeneity and improved resource utilization:* With the use of its standard programmable interface, such as OpenFlow, SDN architecture supports the device heterogeneity, i.e., networking devices coming from different vendors can interact with each other and with the control plane entities as long as they are configured with some open communication interfaces (e.g., OF protocol). The controller tries to always keep a current global view of the underlying networking infrastructure. Due to this, more than one real-world application can share, through virtualization techniques, the same physical network to have a logically separate network. It makes the SDN re-usable as well as multi-purpose, i.e., it could be shared among different applications at the same or different point of time. In particular, the controller can instantiate multiple groups of logical OF-enabled switches on top of a single physical network in such a way that each physical entity could logically work for numerous applications. In contrast, each application will get a feel like the entity is working exclusively for it. Such instantiation of data plane entities pushes toward the maximum utilization of network resources by guaranteeing each application a customized performance, which is based on their given requirements.
- *Improved network security:* The controller can gather essential information about the network by communicating with the OF-Switches. These switches can collect the required information by performing network traffic analysis and using various anomaly-detection tools. Later, the controller analyzes and correlates the response from the data plane entities to create or update its global network view. Based on the analysis results, new configurations and policies to avoid the identified or predicted security threats can be installed in the whole network. Hence, these measures could help to improve the network performance and help in faster control and containment of identified security vulnerabilities.
- *Single point of failures:* The centralized SDN controller, low bandwidth communication channel between the controller and OF-Switch, and flow-table size limitation on OF-Switches make the SDN vulnerable to an array of DDoS attacks. Moreover, the lack of (i) trust between data plane entities due to networks support for open programmability, and (ii) best practices specifically to functions and components of SDN; remain significant bottlenecks in the rapid and real-world adoption of SDN.
- *Slow propagation of wrong information:* At OF-Switch, once a packet belonging to a specific traffic flow finds a match in the forwarding table, the switch *knows* how to treat the remaining packets of the same flow. Therefore, it does not require any further interactions with the SDN controller. This increases the traffic forwarding efficiently of the switch, but it also creates issues due to mobility, which makes the forwarding table rules inconsistent with the current network conditions. Therefore, the mismatch between the physical topology and global topology at controller causes packet losses (due to wrong forwarding information at OF-Switches) until the controller updates the forwarding table entries with new rules.

2.3. Emerging technologies

In the following, we overview some of the emerging technologies that are being integrated with SDVNs to improve one or more aspects of their functionality further.

2.3.1. Edge computing

The Edge Computing aims to bring the computation facilities of cloud computing closer to the source of the data. This concept leverages the processing and storage capabilities of devices to provide an intermediate layer between the cloud and the end devices. It resolves the issues of traditional cloud data centers such as network congestion and service quality degradation. The implementation of the Edge layer between the end devices and the cloud depends on the devices that act as intermediate Edge nodes, on the communications protocols and networks used by the Edge layer, and also on the services offered by the Edge layer. In the following, the implementation of the Edge layer can be classified into two types: Mobile Edge Computing (MEC) and Fog Computing (FC). For more details about the Edge Computing, we refer the reader to [53–55].

Fog computing. Cisco Systems introduced the concept of FC in 2012 [53]. It has a computing layer leveraging heterogeneous devices like wireless routers, access points, switches, or IoT gateways. These devices are called Fog Computing nodes and used to compute or store data from the end devices locally before forwarding to the cloud. The computation and storage capacities of these devices are usually lesser than servers. In terms of proximity with the Edge, the closest Fog node may be present multiple hops away from the end device. Moreover, the FC offers support for mobile networks and also protocols such as ZigBee and Bluetooth, and as a result, it can connect to a wide range of end devices. The FC leverages a supervising orchestrator to communicate with nodes to collect information on the resource status. As fog devices are diverse and heterogeneous, an added abstraction layer in the architecture is needed.

Mobile edge computing. The MEC [54] deploys the intermediate nodes with storage and processing capabilities in the base stations of cellular networks. It hence offers cloud computing capabilities inside the radio area network. The MEC nodes or servers are co-located with the radio network controller or the base station. These servers run multiple instances of MEC host and able to perform computation and storage on a virtualized interface. In terms of proximity with the Edge, the end devices in MEC connect directly to the Edge node over mobile networks. Similar to the Fog Computing, MEC also leverages a supervising orchestrator. However, there is no abstraction layer required for MEC since the dedicated devices are used as nodes. The orchestrator maintains a catalog of applications running on the hosts and handles information on the available resource and the network topology. The MEC servers provide real-time information on the network and also offer the location and network information of end devices.

2.3.2. 5G

Due to the exponential increase in the demand of users, 4G was not effectively able to address the new challenges such as higher capacity, higher data rate, massive device connectivity, lower latency, reduced cost, and consistent QoE provisioning. To meet these demands, improvements need to be made in the cellular network, and this pushes network operators to find solutions towards the deployment of 5G mobile networks. 5G networks are built around things and meet the requirements of three type of use cases: (i) Massive broadband (xMBB) that delivers gigabytes of bandwidth on demand, (ii) the Massive machine-type communication (mMTC) that connects billions of sensors and machines, and (iii) Critical machine-type communication (uMTC) that allows immediate feedback with high reliability and enables, for instance, autonomous driving. Moreover, the 5G infrastructures provide tailored network solutions to support verticals such as automotive, agriculture, and energy.

2.3.3. Named data networking (NDN)

Among several reference implementations of Information-Centric Networking (ICN) [56], NDN and Content-Centric Networking (CCN) projects have earned a significant response from the research institutions and industry. Unlike IP's host-based communication, in NDN [57], the client directly requests the named content deprived of addressing the content provider's location. In particular, when NDN client wants to request a specific *content*, it sends a specific *interest* packet referring to that content. The interest is composed of a Uniform Resource Identifier (URI) with a routable name scheme, e.g., `/unipd.com/video4u@BMCS/example.mp3` [57]. In NDN, the producer sign all its content that it produces with its private key so that the receiver/consumer can verify the authenticity of the received data even if the data is being fetched from some intermediate router's cache [58]. In NDN, the routers not only perform the routing operations, but they also perform in-network caching and interest aggregation [57,59]. Upon receipt of an interest packet, the router initially checks whether the content is available in its *cache* called Content Store (CS) or not. If the content is not available in CS, then as a next step, the router checks in its *Pending Interest Table* (PIT) for any similar pending interest, which has already forwarded to the next hop. Only if a PIT miss occurs, the router forwards the interest message towards its destination by using the *Forwarding Information Base* (FIB) table stored at a router. Else, upon a PIT hit, the interest is aggregated in the PIT. Later, when the router receives the requested content, it satisfies all the pending interests in the PIT associated with the received data. The requested data packet follows the in-reverse path of the preceding interest [57] message.

2.3.4. Blockchain

Blockchain was initially introduced as an underlying technique of Bitcoin [60]. A blockchain is a publicly verifiable ledger that strings an increasing chain of blocks via cryptographic hashing on the block headers. Such block includes some user transactions, and a selected miner packs each new block. This miner is chosen according to a preset consensus mechanism, and miners compete with each other to the winning miner to receive certain "financial" rewards as participation incentives. A consortium blockchain [61] is a typical blockchain that is maintained by a few identified parties. It securely records transactions among users who do not fully trust each other. Some applications of blockchain technology include SDVNs [62], 5G [63], and SDN-based Industrial Internet of Things [64]. The detailed working methodology and applications of blockchain technology are provided in research studies such as [65–67].

Table 1
SDN vs SDVN architecture features.

	SDN	SDVN
Reference applications	data centers, cloud computing, IoT, cellular networks, etc.	intelligent transportation system, IoT advertising, surveillance, traffic management, etc.
Control plane services	dedicated server machines acting as controllers	servers, RSU, and RSUC acting as controller supporting different level of functionalities
Data plane elements	SDN-enabled static switches and routers	SDN-enabled BSs and mobile vehicles
Communication technologies	mostly wired	wired, 4G/5G/LTE, DSRC
Mobility	low	high
Security	low	low
Privacy	high	low, mainly due to close interaction with drivers location information

3. SDN based vehicular networks

Applying SDN in VANETs without any modification entails several challenges, mainly due to VANET's highly dynamic network topology, which is attributed to the fast-moving network nodes (i.e., vehicles). In particular, the critical challenges in SDVN that need to be addressed are: (i) the considerable management overhead on the controller, and (ii) the congestion on the control-data communication channel. With the frequently changing network topology, keeping the updated version of global network topology at the controller is not only cost-intensive and time-consuming, but it also introduces inaccuracies in the received updated information. It is true even in cases where the controller can keep an updated global topology view. Also, some of the existing decentralized V2V and V2I communication protocols might not be able to use the benefits of SDN's global topology information system to its full extent. Hence, the network protocols might need redesigning to become adaptable to the SDN entities. Similarly, applying the improvement solutions that address various communication and security issues in SDN directly to SDVN is not feasible. It is due to the different characteristics of SDN and SDVNs, as it is shown in Table 1. The apparent novelty of SDVN w.r.t. traditional SDN implementations are that the data plane is made of vehicular devices instead of static switches. The reason for this is the need for multi-hop data forwarding. Moreover, unlike SDN, in SDVNs, it isn't elementary for the controller to keep an up-to-date global view, which is essential for efficient management of networking infrastructure. It is due to the mobile nature of some of these vehicular devices (e.g., vehicles) that reside at data plane in SDVNs.

3.1. A generic SDVN Architecture

Before we start our survey on the state-of-the-art SDVN proposals, we present an overview of a generic SDVN architecture, which includes a comprehensive set of technologies and features that could satisfy a broad set of VANET applications. Most of the existing SDVN architecture designs could be considered as a subset of it. Fig. 1 provides a top-level view of our generic architecture for an SDN-based VANET along with its major components and their interactions.

The data plane entities (e.g., smart vehicles) communicate with each other, and with control plane entities (global SDN and local RSU controllers, RSUs, and base stations) using the southbound APIs for coordinated and efficient communication. The controllers perform various functions such as routing, information gathering, and providing services to end-users based on the instructions and

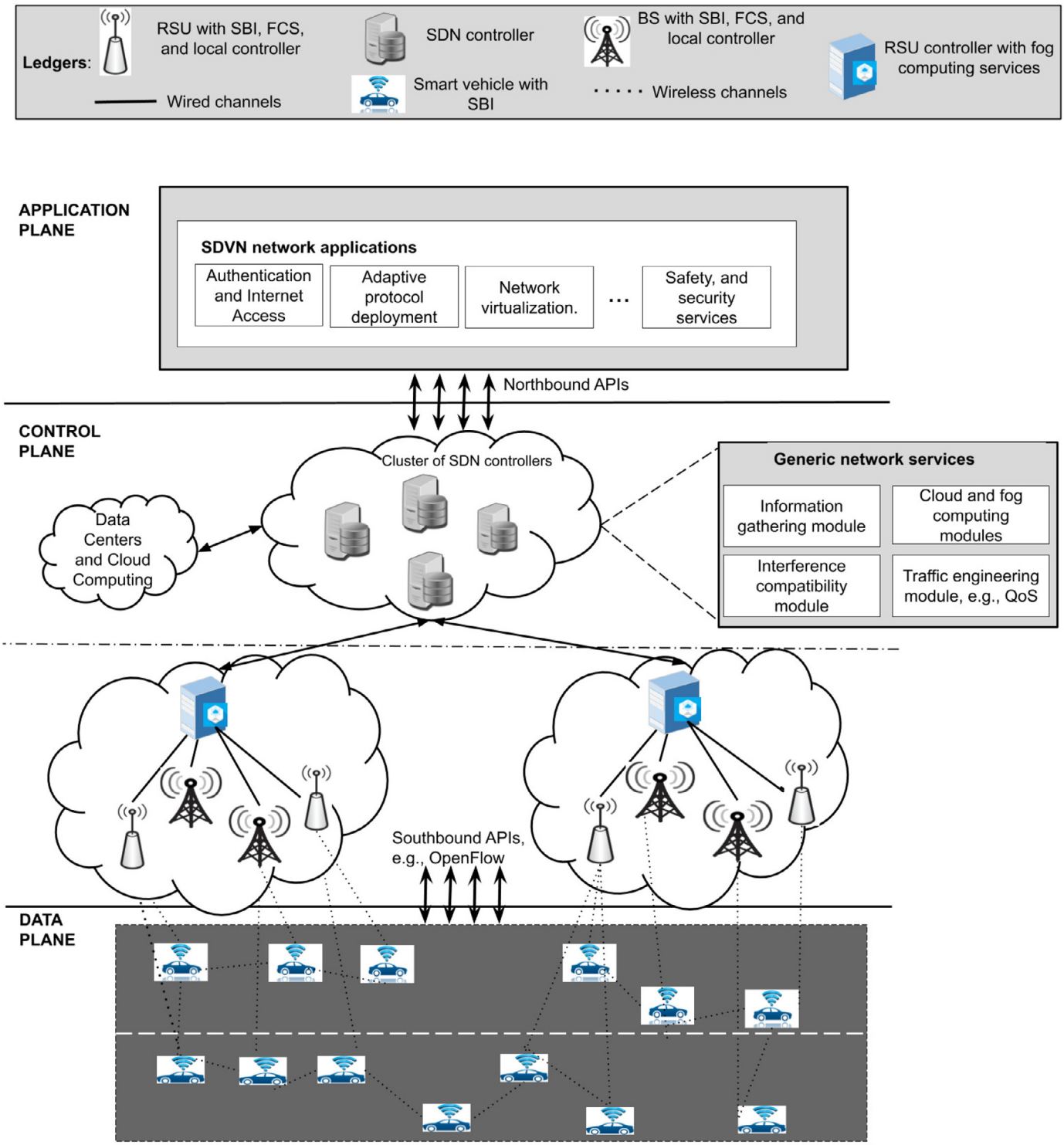

Fig. 1. High level view of a generic SDVN architecture

policies received through northbound APIs from the application layer entities. In particular, the control plane consists of several controllers that are clustered together to share network information and coordinate their decision-making processes. The controller has access to a generic set of network services (e.g., traffic management, interference compatibility module, and information gathering module) that are required by most of the VANET applications which use the SDVN architecture. The controller also provides an up-to-date network view to the application plane that helps it to manage various services (e.g., security, access control, mobility, and QoS) in the network. Specifically, vehicles communicate with their connected RSU or BS (i.e., RSUCs) to enable low latency local networking services and to maintain complete local knowledge. In parallel to serving the vehicle nodes, the RSUCs and BSs share the collected information about the vehicles and the transportation system to the global SDN controller. Based on the information received from the RSUCs, the network administrator sitting at the highest control of the SDN controller builds a comprehensive

view of the data plane entities (i.e., vehicles). To achieve specific user goals, the business and SDVN network applications are available at the application plane of SDVN architecture. These network applications interact with SDN controller (or RSUCs) through NBI protocols to program the data plane entities with the required and optimal network configurations. In particular, the application layer contains SDVN network applications that are designed to satisfy specific application's requirements. These network applications can access and control the data plane devices through the SDN controller. Example of SDVN network applications could include authentication and Internet access, dynamic access control, security protocols, seamless mobility and migration, load balancing modules, and network virtualization.

To reduce the latency while providing time-sensitive services to the vehicles in SDVN, the local controllers could be equipped with fog computing services (refer to Fig. 1). These controllers perform the required processing for time-sensitive tasks on the received data before the data is sent to the cloud computing enabled data centers for further processing and analysis. Due to the availability of local controllers and fog services (i.e., fog enabled data plane elements) in SDVN, the architecture presented in Fig. 1 could operate in Hybrid Control Mode (HCM) which improves network performance and robustness. In HCM, the SDN controller takes partial control of the system, while sharing the remaining information with RSUCs. This arrangement helps in situations where the local controller lost its connectivity with the global controller, and the vehicle nodes can still perform their networking tasks with the help of local controllers.

3.2. Overview of state-of-the-art SDVN architectures

In this section, we provide a comprehensive survey of the existing works on SDVNs. It includes a brief description of the proposed SDVN architectures along with their working methodology. We start our survey with the classification of the future SDVN architectures based on their integration with different emerging paradigms (such as 5G, cloud computing, edge computing, and NDN). The integration of SDVN with other emerging technologies has been done to improve SDVNs performance for specific and generic application domains. As shown in Table 2, we broadly classify the surveyed SDVN architectures in the following three categories.

- *SDN-enabled VANETs:* In this category, we include the research efforts that propose and evaluate an SDN-based architecture for VANETs. In particular, these proposals provide the design, implementation, and analysis of using the SDN paradigm for VANET applications. However, most of these proposals are only evaluated partially by using simulation tools, and they do not provide a detailed analysis of the drawbacks of SDVNs. A full testbed implementation and detailed analysis of its benefits and drawbacks are necessary before the real-world implementations of these proposed SDVNs.
- *Integrating SDVN with new technologies for next-generation VANET applications:* The research community identified that the SDVNs was facing various limitations such as latency, control overhead, limited applicability in next-generation vehicular applications, and mobility management. Therefore, the researchers started to address one or more of these limitations by integrating new emerging technologies (e.g., fog computing, NDN, and 5G) with SDVNs, this category includes all such efforts.
- *Improvements over SDVNs:* This category includes research efforts that take a step forward from SDVNs, and provide various techniques to improve or address specific limitations of the SDVNs such as optimized routing technique, implementing fine-grained access control management to access controller functionalities, and providing support for heterogeneous networking and resource management.

3.2.1. Convergence of SDN and VANET

When the researchers first started their work towards SDN-based VANETs, the primary task was to design an SDVN architecture and define the functionalities and interactions of its various components. Authors in [42] and [43] proposed an architectural design SDVN along with a set of services that it supports. In [42], the proposed architecture aims to improve network flexibility and programmability, and it introduces additional network services, policies, and configurations for VANETs to cope up with the increasingly new requirements of advanced VANET applications. The authors demonstrate the feasibility and communication efficiency of SDVNs deployment by evaluating the performance of SDVN routing protocols with state-of-the-art MANET and VANET routing schemes. The goal in [43] was to support the rapid integration of innovative network services for efficient vehicular communications. The proposed architecture consists of different entities like vehicles, road-side units, and heterogeneous wireless technologies and devices, which are abstracted from the application layer through SDN controllers and SDN-enabled switches with unified interfaces. The authors also present some useful use cases to demonstrate how their architecture enables rapid network innovation. One advantage of the proposed architecture is that it allows programmability by selecting and deploying routing protocols on demand; another advantage is that it provides flexibility by using network slicing to isolate multiple tenants.

For better resource scheduling, the authors in [68] use the SDN as a unified resource manager in vehicular communications. The proposed solution takes into account the networking resources from the data plane to perform centralized scheduling at the control plane. The SDVN allows the network managers to choose optimal network interfaces whenever an application wants to send data. The integration of SDN with heterogeneous vehicular communication ensures a low-cost communication overhead. In [71], authors present a service-channel allocation scheme adapted to SDVN communications. In particular, an SDN controller keeps a holistic view of network states and available spectrum resources. Based on this view, the controller could decide which channel to use for a service or traffic type. A key benefit of the SDN-enabled vehicular communications is that it avoids conflicts and interference. Additionally, the architecture supports load-balancing between different service channels. In [84], they provide different designs for SDVN architectures that support centralized, partially centralized, and hierarchical placement of the SDN controller. Initial evaluations of the proposed architectures have been presented for packet delivery ratio and delay metrics.

To optimize network management, an SDVN communication technique is proposed in [85], which enforces an optimal share of network resources between the contended entities. A static distribution of network resources to RSUs can be ineffective in situations when traffic density under an RSU's coverage range increases; since this situation forces the RSU to accommodate additional data flows that could result in degradation in QoE of end-users. To address such cases, the authors propose a mechanism for the management of data flows and transmission power and implemented it on the controller. After identifying unsatisfactory vehicles (i.e., their QoE decreases), the model adjusts their signal levels by reducing the interference with RSUs. The key idea is based on a data-flow management technique that distributes unsatisfactory vehicles to each RSU. SDN has also been used to manage cooperative message dissemination in vehicular communications in [14]. In particular, the RSU controls data dissemination over V2V and I2V channels. The centralized RSU directs scheduling decisions for the vehicles with a set of instructions that specifies the channel

Table 2
Classification of SDVN Architectures.

Research efforts classification	Proposal	Year	Additional technology	Aim	Use cases or applications
SDN-enabled VANETs	[42]	2014	none	shows the key benefits of SDVNs	generic VANET applications
	[14]	2015	none	data scheduling through cooperation to improve network scalability and service latency	efficient data services in hybrid I2V/V2V scenarios
	[43]	2016	none	SDN for resource management and enabling heterogeneous communications in SDVNs	generic VANET applications
	[68]	2016	none	efficient resource management and low communication cost	generic VANET applications
	[69]	2016	none	improve performance of vehicular clouds, resource utilization and vehicles location privacy	secure vehicular cloud computing
	[70]	2017	none	detect drivers psychological state through its fatigue and mood swings	safety services
	[71]	2017	none	fair and interference-aware channel allocation in high mobility topologies	infotainment and multimedia services
Integrating SDVN with new technologies for next-generation VANET applications	[72]	2015	fog computing	optimizing resources utility and reducing latency	data streaming and lane-change assistance
	[44]	2017	edge computing	improve responsiveness and enhance QoE	urban traffic management and latency-sensitive applications
	[45]	2017	cloud computing	flexibility for deploying software updates on vehicles	over the air software updates
	[73]	2017	edge nodes	adaptive and low latency	wireless applications for the next generation driving machines
	[74]	2017	5G and fog	low transmission delay and high throughput	pilotless vehicles
	[75]	2017	5G	minimum delay and better QoS with high PSNR	multimedia streaming over vehicular 5G networks
	[76]	2017	5G	data offloading for better resource management and spectrum utilization	managing requirements of vehicles in 5G scenario
	[77]	2017	5G	low bit-error rate and high throughput	5G-enabled vehicular applications
	[78]	2017	NDN	identify pros and cons of NDN integration in SDVNs	generic VANET applications
	[79]	2019	NDN	mitigate the broadcast storm issue	generic VANET applications
Improvements over SDVNs	[80]	2016	none	use of cellular networking infrastructure and securing SBI for control plane optimization	generic SDVN applications
	[81]	2017	none	reliable communication in the controller-miss situation in SDVNs	generic SDVN applications
	[82]	2018	none	support for heterogeneous VANETs, load balancing with low latency	generic SDVN applications
	[5]	2019	none	scalable and dynamic AC scheme at NBI, make AC policy change independent to controller	High mobility SDVN applications
	[83]	2019	none	improved data communication with an optimized	generic SDVN applications
	[35]	2019	LNN	low latency, mobility prediction, heterogeneous communication	generic SDVN applications

to which it should tune to transmit or receive the data packets. This approach enables cooperative dissemination by using the SDN paradigm. In order to address security issues in group-oriented vehicular applications, the authors in [86] propose a 5G-enabled SDVN architecture to provide secure and privacy-preserving access to group members and mobility management of the members in centralized as well as decentralized networks. The experiment results show the effectiveness of the proposed framework in terms of network overhead and handover latency. However, the security and privacy metrics are not evaluated, which raises concern to its

overall effectiveness. Similarly, the security aspect of VANETs using SDN is also provided in [87], where the authors present an initial implementation and analysis of software-defined security solutions for VANETs. The work uses the centralized controller for dynamically and flexibly program the data plane devices with policies that enforce data flow control and confidentiality in VANETs.

3.2.2. SDNVs integration with other emerging technologies

To meet the requirements of future VANET scenarios such as ITS, automated overtake, and autonomous driving, the authors in [72,88] propose an SDVN architecture that uses fog computing services, since these applications are delay-sensitive and location-aware. However, the paper lacks the validation of their proposed architecture. Taking a step further, authors in [44] propose a new SDVN architecture assisted by mobile edge computing (MEC) services to provide integration support for heterogeneous access technologies. The aim is to provide low-latency and high-reliability communication in the network. The validation of the proposed architecture concerning reliable data communication is carried out through a case study of *urban traffic management*. The simulation results show that the architecture meets the application-specific requirements concerning latency, reliability, and data rate. Also, authors in [45] propose an SDVN architecture with edge computing services to distribute software updates to vehicles in a flexible way. The architecture uses V2V beaconing information to create a global topology view at SDN controllers, which helps in systematic network management. Additionally, to tackle the challenges caused by interference and hidden nodes, the controller runs a technique that uses mathematical optimization models for assigning distinct operating frequencies to each vehicle.

With the rapid advancements in next-generation technologies such as 5G and automotive applications, an integration between VANETs and 5G technology is envisioned by the network developers and service providers. To perform this integration efficiently, SDN is being used as a key enabler. For instance, the authors in [89] propose an integrated architecture of these three technologies (i.e., VANETs, SDN, and 5G) for providing a security-by-design approach in VANETs, and also to strike a fair balance between networking services, vehicle mobility, network performance, and security features. The proposed architecture is evaluated against an array of security threats (e.g., DoS, resource exhaustion, and link-layer discovery attacks) targeting either the SDN controllers or the vehicles. Additionally, the authors discuss several possible techniques to identify the source of attacks for their mitigation. Similarly, authors in [75] propose an SDN-enabled integrated VANET and 5G network architecture, which uses a novel buffer-aware streaming technique for real-time multimedia streaming applications. The proposal also aims to keep minimum communication latency and ensures good QoS during connection handovers between consecutive eNodeBs. To achieve adequate QoS, the SDN gathers information regarding user mobility and status of the player buffer, and the strength of the network signal is used to provide an efficient transmission strategy for multimedia streaming.

To further minimize the communication latency and to improve the QoS, the authors in [74] and [90] propose a 5G-based SDVN architecture that also integrates the cloud and fog computing services to improve the network performance further. The proposal uses SDN to improve the scalability and flexibility of vehicular networks. At the same time, fog cells have been introduced, and fog computing is performed at the network-edge to lower the communication latency. The overall architecture is composed of various elements that include cloud-fog computing services, SDN and RSU controllers, RSUs, BSs, and vehicles. The controllers gather and share the state information of fog computing clusters to the cloud computing data centers. The data plane consists of network entities (e.g., vehicles, BSs, and RSUs), while the control plane includes controllers (including RSU centers). The RSU center acts as a controller for an individual fog cell, which consists of vehicles and an RSU to avoid the frequent handovers between vehicles and RSUs. Vehicles in a fog cell communicate using a multi-hop relay. Authors in [91] examine possible techniques for integration of clustering algorithms with VANET supported 5G networks to minimize the spectrum resources usage and the network congestion and to improve the packet delivery ratio. Due to the challenges of finding an effective clustering algorithm which should be adaptive to dynamic VANETs, the authors consider the SDN paradigm. In particular, the authors propose a social-aware clustering algorithm supported by the SDN paradigm for 5G-VANET systems. The algorithm exploits the social patterns such as future routes of vehicles, which helps to develop a prediction model to improve the stability of the clusters.

Authors in [92] provide a hierarchical VANET architecture supported with 5G technology that also integrates the SDN's centralization and flexibility features. The architecture also uses Cloud Radio Access Network (C-RAN) with a 5G paradigm for the effective allocation of resources using the SDN global view. Moreover, the architecture incorporates a fog computing framework to minimize the number of handovers (between vehicles and RSUs) that occurs over a defined period by using the zones and clustering techniques at the network-edge.

The centralised controller is vulnerable to various attacks and single points of failure. Therefore, the use of distributed controllers has been envisioned in various research works. However, reaching a consensus in the presence of multiple controllers is remain a problem in SDVNs with distributed controllers. To address this problem, the authors in [93] propose a blockchain-assisted distributed SDVN framework. The proposed framework aims to design a secure and reliable SDVN architecture that functions in a distributed manner to address the security issues of VANETs. Due to the inherent characteristics of blockchain, such as decentralization and immutability, a blockchain-based security framework is proposed in [62] to support the vehicular IoT services (i.e., real-time cloud-based video report and trust management on vehicular messages) in an SDN-based 5G-VANET. In particular, the work explicitly demonstrates the SDN-based 5G-VANET model and the scheduling procedures of the proposed blockchain-based framework.

3.2.3. Towards improvement in SDVNs

After proposing different designs for SDVN architectures, the research community has shifted its focus towards evaluating and improving the data communication process and other networking services (such as QoS, security, and privacy). To this end, various solutions have been proposed that either exploit the unique in-built features of SDN or develop new techniques to achieve the application-specific or general requirements in SDVNs. For instance, authors in [76] propose SDN based solutions to improve the data offloading mechanism in vehicular networks. The mechanism comprises load balancing and priority managing services that reside at the SDN controller. Additionally, the data offloading approach is used to minimize network congestion, which leads to higher network scalability at a lower cost. Similarly, authors in [94] propose a data offloading technique for V2V communications in a cellular network inside an SDN-based Mobile Edge Computing (MEC) architecture. The proposed offloading method uses each vehicle's context information (e.g., location, speed, direction, and IDs), and it takes a centralized management approach (e.g., SDN controller services) for estimation and notification of communication routes between vehicles that are currently communicating by using a 5G network.

In SDVNs, it is vital that the data plane entities have uninterrupted connectivity with the controller. However, due to interfer-

ence, low link stability due to high mobility, controller overloading, and network partitions, it might be possible that the controller becomes unreachable. To address this issue and to increase the robustness of the communication system in SDVNs, authors in [81] propose a hierarchical SDVN architecture intending to improve the performance in events where connection loss between vehicles and primary SDN controller are considered. Since the control plane in SDVN performs forwarding of messages in V2V and V2I communications, then to support these communications, the data plane forwarding entities have to communicate with the controller frequently. Therefore, this communication between the controller and the data plane must exhibit low latency. In [80], authors propose a design of a hybrid control plane in 5G-based SDVN to strike a trade-off between the cost to access cellular network for controller-data plane communication and latency in this southbound communication process.

Authors in [82] exploit the use of smart identifier networking (SINET) paradigm [95] for SDVNs, in which virtualized function slices are organized flexibly by a set of networking elements using crowdsensing. These network slices could be used to serve different applications depending upon their requirements. In particular, by enhancing crowd collaboration in SDVNs, the authors aim to schedule pervasive network resources smartly. The proposed approach provides several benefits in the network, including enhanced security, traffic management through load balancing, and support for heterogeneous networking.

Authors in [5] propose an adaptive access control scheme for NBI protocols to protect the global knowledge of VANETs stored at the SDN controller in a SDVN scenario. Since the external applications can access the controller via NBI to dynamically provide their requirements or network policies for the underlying networking infrastructure, therefore, a malicious SDN application could cause security threats to various entities (e.g., controller, and vehicles) of SDVN. To this end, the authors propose BENBI, which uses a cryptographic tool identity-based broadcast encryption scheme to secure the NBI of SDVNs. Although BENBI provides fine-grained access control, the use of public key infrastructure for access control is not suitable for delay-sensitive VANET applications, and the overhead caused by the key management process increases the overall network overhead.

Researchers consider SDN as a promising paradigm to fill the gap between the heterogeneity caused by data plane entities (i.e., devices and wireless technologies) and the lack of route discovery schemes that could efficiently handle the dynamic topology changes in VANETs due to the vehicle's inherent mobile nature. The dynamic topology causes packet losses in the network due to short lifetime links, therefore, routing protocols that could effectively analyze the link quality fluctuations are needed. In [83], the authors propose a link-stability based routing protocol for SDVNs, in which the controller's global information is used to dynamically discover multiple routes that are stable and shortest between a given source-destination pair. Moreover, the source routing technique is used to reduce the delay and overhead in the process of installing new flow rules on the intermediate data plane routers on a selected route. However, the scalability and traffic heterogeneity has not been considered along with any security issues for the proposed scheme. Similarly, in [35], the authors propose a machine learning-enabled mobility prediction scheme for routing in SDVNs with low routing delay. In particular, an artificial neural network technique is employed that uses the global network knowledge available at SDN controller in order to predict vehicle mobility in the underlying heterogeneous VANETs. Based on the information available at the controller, it selects the most optimal (i.e., low delay and mobility) path between the source and destination vehicles. The proposal is suitable for delay-sensitive applications, but it depends on the availability of the accurate network information at controller, which is not always the case due to packet loss, high mobility, and low bandwidth in VANETs.

In all the above discussed SDVNs, the placement of controller and open-flow switches is application-specific. For instance, the SDN controller can be installed at RSUs, base stations, data centers, or vehicles, while the open-flow switch functionalities are usually installed in vehicles. As far as we know, all the proposed SDVN architectures did not consider integrating security modules or analyzing any of the security issues of their proposed architectures, which is a serious concern due to the use of VANETs in life-sensitive applications. Finally, Table 3 provides a summary of all the SDVN research works available in the state-of-the-art, along with their key advantages and drawbacks.

4. SDVNs: benefits and challenges

In Table 4, we summarize the significant benefits and research challenges that we have extracted from our surveyed articles on the SDVN architectures presented in Section 3.2. As can be seen from Table 4 that none of the SDVNs addresses all the essential issues, which is a requirement for next-generation vehicular applications. Moreover, security and privacy (S&P) is the biggest challenge, and it has not been given significant attention while designing SDVNs. Similar to S&P, connectivity is also a key challenge in SDVNs. To ensure the required connectivity in the target network, the proposed SDVN framework should include solutions such as: (i) efficient mobility management technique, (ii) robustness against short-term connectivity losses, and (iii) ensure uninterrupted controller availability or backup solutions in cases of a connection failure with the controller. Also, only a few SDVNs analyze or provide solutions for interoperability challenge, which becomes an important issue when SDVNs are also being integrated with various emerging technologies. Hence, we believe that unified interfaces between various networking components will be needed to achieve overall high network performance. Also, as seen in Table 4, due to the availability of global network information at controller, most of the SDVNs provide support for efficient resource management. Also, with the help of multiple controllers along with edge computing devices, many SDVNs support network scalability. Below, we provide a discussion on a set of generic benefits and challenges along with their implications on various aspects of SDVN architectures.

4.1. Benefits

The benefits of SDVNs are multiple, such as rapid network configuration, improving user experience by efficient resource utilization, minimizing service latency, and resistance to some inherited attacks of SDN or VANETs. Below, we discuss some of the major benefits of SDVNs.

- *Optimized resource utilization* - The availability of a global topology view helps the SDN controller to manage the network resource efficiently in SDVNs [43,72]. For instance, when multiple wireless interfaces or configurable radios (e.g., cognitive radios [96]) are available, then the controller can choose better coordination of channel/frequency [42]. Similarly, due to awareness of network resources, the controller can effectively choose whether and when to change the signal power of wireless interfaces to change the transmission range of the vehicles (or network nodes) [71]. For instance, when an SDN controller discovers that the node density under an RSU coverage area is too sparse, it sends instructions to the existing nodes in that area to re-configure their transmission power to achieve higher packet delivery ratio [97]. Similarly, the SDN controller can take specific requirements from individual applications running on the

Table 3
State-of-the-art SDVN Architectures.

Architecture type	Proposal	Integrated technologies	Description	Advantages	Drawbacks
Centralized	[42]	None	SDVN to improve safety and surveillance services	Communication efficiency	Controller placement, security analysis
	[43]	Network slicing	Heterogeneous vehicular communication	On-demand routing protocols and improved flexible and bandwidth utilization	Benefits and challenges of slicing are not evaluated
	[44]	MEC	MEC-enabled SDVNs for reliable communication in Urban traffic management, and 4K streaming	Low latency and increase data rate	Connection loss with controllers and high mobility scenarios are not considered
	[45]	Cloud computing	SDVN for remote software updates in vehicles	Dealing with interference and hidden node issues	Security, connection loss with controllers and high mobility scenarios are not considered
	[35]	Artificial neural network	Delay-minimization routing for SDVNs with mobility prediction	Predicting mobility patterns in order to route vehicles	No security analysis, no solution when connection loss with controller occurs
	[75]	5G	SDN-enabled buffer-aware multimedia streaming in 5G VANETs	Better QoS during handover	Scalibility and communication robustness
	[91]	5G	Social-aware clustering protocol for SDN-based 5G-VANETs	Reducing network congestion,improving packet delivery	Security issues and connection loss with central controller are not considered
	[76]	5G	Priority-based load balancer approach for data-offloading in SDVNs	Improve scalability and traffic management	No evaluation is performed for mobility and security induced issues
	[94]	5G, and MEC	Improving V2V data offloading in 5G using SDN supported MEC architecture	Contextual information based route discovery, V2V offloading	Identifying accurate contextual information, vehicle privacy
	[68]	None	Advancements vehicular network technologies through SDN's unified network resource management approach	Resource scheduling with a low cost communication overhead	No security analysis, no solution when connection loss with controller occurs
	[80]	5G	Design of a hybrid control plane for SDVN using 5G	Low communication cost and latency between control-data plane	No security and real world performance evaluation
	[83]	None	Link-stability based route discovery protocol	Mobility prediction, low communication cost, high PDR	High routing overhead and latency
Hierarchical	[83]	None	Routing protocol/Shortest travel time	Rapid packet delivery, and low latency and overhead	Maintaining global view at SDN controller
	[81]	None	SDVN architecture to improve network flexibility and programmability	performance improvement is guaranteed even when connection is lost with main controller	insufficient performance evaluation
	[72]	Fog computing	Fog supported SDVN for autonomous driving, and automated overtake	Improve delay sensitive and location awareness services	Effectiveness and correctness of the proposal remains unclear, fog, SDN, and VANET integration issues
	[89]	5G	Using SDN in 5G-enabled VANET to address DDoS attacks	Provides a trade-off between number of network services, dynamic topology, and network performance and security features	Only weak security analysis
	[74], [90]	5G, and cloud/fog computing	Fog-assisted SDN-based 5G VANETs to improve throughput and delay	Reducing communication latency, improving scalability and flexibility	Real-world performance evaluation
	[92]	5G, Cloud-RAN, fog computing	Empowering real-time applications through SDN-enabled delay-sensitive, mobility-aware, and location-aware techniques	Management of cooperative message dissemination	Integration issues with different technologies, evaluation in high mobility scenarios
	[81]	None	Design of a hierarchical SDVN to improve connectivity with controller	Robust against loss of connectivity with controller, dynamic controller creation	Security and scalability issues

top, and it can implement an optimal configuration for the network devices and resources to meet these requirements [98]. In particular, having an up-to-date network topology and resources view at the controller opens-up new opportunities to improve the network performance by optimally allocating the resources based on the current network conditions. For example, in [99], the authors utilize the global network knowledge for enabling GeoBroadcast in SDVNs. Another example, which shows how SDN improves the network resource usage is demonstrated in the work presented in [100]. In traditional VANETs, any warning message by a source node in an intelligent transport system application is first sent to the nearest RSU. The RSU forwards it to the control center, from where the message is transmitted to all the other RSUs that reside in the geographical area. Finally, these RSUs will broadcast the message in their coverage area. This process of disseminating

Table 4
Status of key challenges addressed by state-of-the-art SDVN architectures.

	Resource utility	Flexibility	Latency control	Interoperability	Connectivity	Security & privacy	Scalability
[14]			✓				✓
[43]	✓			✓			✓
[68]	✓			✓			
[69]	✓	✓				✓	
[71]	✓						
[72]	✓		✓				
[44]			✓				✓
[45]		✓					
[74]			✓				
[75]			✓		✓		
[76]		✓					✓
[77]	✓	✓	✓				
[78]					✓		
[79]					✓		✓
[80]	✓		✓				
[81]					✓		
[5]		✓				✓	✓
[83]					✓		
[35]	✓		✓	✓	✓		

the warning message causes huge overhead concerning network bandwidth and latency. In [100], the authors perform the above operation in an efficient way by using the SDN technology which is as follows: (i) the source RSU forwards the first warning message to the SDN controller, (ii) the controller configures the routes (via flow entries) to the destination RSUs, and (iii) until modified, the same routes will be followed by all the upcoming warning messages to disseminate. In this way, the controller reduces network control overhead, communication latency, and bandwidth usage. The efficient use of network resources in SDVNs can significantly improve network performance for many target scenarios, including both static (e.g., road accidents) and dynamic (e.g., make way for an ambulance).

- *Fast and flexible network configuration* - The separation of control and logic plane in SDVNs provide support to the rapid and flexible network configurations. It will help to meet the varying requirements of the applications and to adapt the changes in network topology caused by vehicle mobility. For instance, Authors in [101] propose a data-driven approach for designing an artificially intelligent model for vehicular traffic behavior prediction. In particular, they combine the flexibility, adaptability, and scalability of SDVN architectures with the machine learning techniques to model the traffic flow efficiently. Moreover, due to the shortest path routing approach or due to dominant video applications that occupy large bandwidth on the route, congestion has occurred on a few selected forwarding nodes. With the help of up-to-date network information at SDN controller, such a situation could be easily detected along with the IDs of the congested nodes, and the controller could perform a traffic rerouting process to avoid congested nodes which lead to improvements in network resource utilization and performance. It also reduces congestion points in the network [102] and energy consumption at low power devices [11].
- *Heterogeneous network integration* - In SDVNs, the controller provides the abstraction between VANET applications and networking infrastructure, which enables support for the integration of heterogeneous networks (e.g., wired and wireless) and communication technologies (e.g., DSRC, WiFi, LTE, and 5G) that reside at the data plane. The use of communication protocol, such as OpenFlow, dramatically simplifies the interactions between the data plane and control plane entities. For instance, irrespective of the vendor and hardware configuration, an OpenFlow-enabled data plane switch could communicate with the controller through the well-defined southbound APIs. However, the coexistence of heterogeneous V2X networks requires efficient interworking mechanisms that allow efficient communication between these networks. Also, the existing SDVN architectures are lacking standardized Eastbound/Westbound APIs and Northbound APIs for vehicular applications.
- Minimizing service latency - The use of SDN enables the optimal implementation and management of fog computing services at network edge routers, which significantly reduces the service latency for delay-sensitive applications. Specifically, SDN's programming flexibility feature provides great support for implementing fog computing services at SDN-enabled edge devices. For instance, authors in [103] propose a scheme for balancing service latency and cost by using genetic algorithms in SDVNs, and authors in [35] proposes a centralized routing scheme with mobility prediction for SDVNs to minimize the overall vehicular service delay. It also uses an artificial intelligence-powered SDN controller. Moreover, the use of SDN global topology information allows dynamic re-configuration in flow tables of routers to provide support for the implementation of adaptive networking services, which helps in minimizing service latency. Thus, it leads to improved end-user experience. In particular, the resource management capabilities at the controller helps it to dynamically allocate resources as per the changing requirements of the VANET applications. For example, let's suppose a vehicle *X* goes outside the coverage area of an RSU. However, *X* could still receive service messages from a neighbor vehicle *Y*, and *Y* is within the coverage area of RSU. In such a scenario, an RSUC can assign additional resources to vehicle *Y* to support its increased needs (i.e., providing support to vehicle *X*). This process will reduce service latency for vehicle *X*. Authors in [104] provide such services to the lost vehicles by exploiting the inherent features of Information-Centric Networking (ICN).

4.2. Challenges

The state-of-the-art SDVNs faces issues in their large scale deployment in real-world applications, and it is due to the following challenges in these architectures.

- *Connectivity*- The high vehicle mobility causes rapid changes in SDVN topology and fluctuations in radio communication channels. The frequent topology changes also hinder the real-time collection of the networking knowledge that is required at the

controller to maintain a current view of the data plane resources. The delayed or inaccurate global perspective leads the controller to experience delays in distributing commands to network elements. Therefore, to support the rapid adoption of SDN paradigm in VANETs, it is required to develop mechanisms that could handle high network mobility management issues in target SDVNs. To this end, there exist few techniques (such as use of fog computing and local controllers at network edges) that try to minimize the effect of network mobility in VANETs. However, these techniques are not in the advanced stages, and thus, these cannot be ported directly (i.e., without any optimizations) in SDVNs. At present, the most effective solutions to handle the mobility caused issues in SDVNs could be the ones, in which a vehicle's future directions can be predicted based on a set of metrics (e.g., velocity, past driving patterns, and GPS location) by applying machine learning tools. However, a correct and valid implementation of such solutions is challenging due to the privacy concerns and high deployment complexity. Apart from mobility management in SDVNs, providing uninterrupted connectivity with the controller is a difficult task, and it could become more challenging if the connection between the controller(s) and data plane devices is wireless (e.g., WiFi or LTE) which might increase the communication latency and packet loss rate. In such scenarios, a fallback scheme should be in place to maintain the essential network services, i.e., the isolated vehicles can surely get the necessary services. For instance, it can be achieved with the help of deploying a set of relay nodes in the network that allows isolated nodes to reach to the controller.

- *Broader flow rule definitions and policies* - In SDN, the data plane switches maintain forwarding tables which mainly consists of the following three entries: (i) packet forwarding rules, (ii) one or more action corresponding each rule, and (iii) a set of counters associated with a data flow to keep track of the number of packets or bytes handled. However, the existing flow rules and policies that govern the data communication in the SDN network needs to be enhanced to handle the essential demands of the broad range of new VANET applications. For example, the SDN controllers could offload some of the tasks to the RSUs and BSs, which act as local (or lower level) controllers by sending general flow rules or policies instead of specific rules associated with a data flow. Latter, these local controllers could provide or install data flow rules and policies depending on their local knowledge of the network. Similarly, the RSUs and BSs could process the collected networking information locally for making some of the decisions, and also sent the same information to cloud data centers and SDN controllers via a southbound interface for global, long-term usage [72].
- *Security and privacy considerations* - In SDVNs, the SDN controllers manage network resources and also control various networking services (e.g., security, traffic management, and QoS services), therefore it is imperative to protect the SDN controllers from different cyber attacks. For instance, the propagation of malicious information to the controller from adversaries can lead to severe accidents. An adversary could launch a man-in-the-middle attack by exploiting northbound or southbound communication channels, and such attacks can be addressed by using proper access control mechanisms and cryptographic communication protocols (e.g., transport layer security). DoS attacks can also be launched to paralyze the operations of controllers, or controllers can be compromised via inside attacks. Therefore, the security of the controller becomes a priority as it is a centralized decision making entity in SDVNs. Other security threats include the ones we mentioned in Table 5. Although many solutions exist, these cannot be directly adopted in VANETs due to their different characteristics. Additionally, the new security vulnerabilities that might occur due to the integration of the VANET and SDN or other technologies with SDVNs should be investigated before the deployment of such hybrid architectures.

  The SDVNs should also satisfy the essential privacy requirements, for instance, the SDN controller should only be accessible by authorized applications (SDN or VANET) via a secure northbound interface protocol, and the drivers' sensitive information that is stored at edge computing devices or SDN controller must be protected from malicious entities in the network. Moreover, emerging SDVNs require new security measures due to the existence of new networking and architectural components. The layered design of SDVN makes it more vulnerable to security threats. It is because threats at one layer could cause severe damage at other layers due to high functional dependency between the layers. Therefore, to effectively address the new security threats in SDVNs, a systematic top-down approach is suggested as a way forward in [105]. The key requirements to address the security issues in SDVNs should be identified, and the target SDVN architecture needs to support these requirements efficiently.
- *Controller placement optimization* - The use of SDN in VANETs provides improvements in various aspects of VANETs by leveraging the unique features of SDN like flexibility, scalability, and adaptability. However, this improvement comes at the cost of higher service latency. It is because in the existing SDVN the controllers are placed at the control plane, which is far away from the data plane devices. As an alternative, various proposals have been proposed to bring the control plane down to RSUs and BSs (please refer to lower entries in Table 3). In particular, hierarchical distributed controller architectures where the top tier controllers are regionally distributed on the Internet and the bottom tier controllers are placed in a set of preselected RSUs and BSs. These RSUs and BSs are closer to the vehicles. Thus, it reduces the latency induced by the system [106]. However, the optimised controller placement is a challenging task even in SDN only networks, and it becomes more problematic in SDVNs due to additional components and characteristics of the VANETs that need to be considered while designing a placement scheme [107].
- *Misbehavior of elements from different integrating technologies (e.g., cloud, 5G, and ICN)* - The use of various technologies and architectures in realizing the next generation VANET applications also increases its attack vector. It is because misbehaving or vulnerability in any one of the integrated technology might affect the operations of the whole VANET. For instance, we have discussed above that the use of SDN controller adds a new set of security vulnerabilities in the network. Similarly, the drawbacks in other integrating technologies (e.g., cloud, 5G, and ICN) can significantly increase the threats in the integrated network. In [105], the authors present general security vulnerabilities and attacks for an SDVN. The work discusses the security implications of SDVN architectures at each layer. The layered (i.e., application, control, and data planes) architecture of SDVN must be secured in a way that the security solutions address cross-layer threats because the security breaches pertaining to one layer could cause harm to other layers as the layers are heavily dependent to each other.

5. SDVNs security analysis & countermeasures

In this section, we discuss the weaknesses of the state-of-the-art SDVNs against major security attacks that violate security services such as availability, confidentiality, authentication, and data integrity. We also discuss the existing countermeasures and provide possible solutions to handle the identified vulnerabilities.

Table 5
Attacks with varying technologies.

Attacks	SDN	VANET	SDVN	Example of Countermeasures
Control Plane Resource Consumption	Requests to the control plane from the data plane		Requests sent to the control plane and RSU controllers	Packet migration concept and data plane cache concept [108]. Blacklisting [109]
Network topology poisoning	Hijacking information including switch discovery, host discovery, switch-to-switch link discovery		hijacking locations of vehicles, or RSUs, or injecting false links in the topology	TOPOGUARD [110] and SPHINX [111] based solutions: topology update checker, anomaly detection approach based on verifying the inconsistencies in network states
Distributed DoS	Injection of more random false packets	injection of more random false packets	Injection of more random false packets that threatens the network availability	Solutions based in [112] and Floodguard [113]
Rule Conflicts violating existing security policies	Rules are overridden by other rules		Rules are overridden by other rules	FortNOX based solutions [114] enabling an authorization enforcement in the controller.
On-board tampering		Disrupting communications of other vehicles	Data modification, tampering with the on-board sensing	Anomaly detection behaviors. Watchdog dogs to monitor the behaviors of the relaying nodes [115].
Privacy violation	Disclosing sensitive information	Revealing identity of vehicles, their license plate, their location, etc.	Sensitive information leakage about vehicle or RSU controller status	Conditional privacy preserving mechanisms. Solutions based on GSIS [116] for identity privacy, or on location anonymity [117].
Forgery	Forging and transmitting false rules	transmitting false messages	Transmitting fake rules and messages	Techniques based on autonomous position verification [118], verifiable multilateration [119]
Jamming		Jamming a network by using a powerful transmitter	Jamming network by partitioning the network, controllers will not be able to guide vehicles or have the correct view of the network	Monitoring the quality of channels [71]
Impersonation		Masquerade as another entity in the network, or spoofing messages by impersonating RSUs	Masquerade as another entity, influence the route by spreading incorrect information	Solutions based on position verification, detection at the time of topology discovery by using the link layer discovery protocols to detect impersonation attacks [120]
Application-based attacks		Attacks related to specific vehicular applications	False Rules installed in the controller	Anomaly detection systems [121]
Malware attack injection	Injecting a malicious software in the controller	Injecting a malicious software on the vehicles	Injecting malicious codes in the different layers of the infrastructure: vehicles, RSU controllers, or controllers and applications	Malware attack detection schemes by using authentication mechanisms. Remote secure updates and attestation [122]
Routing attacks	Attacks affecting the forwarding of packets	Attacks affecting the routing path	Attacks affecting the path of messages in safety and non-safety applications	Approaches based on detecting infecting regions using geo-statistical model, analyzing the signal strength distribution, statistical analysis, and passive overhearing by fixed points, authentication and authorization mechanisms [123–125]

In Table 5, we present the main attacks that threaten SDN systems, VANET, and whether they could be persistent in SDVN environments. When an attack targets the software-defined networks, it mostly impacts also the SDVN architectures such as the control plane resource consumption, the network topology poisoning, and rule conflicts. Moreover, attacks that are tailored against vehicular systems are most of them persistent on the SDVN architectures such as the on-board tampering, the jamming, and the application-based attacks. Attacks as the replay attack, the sybil, the sinkhole, malware injection, privacy violation, forgery, distributed DoS are persistent in SDN, VANET, and SDVN but with different requirements and impact on each technology.

5.1. Control plane resource consumption.

Most of the SDVN architectures proposed in the literature [42,43,75,81,89,92] have been designed without security in mind. In particular, they are vulnerable to control plane resource consumption, which is a significant weakness in SDN networks. The control plane resource consumption attack is triggered when there are many requests to the control plane from the data plane. In SDVN, the control plane is composed of different RSU controllers that can enforce flow rules and then enables to control the network efficiently. However, this control mode can cause severe problems in particular due to many requests sent to the control plane. In SDVN like architectures, the RSU controller in [42,81] should support a maximum of requests than usual. For instance, in some situations, network packets in some RSU should wait until the vehicle deletes old flow rules. Finally, the impact of this attack is that it consumes resources of the control plane through the number of flow rules that could be handled, and the data plane through the number of flow rule entries.

Possible countermeasures to the control plane resource consumption in SDVN architectures can be the adoption of current solutions in SDN, such as in [108,109,126,127]. In [108], the authors proposed to keep both control plane and data plane func-

tional even when there is a data-to-control plane saturation attack. In particular, they adopt the packet migration concept. Also, they used the data plane cache concept to reduce fake packets by distinguishing them from normal ones. In a typical SDVN architecture, the two modules can be added at the controller level. In [109], the authors proposed LineSwitch, a solution based on two concepts related to probability and blacklisting. The solution provides both resiliency against SYN flooding saturation attacks and protection from buffer saturation. In [127], FloodDefender is based on three techniques that are the table-miss engineering, the packet filtering, and the flow rule management. The main goal of this solution is to reduce the bandwidth jamming and save the memory space of switches.

Solutions dedicated to SDN networks might be adopted in SDVN by taking into account their characteristics such as high mobility of devices and dynamic network topology. In particular, techniques based on deep learning for reducing fake packets could be efficient for handling mobile networks with a huge amount of data. Deep learning is distinguished by automatically extracting high-level features from a huge amount of data and prevents overfitting due to the use of recent regularization techniques. However, traditional machine learning classification techniques rely upon feature engineering methods to reduce the dimensionality of the input.

5.2. Network Topology Poisoning.

The topology information is mostly related to upper-layer applications such as packet routing, network virtualization and optimization, and mobility tracking [128,129]. The controller maintains topology information and provides it to upper layers and services. In the case of SDN network, the topology management includes switch discovery, the host discovery, and switch-to-switch link discovery. A network topology poisoning consists of modifying the topology information on the controller side. When a network topology poisoning attack happens in SDVN, this will cause dangerous situations since all the dependent services and applications will be affected. This attack infects SDN and SDVN networks. For instance, the packet routing can be affected, and this will incur a man-in-the-middle attack or black-hole routing path. Another scenario illustrates the impact of an attacker succeeding to hijack the location of a network server to phish its subscribers. In a smart parking application using the SDVN architectures in [90], the attacker can hijack the location of a controller to phish its service subscribers. Moreover, the impact of the attack could be that the controller will not be able to found the correct parking lot information. By executing a topology poisoning attack, the attacker can even create black-hole routes by injecting false links in the topology in safety applications. Architectures in [42,43,68,76,81,90] are vulnerable to the network topology poisoning. Two known solutions TopoGuard [110] and SPHINX [111], detect these topology poisoning attacks via packet monitoring. TopoGuard detects false network links based on behavioral profiling. In particular, the authors of TopoGuard propose a topology update checker module to monitor the network topology and validate topology updates [110]. In SPHINX, the authors propose an anomaly-detection approach based on verifying the inconsistencies in network states. In [129], the authors propose an extension to TopoGuard called TopoGuard+. The solution monitors the characteristic control plane message patterns, and then defend against out-of-band port amnesia attacks.

5.3. Distributed denial of service attacks.

Distributed Denial of Service (DDoS) attacks affect the SDN, VANET, as well as the SDVN networks in [42,43,75,81,89,92]. Most of the SDVN architectures [89,92,130] are vulnerable to Distributed Denial of Service (DDoS) attacks. Since SDVNs architectures are split into three main functional layers: infrastructure layer (vehicles, RSU), control layer (RSU controllers), and application layer, then potential DDoS attacks can be launched on any one or more of these three layers. For instance, an attacker executes a DDoS by injecting more random fake packets into the network. The controller must process and generate the corresponding flow entries. The new entries will consume the overall flow table in the switch, and the quality of service of this later is downgraded. The impact of this attack is that it depletes the resources. In the case of infotainment applications, when attackers inject more fake packets, this will consume the resources of RSU controllers and switches/vehicles, and could even threaten the service availability.

As a countermeasure to DDoS, one might use the solution in [112], where the authors propose a machine learning technique for DDoS detection. In particular, the flow statistics are collected from the switches or vehicle sensors and then trained. However, using such a solution at vehicles could be problematic due to the resource constraint nature of sensors when compared with the generic SDN switches. Another solution Floodguard [113], consists of preventing DDoS attacks by using packet migration and data plane cache. The packet migration technique aims to protect both the controllers and the switches, and the data plane cache technique stores table-miss packets and differentiate anomalous packets from normal ones.

5.4. Rule conflicts.

In SDN, an OpenFlow switch specifies a flow table that contains a set of flow rules. These rules aim to provide instructions on how to forward, modify, or even drop each packet that traverses the switch, and it specifies how the data plane should process all active network flows. The rule conflicts are triggered when (secure) rules are overridden by other (non-secure) rules. Rule conflicts could have dreadful attacks in OpenFlow applications in SDN and SDVN networks. For instance, some rules could be dedicated to quarantine a server that is overridden by a load-balancing application that may determine that the targeted host is the least-loaded server [121]. An attacker can exploit such vulnerabilities in the SDVN architectures presented in [42,44,68,76,91].

Possible countermeasures can be adopted to solve the rule conflicts in SDN based applications. For instance, FortNOX [114] detects rule conflicts that violate existing security policies and offers authorization enforcement in the controller kernel. One may install FortNOX features in the RSU controller in SDVN based architectures.

5.5. Privacy.

Privacy leakage affects SDN, VANET, and SDVN architectures. In SDVN based architectures, various user-related information has to be protected, such as the license plate, the position, and the driver's name. However, the authorities should be able to reveal their identities in case of an accident or a dispute [131]. Conditional privacy-preserving mechanisms in vehicular communications can be adapted to vehicular software architectures. In [116,132], the authors propose solutions that integrate the group based signatures and ID-based signatures, and offer security and privacy-preserving mechanisms between different OBUs, and between OBUs and RSUs. In [117], the authors propose a location privacy-preserving authentication scheme based on the blind signature. The scheme guarantees the location anonymity to the public. Using the proposed scheme, the probability of tracing a vehicle's route is small. In [70], the authors propose a distributed aggregate privacy-preserving authentication mechanism. In particular, the protocol is based on a one-time identity-based aggregate

signature technique, where a vehicle could verify multiple messages at the same time. In SDVNs, the lack of secure communication channel (i.e., southbound interface) between the control and data plane, and disclosure on network resources stored at SDN or RSU controllers could expose the VANET users to various privacy risks. Moreover, the northbound interface protocols should be secured, and fine-grained access control needs to be enforced before the SDN or VANET applications access the controller information. In particular, the global information residing at the controller should be protected from any privacy leakages caused by adversaries residing at any of the three planes.

5.6. Forgery.

This attack consists of forging and transmitting false messages in SDN, Vanet, or SDVN networks. In safety applications, an attacker forging a false warning message could contaminate large portions of roads [37,39]. For instance, an attacker can broadcast a forged GPS signal to mislead vehicles to get wrong location information. An example of traditional countermeasures against this attack is to ensure secure localization. In [133], the authors present the triangulation as a technique to determine the position of a vehicle from three reference points. Using this technique, attackers cannot decrease the distance between two neighboring vehicles. In [134], the authors propose a technique to localize cheating nodes. In [119], the authors design a verifiable multilateration technique to determine the position of a vehicle from a set of reference points whose locations are known in advance. Autonomous position verification [118] is a mechanism to detect the impact of falsified position information in particular for position-based routing protocols at VANETs. It is based on various concepts such as the maximum density threshold, and position claim overhearing. In [37], the authors propose a secure, distributed location verification to detect vehicles cheating about their positions. The detection mechanism does not rely on additional hardware but only on collaborative neighbors.

5.7. Tampering.

The tampering attack could be executed in different forms. A vehicle that acts as a relay in safety applications or infotainment applications can disrupt communications of other vehicles, thus leading to in-transit tampering. Hence, this attack will let the vehicle drop or modify or corrupt transmitted messages in the area of interest. Moreover, another kind of tampering is the onboard tampering, which consists of leveraging the data plane level of SDVN architectures composed of different vehicles. In particular, an attacker may modify data, tamper with the onboard sensing in the different vehicular applications (safety and non-safety ones). To detect tampered data packets, the existing approaches are based on anomaly detection behaviors [135]. For instance, in [115], the authors propose an autonomous watchdog formation to ensure that watchdog nodes monitor the behaviors of the relaying nodes.

5.8. Jamming.

In a jamming attack, an attacker can partition the network even without compromising cryptographic mechanisms [47] in Vanet or SDVN applications. Due to the broadcast nature of wireless communication, an attacker can jam the network by using a powerful transmitter. This attack could lead to preventing the reception of sensed data in case of a smart parking application or a safety application that alerts vehicles about possible dangers. Moreover, the RSU controller will not be able to guide vehicles. In the SDVN based architectures, this attack could be mitigated. In particular, the RSU gathers and monitors the quality of channels, and then forwards the report to a controller. This later selects the list of bad channels and asks the RSU to forward this list to all deployed sensors [71].

5.9. Impersonation.

In this type of attack, an attacker can masquerade as police to mislead other vehicles to slow down or change direction [47] in vehicular safety applications. An attacker can also spoof safety messages or service advertisements, and then impersonates roadside unit controllers. Moreover, an attacker can influence the route of its neighbor vehicles by spreading incorrect information about road conditions. Different approaches have been proposed to detect impersonation attacks [120,136–138] in vehicular systems. In [136], the authors propose a distributed approach, where every vehicle can verify the claimed positions of its nearby vehicles to detect misbehaving vehicles. The proposed method is based on statistic algorithms to enhance the accuracy of position verification. The detection of cheating nodes is confirmed when observing the signal strength distribution of a suspect vehicle over a while. In [120], the authors propose to trace back the potential sources of an anomaly in the network. In particular, they propose a method to identify the different switches composing the network path of an anomaly in the SDN. In SDVNs, the impersonation attacks could be detected at the time of topology discovery, and the SDN controllers perform that by using the link-layer discovery protocols.

5.10. Malware Attack Injection.

In SDVN based architectures, an attacker can maliciously inject a software that replicates itself through the different controllers and switches/vehicles, and in different layers of the SDVN architecture. This attack affects the SDN, VANET, and SDVN networks. Remote attacks through Bluetooth or cellular communications allow the attacker to take control of a vehicle. One of the vulnerability limitations resides in the lack of message authentication of the controller area network (CAN). In [122], the authors propose a framework for vehicular systems that employs a trust group structure to authenticate messages of the CAN bus.

5.11. Routing based attacks.

SDN, VANETs, and SDVN based architectures are vulnerable to routing attacks such as sinkhole, sybil, and replay attacks. The sinkhole attack is executed by a vehicle or an RSU to route all traffic to it. For instance, in service-based advertisements or alert warning message applications, an RSU controller can execute this attack to instruct a portion of vehicles to route all traffic to it. Hence, this malicious RSU behaves as a malicious gateway that could either stop the propagation of messages or not inform other vehicles in a particular area of interest. To remediate against this kind of attack infecting safety and non-safety applications, the authors in [139] propose a centralized approach to detect infected regions in the network using a geo-statistical model. Moreover, the authors propose a distributed monitoring approach to explore neighbors to identify malicious nodes.

Another dreadful attack impacting the performance of most SDVN based architectures is the sybil attack. A sybil attack consists of creating multiple fictitious identities of vehicles to create an illusion of traffic congestion in the road. This attack has an impact on safety applications and degrades the performance of the system. Examples of approaches to alleviating against the sybil attack detection in SDVN architectures are the ones proposed in [123–125]. In particular, the solutions analyze the signal strength distribution to detect sybil attacks. In [123], the authors propose a statistical method that verifies where a vehicle comes from. This approach

uses statistical analysis over a period to improve detection accuracy. In [125], the detection of sybil nodes is done through passive overhearing by fixed points in the road. When executing a replay attack, the attacker first sniffs a message and then reuses it to access to a restricted network. Approaches such as as [116] for message authentication and authorization might be used in this context.

5.12. Application-based attacks.

In the following, we consider two specific applications, such as smart grid and platoon management.

- In a smart grid application, SDVN architecture can be used where data plane includes Electric Vehicles (EVs) and Electrical Vehicle Supply Equipments (EVSEs). Attacks on the smart grid include the previously mentioned attacks, such as network flooding, topology poisoning, and transmission jamming. When an electric vehicle needs to connect to the EVSEs, an information message is sent to the controller in order to track the current network topology and status of the network. Anomaly detection systems such as the ones in [121] can be added to the controller to monitor network traffic and detect compromised data. The controller can install forwarding rules, and it can detect attacks implied by unusual behaviors in the smart grid application.
- In platooning vehicular applications, attacks such as changing lane, merging, accelerating, decelerating, redirecting traffic, or changing direction can be performed. In SDVN architectures, the controller can install the appropriate rules related to the acceleration/deceleration, merging/splitting, and changing lane taking into account inputs from traffic conditions and events on the roads. Then a controller can collect information on road status and anomalous vehicle behavior by using exchanged messages. In particular, mechanisms such as the ones deployed in [116] can be efficient to detect misbehavior in platooning SDVN applications, or detect rule conflicts attacks by using [121]. To ensure better network utilisation, the RSU controller in SDVN based applications have the role of instructing the platoon leader to set different parameters. These parameters include the scheduling policy of data messages, acceleration, or deceleration. Furthermore, an RSU controller can detect attacks such as jamming, replay, or attacks targeting the management protocols. These attacks can induce maneuvers such as splitting, merging, or lane changing, and have an impact on VANET and SDVN networks.

6. Discussion and open issues

In this section, first, we summarize our findings along with the lessons learned that are gathered from our review on the state-of-the-art efforts of SDVN and its integration with other technologies (e.g., fog computing, vehicular cloud, NDN, and 5G) for supporting emerging vehicular network applications and services. Then we present the possible research directions along with future issues and challenges. Some of these challenges we have covered in Section 4. However, this section briefly includes the rest of the challenges and open research directions.

As confirmed by the large number of research works that we have discussed in our survey, the industry and academia are pushing towards the design and configuration of new SDVN architectures. The rapid push in this direction is the result of the emerging and innovative applications (e.g., 5G, Automated Transport Systems, and Internet of Vehicles) of VANETs that have stringent requirements concerning robustness, flexibility, latency (i.e., time constraints for critical real-time decision making), security, and privacy. In the literature, the researchers envision the efficient deployment of these applications by using the SDVNs coupled with other next-generation technologies such as mobile edge/fog computing, Name Data Networking (NDN), and Network Function Virtualization (NFV).

6.1. Lessons learned

Below we discuss the key lessons learned from our comprehensive survey on SDVN architectures and their usage in emerging vehicular applications.

- Although various architecture designs for SDVNs have been proposed in the literature to improve the communication reliability and security in VANET scenarios, the comprehensive investigation to evaluate the deployment feasibility, effectiveness, and correctness of these architectures remains an open issue. In particular, the new security and privacy vulnerabilities that arise due to the coupling of new technologies (such as SDN, NFV, and mobile edge computing) with the existing VANET should be carefully studied, and the same is completely missing so far. For instance, researchers should not only report the benefits of using SDN to improve VANET architecture, but the new issues (e.g., service latency, mobility, and securing the SDN controller) that are inherent to SDN and now hindering the performance of the SDVNs should also be investigated and discussed.
- The placement of the SDN controller is considered as a key design problem at the control plane, and its optimal placement is regarded as a challenging task [140]. It is because the impact of the controller position is vast, ranging from communication latency to resiliency, from resource management to optimal routing, and so on. With SDVN, the controller placement problem becomes more complicated and unique, as there are new candidates such as BSUs and RSUs that could be considered as controllers. However, none of the state-of-the-art SDVN proposals address this particular issue.
- Security & privacy (S&P) is one of the most critical requirements of VANETs because of its usage in mission-critical and life-sensitive applications. For instance, (i) an adversary could maliciously take control of vehicles in an ITS or driverless scenario, and it could cause serious damage to infrastructure and human life, or (ii) the driver and vehicles sensitive information (e.g., location or travel route) could be leaked from a centralized controller. However, most of the existing SDVNs ignore S&P issues. Yet, since the design and implementation of SDVNs are in the early stages, the developers have a great chance to provide S&P by design.
- It is vital to look at how dynamic real-time change, rapid on-demand growth (scalability), and integration of service context will play a key role in enabling successful deployment and avoiding performance visibility gaps in SDVNs. Since, in the recent future, the VANET architecture will continuously be evolving to satisfy the rapidly growing requirements of its new applications.
- Finally, setting up local and global test-bed(s) deployed in real scenarios to evaluate the performance of the new SDVN architectures, and the feasibility of the solutions, designed to mitigate the S&P affecting a VANET application seemed an essential requirement when we looked into the SDVNs state-of-the-art.

6.2. Future directions

Next, we present a few research directions that should be exploited in the course of improving SDVN architecture design and functionalities at various fronts.

- *Security of 5G slicing for V2X Services:* SDN is one of the key enablers for 5G systems. This will hinder applications characterized by single or multi-tenancy. The diverging 5G V2X services span from a single automated vehicle in a smart city to enhanced real-time navigation systems on board. In traditional networks, different services can be supported in the same architecture and can be built without elasticity in mind. Moreover, these services share the same resources and are processed by the same network elements. The concept of network slices has emerged as a novel technology that isolates network functions and resources [141–144]. As defined by [145,146], a network slice represents a collection of 5G network functions and specific parameters that are combined to provide a particular use case or a business model. These resources and functions are tailored to a market's need on a shared infrastructure. The network slicing is based on virtualization, where the Network Function Virtualization (NFV) paradigm is based on the fact that network functions are not tied to the hardware. Hence, these network functions can be deployed as virtual network functions, and they run on different platforms. The SDN controller configures the different VNF and physical network functions in one slice. Due to the features of V2V or V2I [142–144], different network slices can be presented such as: 1) slice for autonomous driving, 2) slice for teleoperated driving; 3) slice for vehicular infotainment applications; and 4) slice for vehicle remote diagnostics. Security and privacy challenges could be raised in one slice (intra-slice) or inter-slice communication. One should ensure that one slice cannot consume other slice's resources. Also, sharing a physical platform might lead to attacks such as side-channel attacks and privacy leaks. Moreover, an adversary might obtain capabilities to launch attacks to slices and on-going slices, for instance, to modify the configuration of other customer's slice instances, compromising a network function, or even terminate a slice. Hence, this will expose the services and network to disclosure and removal. We identify here the need to investigate security requirements and security solutions for network V2X slicing. Moreover, we should mention that important efforts are still needed from researchers and industries to design a complete approach to enable secure slicing in 5G vertical domains such as the automotive systems.
- *Secure Function Chaining in SDVNs:* In virtualized environments, vehicles will require to communicate with the infrastructure to provide services such as traffic management, collision avoidance, online gaming, etc. Hence, this will require the deployment of specific VNFs tailored for the network (as self-healing virtual functions: self-organization, terminal self-discovery, and mobility management) and virtual functions for the intra-vehicle domain such as the virtual On-Board Unit function. On the other hand, to monitor traffic and avoid security attacks, network operators need to specify also security functions such as the virtual intrusion detection system, virtual Firewall, virtual Intrusion Protection system, and virtual DDoS. Different tenants might have different security requirements for their flows by considering a set of security functions their flow should pass by. Hence, one should consider the placement and the ordering of these VNFs. In [147,148], the authors consider different approaches to secure VNF placement concerning their order and instantiation in the traffic. This placement of secure functions throughout the flow traffic of tenants should be dynamic to cope with the mobility of vehicles and the different services that they provide. In [149], the authors present security threats regarding the deployment and implementation of virtual network functions.
- *Mobile Edge Computing Security:* The MEC could host different VNFs to allow secure and trusted communications of services between vehicles or between vehicles to infrastructures. However, the MEC comes up with security challenges related to: (i) the secure service chaining of different VNFs hosted in the MEC, (ii) the certification of VNFs at the MEC, and (iii) the use of distributed machine learning algorithms for intrusion detection at MEC to reduce the bottleneck and energy consumption of vehicles/sensors.
- *Information Centric Networking (ICN) based Solutions:* Originally, the ICN was envisioned to address the pressing needs (e.g., device mobility, network scalability, fast access to information, and distributed content production) of today's Internet. However, due to its unique advantages that suit the various requirements of different network architectures, including SDN [150], 5G [151], and VANETs [79,152,153], the use of ICN paradigm is envisioned in these architectures as well. To this end, there are several preliminary solutions (i.e., ICN enabled SDVNs) that have been proposed by using a widely known ICN instance, namely Named-Data Networking (NDN). The communication model of NDN replaces the traditional host-centric paradigm to a new information-centric one. Due to the various benefits that NDN provides, researchers have investigated its usage for addressing different VANET challenges [154–157]. For instance, authors in [152] propose a V2I communication architecture that exploits deployed RSU infrastructure for content retrieval in NDN-VANETs. The authors show that the use of NDN could provide improvements in VANET concerning mobility management, resource consumption, and faster content retrieval. We believe that the use of NDN in SDVNs or SDN in NDN-VANETs has significant potential to improve the VANETs. However, these domains still remain highly under-investigated and need significant work to move forward for real-world deployments. In particular, the new issues and challenges that arise from the combination of these three technologies need to be fully understood, and adequate solutions for the identified problems should be envisioned [158].
- *Mobility Management:* Providing efficient mobility management in SDVNs is important to keep a consistent and accurate global topology view at the SDN controller, which is needed to enable various networking functionalities (e.g., routing, traffic management, security services, and network virtualization) correctly in the network. Although the SDN provides network control, which is flexible and programmable, but its applicability to mobile networks (such as VANETs and 5G) is still in its infancy. Therefore, new mobility management techniques such as proactive mobility management algorithm implementation and hybrid control plane switches to whom the controller can delegate partial load for mobility management are needed [159]. One way to minimize the mobility induced communication challenges is to develop efficient and accurate mobility prediction models [35]. In SDVNs, firstly, the availability of the network-wide topology at the SDN controller could help to predict the accurate mobility of vehicles through advanced machine learning algorithms (e.g., artificial neural network (ANN)). Secondly, these prediction results can be used by the RSUs and BS during high mobility events, to estimate the precise Expected Transmission Count (ETX) probability and end-to-end delay of each vehicle's request. Another option is to use ICN paradigm, which supports efficient data retrieval in high mobility scenarios [160]. ICN effectively handles mobility issues because it facilitates data retrieval that is independent of the physical location of the source or producer of the data. Hence it could be seen as a key enabler for future vehicular networks [161]. However, the ICN architecture also presents a new set of security vulnerabilities such as router cache poisoning, Interest flooding, and privacy leakage attacks, these threats need to be properly investigated before its use in SDVNs [162].

7. Conclusions

In this paper, we thoroughly investigate state-of-the-art SDVN architectures for their positive and negative impacts, mainly in terms of security and privacy. Based on the existing SDVN architecture, we analyze different security vulnerabilities and attacks. We propose an array of open security research issues that require the attention of industries and researchers to establish a way forward for more secure and efficient SDVNs. Moreover, we discuss the applicability of the existing solutions and propose possible countermeasures to handle these attacks. At this point, we can safely conclude that the research on SDVNs is just beginning, and SDN can support VANET to achieve the objectives that are needed to use it for next-generation intelligent VANET applications and services. However, many issues need to be addressed before its practical deployment. This paper opens the debate for secure slicing in V2X communications, secure mobile edge computing, mobility management, and usage of information-centric networking in SDVNs. Through the future research directions that we have raised, this work acts as a catalyst to address emergent security and privacy issues of future SDVN architectures.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

Wafa Ben Jaballah is partially supported by the H2020 PHOENIX under grant H2020-SU-DS-2018-832989. Mauro Conti and Chhagan Lal are partially supported in part by EU LOCARD Project under Grant H2020-SU-SEC-2018-832735. The work of M. Conti was supported by the Marie Curie Fellowship through European Commission under Agreement PCIG11-GA-2012-321980.

References

[1] R.G. Engoulou, M. Bellaíche, S. Pierre, A. Quintero, Vanet security surveys, Comput. Commun. 44 (2014) 1–13.
[2] A. Boukerche, R.E.D. Grande, Vehicular cloud computing: architectures, applications, and mobility, Comput. Netw. 135 (2018) 171–189.
[3] H. Aksu, L. Babun, M. Conti, G. Tolomei, A.S. Uluagac., Advertising in the iot era: vision and challenges, IEEE Commun. Mag. (2018).
[4] A. Ydenberg, N. Heir, B. Gill, Security, sdn, and vanet technology of driver-less cars, in: 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), 2018, pp. 313–316.
[5] J. Weng, J. Weng, Y. Zhang, W. Luo, W. Lan, Benbi: scalable and dynamic access control on the northbound interface of sdn-based vanet, IEEE Trans. Veh. Technol. 68 (1) (2019) 822–831.
[6] C. Jiacheng, Z. Haibo, Z. Ning, Y. Peng, G. Lin, S. Xuemin (Sherman), Software defined internet of vehicles: architecture, challenges and solutions, J. Commun. Inf. Netw. 1 (1) (2016) 14–26.
[7] I. Yaqoob, I. Ahmad, E. Ahmed, A. Gani, M. Imran, N. Guizani, Overcoming the key challenges to establishing vehicular communication: Is sdn the answer? IEEE Commun. Mag. 55 (7) (2017) 128–134.
[8] M. Chahal, S. Harit, K.K. Mishra, A.K. Sangaiah, Z. Zheng, A survey on software-defined networking in vehicular ad hoc networks: Challenges, applications and use cases, Sustain. Cities Soc. 35 (2017) 830–840.
[9] R.A.R. H. Shafiq, B. Kim, Services and security threats in sdn based vanets: asurvey, Wirel. Commun. Mob. Comput. (2018) 1–14.
[10] L. Xie, Y. Ding, H. Yang, X. Wang, Blockchain-based secure and trustworthy internet of things in sdn-enabled 5g-vanets, IEEE Access (2019) 56656–56666.
[11] A.J. Kadhim, S.A.H. Seno, Energy-efficient multicast routing protocol based on sdn and fog computing for vehicular networks, Ad Hoc Netw. 84 (2019) 68–81.
[12] S. Din, A. Paul, A. Rehman, 5g-enabled hierarchical architecture for software-defined intelligent transportation system, Comput. Netw. 150 (2019) 81–89.
[13] D. Kreutz, F.M.V. Ramos, P.E. Verissimo, C.E. Rothenberg, S. Azodolmolky, S. Uhlig, Software-defined networking: a comprehensive survey, Proc. IEEE 103 (1) (2015) 14–76.
[14] K. Liu, J.K.Y. Ng, V.C.S. Lee, S.H. Son, I. Stojmenovic, Cooperative data scheduling in hybrid vehicular ad hoc networks: vanet as a software defined network, IEEE/ACM Trans. Netw. 24 (3) (2016) 1759–1773.
[15] S. Jiang, X. Zhu, L. Wang, An efficient anonymous batch authentication scheme based on hmac for vanets, IEEE Trans. Intel. Transp. Systems 17 (8) (2016) 2193–2204.
[16] J.C. Mukherjee, A. Gupta, R.C. Sreenivas, Event notification in vanet with capacitated roadside units, IEEE Trans. Intel. Transp. Systems 17 (7) (2016) 1867–1879.
[17] J. Heinovski, F. Klingler, F. Dressler, C. Sommer, Performance comparison of ieee 802.11p and arib std-t109, in: 2016 IEEE Vehicular Networking Conference (VNC), 2016, pp. 1–8.
[18] I.A. Sumra, H.B. Hasbullah, J. AbManan, Attacks on security goals (confidentiality, integrity, availability) in vanet: a survey, in: A. Laouiti, A. Qayyum, M.N. Mohamad Saad (Eds.), Vehicular Ad-Hoc Networks for Smart Cities, Springer Singapore, Singapore, 2015, pp. 51–61.
[19] S. Tuohy, M. Glavin, C. Hughes, E. Jones, M. Trivedi, L. Kilmartin, Intra-vehicle networks: a review, IEEE Trans. Intel. Transp. Syst. 16 (2) (2015) 534–545.
[20] J. Huang, M. Zhao, Y. Zhou, C. Xing, In-vehicle networking: protocols, challenges, and solutions, IEEE Netw. 33 (1) (2019) 92–98.
[21] F.D. da Cunha, L. Villas, G. Maia, A.C. Viana, Data communication in vanets: survey, applications and challenges, Elsevier Ad Hoc Netw. 44 (2016) 90–103.
[22] D. Lin, J. Kang, A. Squicciarini, Y. Wu, S. Gurung, O. Tonguz, Mozo: a moving zone based routing protocol using pure v2v communication in vanets, IEEE Trans. Mob. Comput. 16 (5) (2017) 1357–1370.
[23] J. Liu, J. Wan, Q. Wang, P. Deng, K. Zhou, Y. Qiao, A survey on position-based routing for vehicular ad hoc networks, Telecommun. Syst. 62 (1) (2016).
[24] F. Abbas, P. Fan, Clustering-based reliable low-latency routing scheme using aco method for vehicular networks, Elsevier Veh. Communi. 12 (1) (2018) 66–74.
[25] (https://www.3gpp.org/).
[26] K. Abboud, H.A. Omar, W. Zhuang, Interworking of dsrc and cellular network technologies for v2x communications: A survey, IEEE Trans. Veh. Technol. 65 (12) (2016) 9457–9470.
[27] Q. Xu, T. Mak, J. Ko, R. Sengupta, Vehicle-to-vehicle safety messaging in dsrc, in: Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks, in: VANET '04, 2004, pp. 19–28.
[28] S. Chen, J. Hu, Y. Shi, Y. Peng, J. Fang, R. Zhao, L. Zhao, Vehicle-to-everything (v2x) services supported by lte-based systems and 5g, IEEE Communications Standards Magazine 1 (2) (2017) 70–76.
[29] R. Molina-Masegosa, J. Gozalvez, Lte-v for sidelink 5g v2x vehicular communications: A new 5g technology for short-range vehicle-to-everything communications, IEEE Vehicular Technology Magazine 12 (4) (2017) 30–39.
[30] Intelligent Transport Systems (ITS); European Profile Standard for the Physical and Medium Access Control Layer of Intelligent Transport Systems Operating in the 5 GHz Frequency Band, ETSI ES 202 663 V1.1.0, 2010.
[31] IEEE Standard for Information Technology Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std. 802.11-2012 (Revision of IEEE Std. 802.11-2007), 2012.
[32] Standard Specification for Dedicated Short Range Communication (DSRC) Physical Layer Using Microwave in the 902 to 928 MHz Band (Withdrawn 2010), ASTM E2158-01, 2001.
[33] C. Campolo, A. Molinaro, A. Iera, A reference framework for social-enhanced vehicle-to-everything communications in 5g scenarios, Comput. Netw. 143 (2018) 140–152.
[34] W.B. Jaballah, M. Conti, C.E. Palazzi, The position cheating attack on inter-vehicular online gaming, in: 2018 15th IEEE Annual Consumer Communications Networking Conference (CCNC), 2018, pp. 1–6.
[35] Y. Tang, N. Cheng, W. Wu, M. Wang, Y. Dai, X. Shen, Delay-minimization routing for heterogeneous vanets with machine learning based mobility prediction, IEEE Transactions on Vehicular Technology (2019). 1–1
[36] B.T. Sharef, R.A. Alsaqour, M. Ismail, Vehicular communication ad hoc routing protocols: a survey, J. Netw. Comput. Appl. 40 (Supplement C) (2014) 363–396.
[37] W.B. Jaballah, M. Conti, M. Mosbah, C.E. Palazzi, Fast and secure multihop broadcast solutions for intervehicular communication, IEEE Trans. Intel. Transp. Syst. 15 (1) (2014) 433–450.
[38] C.-T. Li, M.-S. Hwang, Y.-P. Chu, A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks, Comput. Commun. 31 (12) (2008) 2803–2814.
[39] W.B. Jaballah, M. Conti, M. Mosbah, C.E. Palazzi, The impact of malicious nodes positioning on vehicular alert messaging system, Ad Hoc Netw. 52 (Supplement C) (2016) 3–16.
[40] C.E. Palazzi, M. Roccetti, S. Ferretti, An intervehicular communication architecture for safety and entertainment, IEEE Trans. Intel. Transp. Syst. 11 (1) (2010) 90–99.
[41] M.B. Younes, A. Boukerche, Intelligent traffic light controlling algorithms using vehicular networks, IEEE Trans. Veh. Technol. 65 (8) (2016) 5887–5899.
[42] I. Ku, Y. Lu, M. Gerla, R.L. Gomes, F. Ongaro, E. Cerqueira, Towards software-defined vanet: architecture and services, in: 2014 13th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET), 2014, pp. 103–110.
[43] Z. He, J. Cao, X. Liu, SDVN: enabling rapid network innovation for heterogeneous vehicular communication, IEEE Netw. 30 (4) (2016) 10–15.

[44] J. Liu, J. Wan, B. Zeng, Q. Wang, H. Song, M. Qiu, A scalable and quick-response software defined vehicular network assisted by mobile edge computing, IEEE Commun. Mag. 55 (7) (2017) 94–100.
[45] M. Azizian, S. Cherkaoui, A.S. Hafid, Vehicle software updates distribution with sdn and cloud computing, IEEE Commun. Mag. 55 (8) (2017) 74–79.
[46] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, B. Qin, Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response, IEEE Trans. Comput. 65 (8) (2016) 2562–2574.
[47] M. Raya, J.P. Hubaux, Securing vehicular ad hoc networks, Elsevier Comput. Secur. 15 (1) (2007) 39–68.
[48] G. Yan, D. Wen, S. Olariu, M.C. Weigle, Security challenges in vehicular cloud computing, IEEE Trans. Intel. Transp. Systems 14 (1) (2013) 284–294.
[49] F. Qu, Z. Wu, F. Wang, W. Cho, A security and privacy review of vanets, IEEE Trans. Intel. Transp. Systems 16 (6) (2015) 2985–2996.
[50] W. Xia, Y. Wen, C.H. Foh, D. Niyato, H. Xie, A survey on software-defined networking, IEEE Commun. Surv. Tutor. 17 (1) (2015) 27–51.
[51] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, J. Turner, Openflow: enabling innovation in campus networks, SIGCOMM Comput. Commun. Rev. 38 (2) (2008) 69–74.
[52] S. Scott-Hayward, S. Natarajan, S. Sezer, A survey of security in software defined networks, IEEE Commun. Surv. Tutor. 18 (1) (2016) 623–654.
[53] F. Bonomi, R. Milito, J. Zhu, S. Addepalli, Fog computing and its role in the internet of things, in: Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, in: MCC '12, 2012, pp. 13–16.
[54] R. Roman, J. Lopez, M. Mambo, Mobile edge computing, fog et al.: a survey and analysis of security threats and challenges, Future Gener. Comput. Syst. 78 (2018) 680–698.
[55] K. Dolui, S.K. Datta, Comparison of edge computing implementations: fog computing, cloudlet and mobile edge computing, in: 2017 Global Internet of Things Summit (GIoTS), 2017, pp. 1–6.
[56] M. Ambrosin, A. Compagno, M. Conti, C. Ghali, G. Tsudik, Security and privacy analysis of national science foundation future internet architectures, IEEE Commun. Surv. Tutor. 20 (2) (2018) 1418–1442.
[57] L. Zhang, et al., Named data networking, ACM SIGCOMM CCR 44 (3) (2014) 66–73.
[58] A. Compagno, M. Conti, M. Hassan, An ICN-Based Authentication Protocol for a Simplified LTE Architecture, Springer International Publishing, Cham.
[59] V. Jacobson, et al., Networking named content, in: ACM International Conference on Emerging Networking Experiments and Technologies, 2009, pp. 1–12.
[60] S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system, Available: http://bitcoin.org/bitcoin.pdf (2008).
[61] A. et.al, Hyperledger fabric: a distributed operating system for permissioned blockchains, in: Proceedings of the Thirteenth EuroSys Conference, EuroSys '18, 2018, pp. 30:1–30:15.
[62] L. Xie, Y. Ding, H. Yang, X. Wang, Blockchain-based secure and trustworthy internet of things in sdn-enabled 5g-vanets, IEEE Access 7 (2019) 56656–56666.
[63] B. Nour, A. Ksentini, N. Herbaut, P.A. Frangoudis, H. Moungla, A blockchain-based network slice broker for 5g services, IEEE Netw. Lett. 1 (3) (2019) 99–102.
[64] C. Qiu, F.R. Yu, H. Yao, C. Jiang, F. Xu, C. Zhao, Blockchain-based software-defined industrial internet of things: A dueling deep Q -learning approach, IEEE Internet Things J. 6 (3) (2019) 4627–4639.
[65] M. Conti, E. Sandeep Kumar, C. Lal, S. Ruj, A survey on security and privacy issues of bitcoin, IEEE Commun. Surv. Tutor. 20 (4) (2018) 3416–3452.
[66] F. Tschorsch, B. Scheuermann, Bitcoin and beyond: a technical survey on decentralized digital currencies, IEEE Commun. Surv. Tutor. 18 (3) (2016) 2084–2123.
[67] M. Belotti, N. Božić, G. Pujolle, S. Secci, A vademecum on blockchain technologies: When, which and how, IEEE Communications Surveys Tutorials (2019). 1–1
[68] Z. He, D. Zhang, J. Liang, Cost-efficient sensory data transmission in heterogeneous software-defined vehicular networks, IEEE Sensors Journal 16 (20) (2016) 7342–7354.
[69] X. Huang, R. Yu, J. Kang, N. Wang, S. Maharjan, Y. Zhang, Software defined networking with pseudonym systems for secure vehicular clouds, IEEE Access 4 (2016) 3522–3534.
[70] Y. Zhang, M. Chen, N. Guizani, D. Wu, V.C.M. Leung, Sovcan: safety-oriented vehicular controller area network, IEEE Commun. Mag. 55 (8) (2017) 94–99.
[71] I. Radhakrishnan, R. Soua, M.R. Palattellaz, T. Engel, An efficient service channel allocation scheme in sdn-enabled vanets, in: 2017 16th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net), 2017, pp. 1–7.
[72] N.B. Truong, G.M. Lee, Y. Ghamri-Doudane, Software defined networking-based vehicular adhoc network with fog computing, in: 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), 2015, pp. 1202–1207.
[73] D.J. Deng, S.Y. Lien, C.C. Lin, S.C. Hung, W.B. Chen, Latency control in software-defined mobile-edge vehicular networking, IEEE Commun. Mag. 55 (8) (2017) 87–93.
[74] X. Ge, Z. Li, S. Li, 5G software defined vehicular networks, IEEE Commun. Mag. 55 (7) (2017) 87–93.
[75] C.F. Lai, Y.C. Chang, H.C. Chao, M.S. Hossain, A. Ghoneim, A buffer-aware qos streaming approach for sdn-enabled 5g vehicular networks, IEEE Commun. Mag. 55 (8) (2017) 68–73.
[76] G.S. Aujla, R. Chaudhary, N. Kumar, J.J.P.C. Rodrigues, A. Vinel, Data offloading in 5g-enabled software-defined vehicular networks: A stackelberg-game-based approach, IEEE Commun. Mag. 55 (8) (2017) 100–108.
[77] X. Duan, Y. Liu, X. Wang, Sdn enabled 5g-vanet: adaptive vehicle clustering and beamformed transmission for aggregated traffic, IEEE Commun. Mag. 55 (7) (2017) 120–127.
[78] S.H. Ahmed, S.H. Bouk, D. Kim, D.B. Rawat, H. Song, Named data networking for software defined vehicular networks, IEEE Commun. Mag. 55 (8) (2017) 60–66.
[79] A. Arsalan, R.A. Rehman, Distance-based scheme for broadcast storm mitigation in named software defined vehicular networks (nsdvn), in: 2019 16th IEEE Annual Consumer Communications Networking Conference (CCNC), 2019, pp. 1–4.
[80] H. Li, M. Dong, K. Ota, Control plane optimization in software-defined vehicular ad hoc networks, IEEE Trans. Veh. Technol. 65 (10) (2016) 7895–7904.
[81] S. Correia, A. Boukerche, R.I. Meneguette, An architecture for hierarchical software-defined vehicular networks, IEEE Commun. Mag. 55 (7) (2017) 80–86.
[82] W. Quan, Y. Liu, H. Zhang, S. Yu, Enhancing crowd collaborations for software defined vehicular networks, IEEE Commun. Mag. 55 (8) (2017) 80–86.
[83] K.S. Kalupahana Liyanage, M. Ma, P.H.J. Chong, Link stability based optimized routing framework for software defined vehicular networks, IEEE Transactions on Vehicular Technology (2019). 1–1
[84] M.O. Kalinin, V.M. Krundyshev, P.V. Semianov, Architectures for building secure vehicular networks based on sdn technology, Autom. Control Comput. Sci. 51 (8) (2017) 907–914.
[85] E. Bozkaya, B. Canberk, QoE-based flow management in software defined vehicular networks, in: 2015 IEEE Globecom Workshops (GC Wkshps), 2015, pp. 1–6.
[86] C. Lai, H. Zhou, N. Cheng, X.S. Shen, Secure group communications in vehicular networks: asoftware-defined network-enabled architecture and solution, IEEE Veh. Technol. Mag. 12 (4) (2017) 40–49.
[87] M. Kalinin, P. Zegzhda, D. Zegzhda, Y. Vasiliev, V. Belenko, Software defined security for vehicular ad hoc networks, in: 2016 International Conference on Information and Communication Technology Convergence (ICTC), 2016, pp. 533–537.
[88] M. Arif, G. Wang, T. Wang, T. Peng, Sdn-based secure vanets communication with fog computing, in: G. Wang, J. Chen, L.T. Yang (Eds.), Security, Privacy, and Anonymity in Computation, Communication, and Storage, Springer International Publishing, Cham, 2018, pp. 46–59.
[89] A. Hussein, I.H. Elhajj, A. Chehab, A. Kayssi, Sdn vanets in 5g: an architecture for resilient security services, in: 2017 Fourth International Conference on Software Defined Systems (SDS), 2017, pp. 67–74.
[90] A. Soua, S. Tohme, Multi-level sdn with vehicles as fog computing infrastructures: a new integrated architecture for 5g-vanets, in: 2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), 2018, pp. 1–8.
[91] W. Qi, Q. Song, X. Wang, L. Guo, Z. Ning, Sdn-enabled social-aware clustering in 5g-vanet systems, IEEE Access 6 (2018) 28213–28224.
[92] A.A. Khan, M. Abolhasan, W. Ni, 5g next generation vanets using sdn and fog computing framework, in: 2018 15th IEEE Annual Consumer Communications Networking Conference (CCNC), 2018, pp. 1–6.
[93] D. Zhang, F.R. Yu, R. Yang, Blockchain-based distributed software-defined vehicular networks: A dueling deep q-learning approach, IEEE Transactions on Cognitive Communications and Networking (2019). 1–1
[94] C. Huang, M. Chiang, D. Dao, W. Su, S. Xu, H. Zhou, V2v data offloading for cellular network based on the software defined network (sdn) inside mobile edge computing (mec) architecture, IEEE Access 6 (2018) 17741–17755.
[95] H. Zhang, P. Dong, W. Quan, B. Hu, Promoting efficient communications for high-speed railway using smart collaborative networking, IEEE Wirel. Commun. 22 (6) (2015) 92–97.
[96] P. Pawelczak, R.V. Prasad, Liang Xia, I.G.M.M. Niemegeers, Cognitive radio emergency networks - requirements and design, in: First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005., 2005, pp. 601–606.
[97] I. Radhakrishnan, R. Souay, M.R. Palattellaz, T. Engel, An efficient service channel allocation scheme in sdn-enabled vanets, in: 2017 16th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net), 2017, pp. 1–7.
[98] M.A. Salahuddin, A. Al-Fuqaha, M. Guizani, Software-defined networking for rsu clouds in support of the internet of vehicles, IEEE Internet Things J. 2 (2) (2015) 133–144.
[99] Y. Liu, C. Chen, S. Chakraborty, A software defined network architecture for geobroadcast in vanets, in: 2015 IEEE International Conference on Communications (ICC), 2015, pp. 6559–6564.
[100] A. Di Maio, M.R. Palattella, R. Soua, L. Lamorte, X. Vilajosana, J. Alonso-Zarate, T. Engel, Enabling sdn in vanets: what is the impact on security? Sensors 16 (12) (2016).
[101] J. Bhatia, R. Dave, H. Bhayani, S. Tanwar, A. Nayyar, Sdn-based real-time urban traffic analysis in vanet environment, Comput. Commun. 149 (2020) 162–175, doi:10.1016/j.comcom.2019.10.011.
[102] M.S. Rayeni, A. Hafid, Routing in heterogeneous vehicular networks using an adapted software defined networking approach, in: 2018 Fifth International Conference on Software Defined Systems (SDS), 2018, pp. 25–31.
[103] C.-C. Lin, H.-H. Chin, W.-B. Chen, Balancing latency and cost in software-defined vehicular networks using genetic algorithm, J. Netw. Comput. Appl. 116 (2018) 35–41, doi:10.1016/j.jnca.2018.05.002.
[104] H. Khelifi, S. Luo, B. Nour, S.C. Shah, Security and privacy issues in vehicular named data networks: an overview, Mob. Inf. Syst. 2018 (2018) 5672154:1–5672154:11.

[105] A. Akhunzada, M.K. Khan, Toward secure software defined vehicular networks: Taxonomy, requirements, and open issues, IEEE Commun. Mag. 55 (7) (2017) 110–118.
[106] K.S.K. Liyanage, M. Ma, P.H.J. Chong, Controller placement optimization in hierarchical distributed software defined vehicular networks, Comput. Netw. 135 (2018) 226–239, doi:10.1016/j.comnet.2018.02.022.
[107] G. Wang, Y. Zhao, J. Huang, W. Wang, The controller placement problem in software defined networking: a survey, IEEE Network 31 (5) (2017) 21–27.
[108] H. Wang, L. Xu, G. Gu, Floodguard: a dos attack prevention extension in software-defined networks, in: 2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, 2015, pp. 239–250.
[109] M. Ambrosin, M. Conti, F. De Gaspari, R. Poovendran, Lineswitch: tackling control plane saturation attacks in software-defined networking, IEEE/ACM Trans. Netw. 25 (2) (2017) 1206–1219.
[110] S. Hong, L. Xu, H. Wang, G. Gu, Poisoning network visibility in software-defined networks: new attacks and countermeasures, in: IEEE NDSS 2015, 2015, pp. 1–9.
[111] M. Dhawan, R. Poddar, K. Mahajan, V. Mann, Sphinx: detecting security attacks in software-defined networks, IEEE Network and Distributed System Security Symposium (NDSS), 2015.
[112] N.M. Tran, P.H. Phong, T.D. Khoa, T.T. Huong, N.P. Ngoc, V.D. Loi, Self-organizing map-based approaches in ddos flooding detection using sdn, in: 2018 International Conference on Information Networking (ICOIN), 2018.
[113] H. Wang, L. Xu, G. Gu, Floodguard: a dos attack prevention extension in software-defined networks, in: 2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, 2015, pp. 239–250.
[114] P. Porras, S. Shin, V. Yegneswaran, M. Fong, M. Tyson, G. Gu, A security enforcement kernel for openflow networks, HotSDN, 2012.
[115] Z. Li, C. Chigan, D. Wong, Awf-na: a complete solution for tampered packet detection in vanets, in: IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference, 2008, pp. 1–6.
[116] X. Lin, X. Sun, P. Ho, X. Shen, Gsis: a secure and privacy-preserving protocol for vehicular communications, IEEE Trans. Veh. Technol. 56 (6) (2007) 3442–3456.
[117] C. Zhang, R. Lu, P. Ho, A. Chen, A location privacy preserving authentication scheme in vehicular networks, in: 2008 IEEE Wireless Communications and Networking Conference, 2008, pp. 2543–2548.
[118] T. Leinmüller, C. Maihöfer, E. Schoch, F. Kargl, Improved security in geographic ad hoc routing through autonomous position verification, in: Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks, in: VANET '06, 2006, pp. 57–66.
[119] S. Capkun, J. Hubaux, Secure positioning in wireless networks, IEEE J. Sel. Areas Commun. 24 (2) (2006) 221–232.
[120] J. Francois, O. Festor, Anomaly traceback using software defined networking, in: 2014 IEEE International Workshop on Information Forensics and Security (WIFS), 2014, pp. 203–208.
[121] S. Shin, P. Porras, V. Yegneswaran, M. Fong, G. Gu, M. Tyson, Fresco: modular composable security services for software-defined networks, IEEE Network and Distributed System Security Symposium (NDSS), 2013.
[122] Q. Wang, S. Sawhney, Vecure: a practical security framework to protect the can bus of vehicles, in: 2014 International Conference on the Internet of Things (IOT), 2014, pp. 13–18.
[123] B. Yu, C.-Z. Xu, B. Xiao, Detecting sybil attacks in vanets, J. Parallel Distrib. Comput. 73 (6) (2013) 746–756.
[124] B. Xiao, B. Yu, C. Gao, Detection and localization of sybil nodes in vanets, in: Proceedings of the 2006 Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks, in: DIWANS '06, 2006, pp. 1–8.
[125] T. Zhou, R.R. Choudhury, P. Ning, K. Chakrabarty, P2dap sybil attacks detection in vehicular ad hoc networks, IEEE J. Sel. Areas Commun. 29 (3) (2011) 582–594.
[126] L. Wei, C. Fung, Flowranger: a request prioritizing algorithm for controller dos attacks in software defined networks, in: 2015 IEEE International Conference on Communications (ICC), 2015, pp. 5254–5259.
[127] G. Shang, P. Zhe, X. Bin, H. Aiqun, R. Kui, Flooddefender: protecting data and control plane resources under sdn-aimed dos attacks, in: IEEE INFOCOM 2017 - IEEE Conference on Computer Communications, 2017, pp. 1–9.
[128] S. Khan, A. Gani, A.W.A. Wahab, M. Guizani, M.K. Khan, Topology discovery in software defined networks: threats, taxonomy, and state-of-the-art, IEEE Commun. Surv. Tutor. 19 (1) (2017) 303–324.
[129] R. Skowyra, L. Xu, G. Gu, V. Dedhia, T. Hobson, H. Okhravi, J. Landry, Effective topology tampering attacks and defenses in software-defined networks, in: 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2018, pp. 374–385.
[130] Q. Yan, F.R. Yu, Distributed denial of service attacks in software-defined networking with cloud computing, IEEE Commun. Mag. 53 (4) (2015) 52–59.
[131] D. He, S. Zeadally, B. Xu, X. Huang, An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks, IEEE Trans. Inf. Forensics Secur. 10 (12) (2015) 2681–2691.
[132] D. He, S. Zeadally, B. Xu, X. Huang, An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks, IEEE Trans. Inf. ForensicsSecur. 10 (12) (2015) 2681–2691.
[133] N. Abu-Ghazaleh, K.-D. Kang, K. Liu, Towards resilient geographic routing in wsns, in: Proceedings of the 1st ACM International Workshop on Quality of Service &Amp; Security in Wireless and Mobile Networks, in: Q2SWinet '05, 2005, pp. 71–78.
[134] S. Han, D. Ban, W. Park, M. Gerla, Localization of sybil nodes with electro-acoustic positioning in vanets, in: GLOBECOM 2017 - 2017 IEEE Global Communications Conference, 2017, pp. 1–6.
[135] H. Alipour, Y.B. Al-Nashif, P. Satam, S. Hariri, Wireless anomaly detection based on ieee 802.11 behavior analysis, IEEE Trans. Inf. ForensicsSecur. 10 (10) (2015) 2158–2170.
[136] B. Xiao, B. Yu, C. Gao, Detection and localization of sybil nodes in vanets, in: Proceedings of the 2006 Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks, in: DIWANS '06, 2006, pp. 1–8.
[137] C. Chen, X. Wang, W. Han, B. Zang, A robust detection of the sybil attack in urban vanets, in: 2009 29th IEEE International Conference on Distributed Computing Systems Workshops, 2009, pp. 270–276.
[138] J. Grover, M.S. Gaur, V. Laxmi, N.K. Prajapati, A sybil attack detection approach using neighboring vehicles in vanet, in: Proceedings of the 4th International Conference on Security of Information and Networks, in: SIN '11, 2011, pp. 151–158.
[139] H. Shafiei, A. Khonsari, H. Derakhshi, P. Mousavi, Detection and mitigation of sinkhole attacks in wireless sensor networks, Journal of Computer and System Sciences 80 (3) (2014) 644–653. Special Issue on Wireless Network Intrusion
[140] T. Das, V. Sridharan, M. Gurusamy, A survey on controller placement in sdn, IEEE Communications Surveys Tutorials (2019), doi:10.1109/COMST.2019.2935453. 1–1
[141] C. Campolo, A. Molinaro, A. Iera, R.R. Fontes, C.E. Rothenberg, Towards 5g network slicing for the v2x ecosystem, in: 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft), 2018, pp. 400–405.
[142] C. Campolo, A. Molinaro, A. Iera, F. Menichella, 5g network slicing for vehicle-to-everything services, IEEE Wirel. Commun. 24 (6) (2017) 38–45.
[143] H. Khan, P. Luoto, M. Bennis, M. Latva-aho, On the application of network slicing for 5g-v2x, in: European Wireless 2018; 24th European Wireless Conference, 2018, pp. 1–6.
[144] C. Campolo, A. Molinaro, A. Iera, R.R. Fontes, C.E. Rothenberg, Towards 5g network slicing for the v2x ecosystem, in: 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft), 2018.
[145] P. Rost, C. Mannweiler, D.S. Michalopoulos, C. Sartori, V. Sciancalepore, N. Sastry, O. Holland, S. Tayade, B. Han, D. Bega, D. Aziz, H. Bakker, Network slicing to enable scalability and flexibility in 5g mobile networks, IEEE Commun. Mag. 55 (5) (2017) 72–79.
[146] H. Zhang, N. Liu, X. Chu, K. Long, A. Aghvami, V.C.M. Leung, Network slicing based 5g and future mobile networks: Mobility, resource management, and challenges, IEEE Commun. Mag. 55 (8) (2017) 138–145.
[147] M.F. Bari, S.R. Chowdhury, R. Ahmed, R. Boutaba, On orchestrating virtual network functions, in: 2015 11th International Conference on Network and Service Management (CNSM), 2015, pp. 50–56.
[148] G. Sun, Y. Li, D. Liao, V. Chang, Service function chain orchestration across multiple domains: A full mesh aggregation approach, IEEE Trans. Netw. Serv. Manag. 15 (3) (2018) 1175–1191.
[149] S. Lal, T. Taleb, A. Dutta, Nfv: Security threats and best practices, IEEE Commun. Mag. 55 (8) (2017) 211–217.
[150] G. Siracusano, S. Salsano, P. Ventre, A. Detti, O. Rashed, N. Blefari-Melazzi, A framework for experimenting icn over sdn solutions using physical and virtual testbeds, Comput. Netw. 134 (2018) 245–259, doi:10.1016/j.comnet.2018.01.026.
[151] M. Sardara, J. Samain, J. Augé, G. Carofiglio, Application-specific policy-driven 5g transport with hybrid icn, in: 2019 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN), 2019, pp. 1–2.
[152] E. Kalogeiton, T. Braun, Infrastructure-assisted communication for ndn-vanets, in: 2018 IEEE 19th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), 2018, pp. 1–10.
[153] C. Xu, W. Quan, H. Zhang, L.A. Grieco, GrIMS: green information-centric multimedia streaming framework in vehicular ad hoc networks, IEEE Trans. Circuits Syst. Video Technol. 28 (2) (2018) 483–498.
[154] D. Grewe, M. Wagner, H. Frey, A domain-specific comparison of information–centric networking architectures for connected vehicles, IEEE Commun. Surv. Tutor. 20 (3) (2018) 2372–2388.
[155] D. Grewe, M. Wagner, H. Frey, Perceive: Proactive caching in icn-based vanets, in: 2016 IEEE Vehicular Networking Conference (VNC), 2016, pp. 1–8.
[156] E. Kalogeiton, T. Kolonko, T. Braun, A multihop and multipath routing protocol using ndn for vanets, in: 2017 16th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net), 2017, pp. 1–8.
[157] R. Hussain, S.H. Bouk, N. Javaid, A.M. Khan, J. Lee, Realization of vanet-based cloud services through named data networking, IEEE Commun. Mag. 56 (8) (2018) 168–175.
[158] E. Kalogeiton, Z. Zhao, T. Braun, Is sdn the solution for ndn-vanets? in: 2017 16th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net), 2017, pp. 1–6.
[159] M.A. Khan, X.T. Dang, T. Dörsch, S. Peters, Mobility management approaches for sdn-enabled mobile networks, Ann. Telecommun. 73 (11) (2018) 719–731.
[160] M. Conti, M. Hassan, C. Lal, Blockauth: blockchain based distributed producer authentication in icn, Comput. Netw. 164 (2019) 106888, doi:10.1016/j.comnet.2019.106888.
[161] S. Signorello, M.R. Palattella, L.A. Grieco, Security challenges in future ndn-enabled vanets, in: 2016 IEEE Trustcom/BigDataSE/ISPA, 2016, pp. 1771–1775.
[162] R. Tourani, S. Misra, T. Mick, G. Panwar, Security, privacy, and access control in information-centric networking: A survey, IEEE Commun. Surv. Tutor. 20 (1) (2018) 566–600.

Wafa Ben Jaballah is currently working as a research associate in Thales, France. Before that she was a Post-Doc Researcher at Orange Labs, Paris, France. In 2014, she received her Ph.D. degree from the University of Bordeaux. She was a Post-Doc Researcher at the University of Bordeaux, France in 2014. In 2013, she was an Assistant Researcher at the Institut Polytechnique de Bordeaux. Her main research interest is in the area of network security and web security. She has been a Visiting Researcher at the University of Padua (2012, 2013, 2014, and 2015).

Mauro Conti received the Ph.D. degree from the Sapienza University of Rome, Italy, in 2009. He was a Post-Doctoral Researcher with Vrije Universiteit Amsterdam, The Netherlands. In 2011, he joined the University of Padua, Italy, as an Assistant Professor, where he became an Associate Professor in 2015, and a Full Professor in 2018. He was a Visiting Researcher with GMU in 2008 and 2016, UCLA in 2010, UCI in 2012-2014 and 2017, TU Darmstadt in 2013, UF in 2015, and FIU in 2015 and 2016. His research is also funded by companies, including Cisco and Intel. His main research interest is in the area of security and privacy. He has published over 200 papers in topmost international peer-reviewed journals and conference. He was a recipient of the Marie Curie Fellowship by the European Commission in 2012 and the German DAAD in 2013. He is an Associate Editor for several journals, including the IEEE COMMUNICATIONS SURVEYS & TUTORIALS, the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, and the IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT. He was the Program Chair for TRUST 2015, ICISS 2016, and WiSec 2017, and the General Chair for SecureComm 2012 and ACM SACMAT 2013.

Chhagan Lal is currently working as a Research Associate in Department of Mathematics, University of Padua, Italy. He is also affiliate as Associate Professor at Manipal University Jaipur, India. He obtained his Masters degree (M.Tech) in Information Technology with specialization in Wireless communication from Indian Institute of Information Technology, Allahabad in 2009, and Ph.D. in Computer Science and Engineering from Malaviya National Institute of Technology, Jaipur, India in 2014. He has been awarded Canadian Commonwealth scholarship in 2012 under Canadian Commonwealth Scholarship Program to work in University of Saskatchewan in Saskatoon, Saskatchewan, Canada. He has published more than 35 research papers in peer-reviewed Conferences and Journals. His current research areas include Blockchain Analysis, Security in Wireless networks, Software-defined networking, Underwater acoustic networks, and context based security solutions for Internet of Things (IoT) networks.