Vehicular Communications 27 (2021) 100284

Contents lists available at ScienceDirect

Vehicular Communications

www.elsevier.com/locate/vehcom

Security of SDN-based vehicular ad hoc networks: State-of-the-art and challenges

Rukhsar Sultana, Jyoti Grover *, Meenakshi Tripathi

Department of Computer Science and Engineering, Malaviya National Institute of Technology Jaipur, India

ARTICLE INFO

Article history:
Received 15 April 2020
Received in revised form 22 July 2020
Accepted 8 August 2020
Available online 17 August 2020

Keywords:
Software defined networking
VANET
Security
ITS
SDN based VANET
Attacks

ABSTRACT

Development of Software Defined Networking (SDN) based Vehicular Ad Hoc Networks (VANETs) is one of the key enablers of 5G technology. VANETs enable different types of services through communication between vehicles and road side units. Intelligent Transportation System (ITS) introduced this emerging technology to provide travelers comfort, safety, and infotainment services with improved traffic efficiency. Traditional VANET is not sufficient to handle dynamic and large scale networks with their fixed and embedded policies, and complex architecture. Open Network Foundation (ONF) is promoting the adoption of SDN through open standards' development by facilitating logical and centralized control of the entire network. SDN enables VANET to be a flexible and programmable network with the advent of new services and features. A centralized controller in the control plane controls the overall network functionalities and forwarding of data packets through the forwarding devices in the data plane. SDN enhances the efficiency of VANET and provides security benefits to VANET. But, it causes new security problems also with the integration of new technologies and architectural components in the network. This article provides a comprehensive review of VANET, SDN, and SDN based VANETs based on their architectural and implementation details. Then it explains the effect of SDN on the security of VANET when it is integrated with traditional VANET. This paper encompasses a comprehensive review of proposed approaches providing security solutions for SDN based VANETs and outlines emerging research issues as future directions. To the best of our knowledge, this is the first article presenting the comprehensive review of security aspects of SDN based VANET considering architectural and security services on different layers of a network.

1. Introduction

With the increased number of vehicles on roads, the number of accidents and causalities is also increasing. This has been recognized as one of the serious problems confronted by modern society. Vehicular Ad Hoc Network (VANET) [1] is an emerging networking paradigm by Intelligent Transportation System (ITS) for communication. Vehicles disseminate safety and non-safety information regarding events by using Dedicated Short Range Communication (DSRC) [2] between moving vehicles, and between vehicles and infrastructure.

In VANET, the connection established between moving vehicles is transient. It is unrealistic to impose fixed policies in VANET because of its inherent characteristics, such as huge network size, dynamic topology, and many more. VANET characteristics also generate challenging issues for the regular functioning of VANET. High mobility reduces the connection time and routes between moving vehicles and leads to dynamic and intermittent connectivity [3]. Traditional VANET works on the fixed policies implemented in vehicular components to monitor and control traffic density and routing paths. Vehicular networking is obstructed by frequent disconnections, heterogeneous interfaces, flexibility, scalability, and reliability issues [4]. As a consequence of these problems, routing of data packets related to various VANET applications is also affected [5]. High mobility causes packet collision and also affects network performance and cooperation among vehicles. [6–8] address the challenging issues of VANET and provide solutions for enhancing network performance as packet delivery ratio, end-to-end delay, and QoS. Research work proposed in [9,10] addresses high node density, scalability, routing, and security challenges.

VANET lacks innovation in networking due to tightly coupled hardware but SDN works in favour of innovation in network design and operations. That's why SDN appears as a future networking solution for both wired and wireless networks. In recent researches, SDN networking paradigm was implemented in wireless networks

* Corresponding author.
E-mail addresses: 2019rcp9045@mnit.ac.in (R. Sultana), jgrover.cse@mnit.ac.in (J. Grover), mtripathi.cse@mnit.ac.in (M. Tripathi).

https://doi.org/10.1016/j.vehcom.2020.100284
2214-2096/

Table 1
Overview of various surveys on security in SDN based VANET.

Research paper	Year	Overview
Enabling SDN in VANETs: What is the Impact on Security? [15]	2016	Gives an explanation of SDN based VANET and describes SDN based solutions for threats in VANET applications
Toward Secure Software Defined Vehicular Networks: Taxonomy, Requirements, and Open Issues [16]	2017	Provides a fundamentals background of software-defined vehicular network architecture and presents security vulnerabilities, attacks, and challenges of each layer
Services and Security Threats in SDN Based VANETs: A Survey [17]	2018	Presents SDN based VANET overview, services, security threat vector and challenges regarding SDN based VANET
Security and Design Requirements for Software-Defined VANETs [18]	2020	Presents a general architecture design and solutions for performance enhancement of SDN based VANET and discuss threat vector with their solutions in SDN based VANET
Proposed Survey		In addition to a description of SDN based VANET and novel classification of security attacks, we have classified the role of SDN on the security of SDN based VANET, i.e. SDN as a solution to security issues of VANET and SDN as a challenge for SDN based VANET

including ad hoc networks, which is able to simplify the network control and enable flexible and programmable network architecture [11]. Software-defined wireless network is a favorable choice for vehicular application implementation and handling related issues with less complexity and cost. Open Networking Foundation (ONF) introduced SDN technology which consists of a centralized controller [12]. SDN enables the separation of the control plane from the forwarding plane through its three-layer architecture.

SDN introduces several advantages over the traditional network environment [13]. Applying SDN paradigm in VANET overcome all the challenges in VANET and make the network management efficient and the environment highly adaptive. SDN based VANET has separated data plane and control plane along with a logically centralized control which are the key requirements for today's dynamic, scalable, and next-generation VANET environment [14].

SDN based VANET provides various benefits. But, the centralized controller is a single point of failure and an easy target for attackers. Security attacks on VANET can prevent users to adapt new paradigm up to its full potential due to their privacy and safety concerns. If the controller is compromised, it can lead to severe result as traffic congestion, road accidents, and network failure. Thus, SDN based VANET is twofold by nature: It can introduce new vulnerabilities in VANET while simultaneously, it enables security providing solutions in VANET [15]. To detect and mitigate security threats in SDN based VANET, new security approaches are also proposed. These approaches can enhance network performance and deliver security benefits to the network.

1.1. Key contributions

There are some existing research articles, which present a survey on SDN based VANET security. Table 1 shows an overview of existing researches and our work. Most of the researchers have given a classification of attacks in SDN and SDN based VANET, based on the planes where they occur and covered the security benefits of SDN. Major contributions of our work are given as follows:

- Mainly, our work is intended to present a detailed study of SDN based VANET and describe how security is affected on the inclusion of SDN into VANET. Firstly, we discuss VANET and SDN, along with their architectures, communication standards, characteristics, applications, and existing challenges. We have also presented the state of the art SDN based VANET related to their architecture, operation modes, applications particularly safety applications, services, and use cases in smart cities, together with occurring key challenges.
- SDN has some vulnerabilities [15,19], which are inherited from its characteristics and architecture. Therefore, new security threats can occur with SDN implementation in a network. Based on this fact, for security analysis of SDN based VANET, we classify the role of SDN in SDN based VANET into two categories. In the first role, SDN works as a solution to security issues of VANET and secondly, SDN can be a security challenge for SDN based VANET.
- We present a threat vector in VANET and consider the three principal characteristics of SDN for the categorization of attacks and their solutions possible through these characteristics. Next, we classify security threats in SDN based VANET based on SDN characteristics which can cause these threats. We also depict some novel security paradigms based on the learning process and proposed to detect and mitigate security attacks in SDN based VANET.

1.2. Organization

An outline of this paper is shown in Fig. 1. Next to the introduction, Section 2 presents an overview of VANET and SDN. It provides its architecture description along with characteristics, challenges, and applications. Section 3 explains SDN based VANET, operation modes, its use cases, where SDN is applied to offer advantages in real-time fields, and challenges occur on the integration of SDN into VANET. Section 4 discusses the impact of SDN features and SDN working on the security of SDN based VANET. It analyzes whether SDN is beneficial for VANET from the security point of view or not. This section also presents some novel security mechanisms in SDN based VANET. Section 5 discusses learning outcomes, which helps to understand the challenges of SDN and their impact on the security of VANET. It also presents open research issues based on our findings that can be possible future research directions. Finally, we conclude the paper in Section 6.

2. Overview of VANET and SDN paradigm

This section presents a brief overview of VANET and SDN background. Along with the VANET architecture description, Subsection 2.1 covers characteristics, applications, and challenges in real-time implementation of VANET. It also describes various aspects of security in VANET. Subsection 2.2 outlines the components of SDN architecture, challenges in SDN implementation, SDN services, and applications.

2.1. Vehicular ad hoc networks

ITS introduced VANET as a solution to the incurred problems of traffic congestion and to provide road safety and comfort to

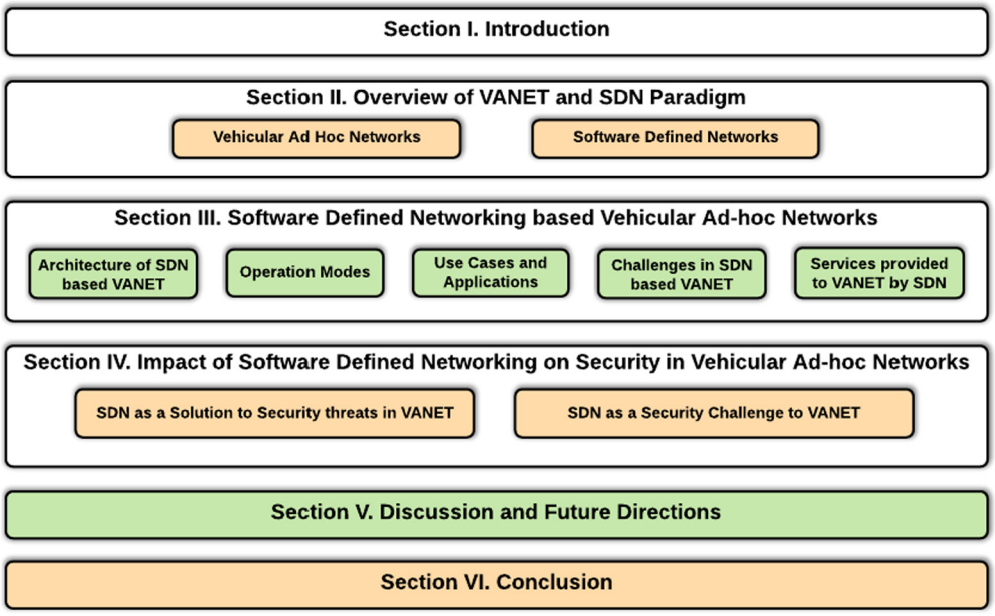

Fig. 1. Structural organization of the paper.

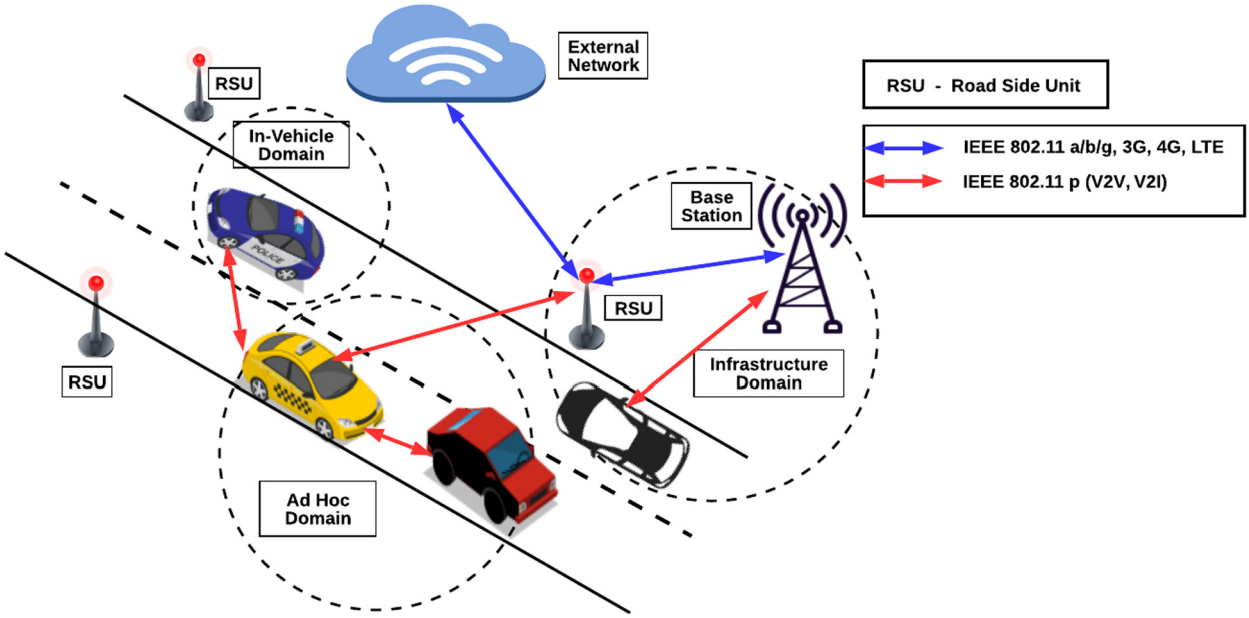

Fig. 2. VANET components and communication.

drivers [3]. In VANET, vehicles can communicate with each other and stationary road side components using incorporated wireless technologies [5]. ANSI/IEEE 1471-2000 [20,21] and ISO/IEC 42010 [22] gives definition and guidelines for conceptual framework of a system architecture [23]. Mainly, vehicular network architecture has three components which are smart vehicles, Road Side Units (RSUs) and vehicular communication [24] as shown in Fig. 2.

Smart vehicles are installed with sensors, event recorders, wireless computation, and communication devices [3,24]. From the security concern, smart vehicles should be installed with Electronic Chassis Number (ECN) or with Electronic License Plate (ELP) in place of conventional license plates that can electronically identify the vehicles [25]. Smart vehicles are embedded with On Board Units (OBUs) [1]. OBU is a portable wireless device mounted on board in a smart vehicle. It contributes to information exchange and provides short-range communication with other OBUs and RSUs, based on IEEE 802.11p [26] radio technology. OBU also enables communication services in the Application Unit (AU). On behalf of other OBUs, it forwards the data in the ad hoc domain [27]. The communication in OBU is provided by using RSU, and in absence of RSU, OBU makes use of other cellular radio networks. These are General Packet Radio Service (GPRS) [28], Global System for Mobile Communications (GSM) [29], Worldwide Interoperability for Microwave Access (WiMAX) [30], Universal Mobile Telecommunications Service (UMTS) [31] and 4G [5]. RSUs are stationary wireless access devices mounted along the road side, junction, or near the parking spaces. They comprise one or more network devices for dedicated short-range communication based on IEEE 802.11p radio networks [5]. RSU provides communication and extends the communication range in the ad hoc network by forwarding information to other OBUs via itself. RSU also generates

alerts for accidents, crashes, and warnings by using the vehicle to infrastructure communication.

Communication between vehicles, and RSU and infrastructural units in VANET takes place mainly in three types of domains as shown in Fig. 2. The in-vehicle domain consists of OBU and one or multiple AUs. To exploit the application provided by the application provider, AU is assigned with the communication capabilities by the OBU [1]. Here communication occurs to detect the driver's sleepiness and performance of vehicles for safety purposes [5]. In the ad hoc domain, two types of communications are possible as Vehicle-to-Vehicle (V2V) communication and Vehicle-to-Road (V2R) or Vehicle-to-Infrastructure (V2I) [3]. Among these communications, V2I links are not much vulnerable to attacks [24]. The infrastructure domain enables vehicles to connect with external Internet infrastructure, trusted third parties, and service providers by using RSU. It also enables advanced vehicle tracking and active traffic assistance.

In VANET environment, there is a variety of communication standards including cellular technologies, IEEE 802.11 a/b/g/n, DSRC [2], Wireless Access in Vehicular Environment (WAVE) and some combined technologies as CAR-2-CAR Communication Consortium (C2C-CC) [32], Continuous Air Interface for Long to Medium range (CALM) [33] etc. DSRC is widely used for V2V and V2I communication and it is an acceptable and efficient technology for vehicular safety applications [3]. DSRC/WAVE or IEEE 802.11p WAVE is improved version of DSRC with IEEE 802.11a and 802.11p [34,35]. There are different kinds of standards in the WAVE IEEE 1609 family which enable communication, resource management, and networking services in VANET [36].

VANET environment exhibits various kinds of characteristics related to the wireless medium, communication, network topology, and different nodes in VANET [3,37]. High mobility is one of the major characteristics and challenges of VANET. It leads to dynamic network topology, while the links between nodes connect and disconnect very often. In a high mobile VANET environment, to design an efficient and secure routing protocol is also a major challenge that can provide better packet forwarding in less time and with a fewer number of packets drops. Therefore, the communication and implementation of security applications should be as fast as possible in order to improve the throughput and reliability of VANET.

Besides the mobility challenge, there are many challenging factors that cause difficulties in the achievement of VANET objectives [5,34]. Secure data transmission, assurance of protection of vehicles and their identity, and authentication of data and communicating entities are the major requirements of security applications in VANET. It is a crucial challenge to deploy security applications in VANET scenario having frequent disconnections, high density, and mobility. However, a number of mechanisms were proposed which address the major security challenges in VANET. Such as [38–40] provide solutions as intrusion detection and malicious node detection for VANET.

In VANET scenario, V2V, and V2I communications allow deploying VANET services in various kinds of applications [41,24,34]. Major applications include safety applications, such as collision avoidance, road condition, and accident alert, weather condition alert etc. Driving assistance applications comprise traffic navigation and assistance, parking availability etc. As well as entertainment applications, uninterrupted Internet access, location, and map tracking are also provided.

In order to exhibit VANET services, researchers have proposed various applications [42]. One application is emergency alert brake light [43] designed to alert drivers for sudden brake performed by the preceding vehicles. SPARK [44], a new parking system, PASS [45], a parking-lot-assisted car-pooling method, an automatic toll collection system [46], long-term secure health care scheme known as RCare [47], Geographical Routing for Mobile Tourist (GRMT) [48] and an authentication scheme based on light-weight RFID (Radio Frequency Identification) [49] for health care are some examples of VANET applications.

Before deploying any VANET application, its various security aspects need to be considered. Secure data transmission, user privacy, and protecting network from misbehaving entities are the challenging issues in vehicular networks. Security threats in VANET and their solutions are elaborated in more detail in subsection 4.1.1 and in Table 4. Being a major research field, a number of novel security schemes were proposed for the detection of major attacks, Sybil attack detection, intrusion detection, and misbehavior detection. Author in [50] proposed a lightweight Sybil attack detection mechanism based on calculated RSS (Received Signal Strength) value for each received beacon from the vehicle node. One more mechanism was proposed in [51] for Sybil attack detection. This mechanism uses the difference in the movement pattern of a legitimate node and Sybil node, and various parameters for more accurate Sybil attack detection. [52] proposes a security protocol for anonymity and privacy in VANET based on the dynamic change of pseudonyms. Authors in [53] give an in-vehicle intrusion detection system using the deep convolutional neural network which has better performance as compared to conventional machine learning algorithms. [54] designs a context-awareness trust management model to evaluate received message trustworthiness and gives an accurate evaluation result using reinforcement learning. A misbehavior detection framework was presented in [55] that allows us to develop, test, and compare the misbehavior detection algorithm. Thus, there are various VANET security approaches developed in recent years.

2.2. Software defined networks

Software-Defined Networks [56] introduced nearly in 2006 has three-layered architecture comprising infrastructure, control, and application layers. It decouples the control plane from the forwarding plane in a network. It provides logically centralized control over the networks in place of integrated control and hardware in the same equipment. SDN enables the interaction between control and forwarding plane using OpenFlow protocol [57,58]. SDN allows network programmers to create new services with flexibility and to add them with just installing a new application [59]. SDN differs from traditional networking paradigms in various factors [60,61] as explained in Table 2.

As shown in Fig. 3, there are three layers in SDN architecture. The upper two layers together are called the control plane and the lower layer is called the forwarding plane or data plane [62]. The working process of the individual layer can be described as follows:

- **Data plane**: Data plane comprises data forwarding devices that forward the data packets according to received forwarding decisions and instructions from SDN controller [59]. OpenFlow is an open communication standard to provide a secure communication channel between controller and switch. Flow instructions and messages related to network changes and communication formats are transmitted through this secure channel [56]. The SDN controller is named as OpenFlow controller and switches are called OpenFlow enabled switches. The communication between controller and switches is provided using Out-of-Band and In-Band methods. For the communication, an optimized path is computed through some algorithms, and switches are selected according to optimized path [63]. The switches are not fixed for a particular communication. If link failure occurs during the communication, then other switches are selected which can provide an optimized communication path.

Table 2
Difference between SDN and other conventional networks.

Factor	SDN	Conventional networks
Features	Control-data plane separation, programmability	Complex network control and a new protocol required for each problem
Configuration	Automated configuration with centralized validation	Error manual configuration
Performance	Dynamic global control with cross layer information	Relatively static configuration and limited information
Innovation	Easy implementation of software for innovation, sufficient test environment with isolation, rapid deployment using software upgrade	Difficult hardware implementation for innovation, limited testing environment, long standardization process

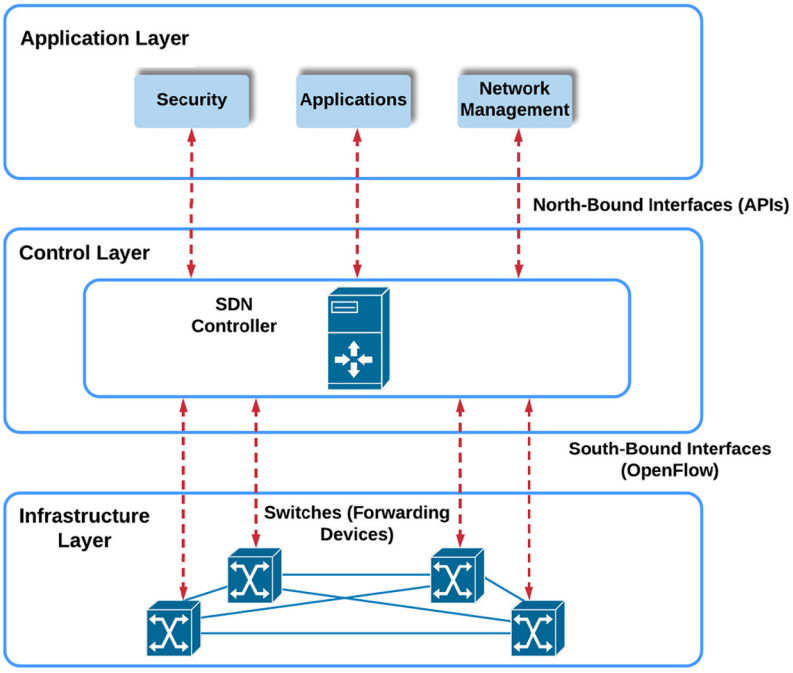

Fig. 3. Layered architecture of SDN.

Switches have flow tables consisting of flow rules. These rules are made up of different fields and installed through the controller. On arrival of a data packet, it is matched with the matching fields for the different flow rules in the flow table. If a match is found, the packet is processed according to the actions specified in the flow rule. Otherwise, a table miss occurs, and then the actions are taken according to the table miss flow entry in the flow table. The controller can insert the rules into the flow table in two ways as pro-actively and re-actively [59,14].

- **Control plane:** Control plane consists of a network controller that can install, manipulate, and remove the flow rules in accordance with running applications. It keeps the flow table updated according to changes in network topology and external service requests. It provides the services and programming interfaces required for the smooth execution of applications [59]. Whenever a table miss occurs in the data plane, the forwarding switch sends an encapsulated packet called "packet-in" to the controller. In response to this, the controller forwards the "flowmod" packet including forwarding instructions to switch [14]. There are different versions of the OpenFlow controller, such as NOX, POX, Beacon, IRIS, NodeFlow, Flowvisor, RouteFlow etc. [64].
- **Application plane:** Applications and network defining services, such as path reservation, network provisioning, and network topology discovery reside in this plane [56]. These applications use services of control plane and data plane. They can manipulate the network services using north-bound interfaces. SDN applications can be developed in two ways. First, that manage the network functionality, such as traffic engineering (TE), security, universal access control list (U-ACL) management, and QoS. The second type includes use cases that are developed to grant some specific services, such as network virtualization (NV), mobile networks, network function virtualization (NFV), and information content networking (ICN) [65].

SDN has some challenging factors [13], such as network scalability, latency, security, single control failure etc. If the network scale increases, the overhead on a single controller influences network performance. Large scale network has several more challenges, such as communication overhead, resource management, network security on increasing of applications in the network [66]. In the ad hoc networks, changes occur frequently. So the network should be flexible enough that can adapt the changes and do the actions according to predicted or unpredicted variations. To execute security and safety applications, the controller requires continuous observance of the network traffic, packet flow etc. And for observation, extra processing resources are required, making the traffic measurement task more crucial. To decrease the latency of a data packet is also challenging for SDN.

Security is the major concern in SDN. Because SDN OpenFlow interface allows integrating third-party applications in the network, which can have security vulnerabilities. The permissions to these types of applications should be constrained. SDN adminis-

trator should strictly prohibit the network and application access from unauthorized tenants by using authorization, authentication, and access control list [66]. Securing the data plane is also a critical aspect because a large amount of information may be exposed through the compromised forwarding devices [62].

There are a large number of solutions proposed that address the SDN challenges. These include hierarchical distributed SDN controller [67] that handles network scalability and [68] that handles flexibility. As well as a model for SDN flow authentication and validation was designed in [69]. Proposed work in [70] detects misbehaving controller and [71] performs detection of various misbehavior using machine learning. Thus, they address security challenges in SDN.

SDN characteristics can be exploited in various fields. There are a number of applications where SDN can be deployed [59,72]. SDN can provide dynamic and logically centralized control over the network together with fast failure recovery, QoS, and network protection. This can be applied in traffic engineering to design a network that optimizes the cost of deployment and maintain service continuity in the network when the traffic goes high. SDN can be used in VANET and other surveillance applications, which have better performance with the integrated SDN. With the global awareness of the network, it can handle the network in a better way. Some frameworks are proposed where the core mobile operator is offloaded by direct transmission of data between the communicating sites [73] without passing through the core network that decreases the overall latency. SDN supporting networks are provided with better security approaches. One of such techniques is OpenFlow Random Host Mutation (OFRHM) [74]. It hides network assets, such as authentic IP from the malicious scanner that tries to launch attacks by allocating a virtual IP to the host. Some OpenFlow controller obtains high-level security through the anomaly detection algorithms [72]. SDN techniques can be exploited to provide middlebox (example load balancer) and in-network services. In some middlebox applications, tags are assigned to outgoing packets to be used on switch for systematic policy enforcement.

Various research works were proposed those implement applications based on SDN. In [75], the author proposes a traffic control system in smart cities based on the integration of SDN and IoT. [76] presents recent works for improving the design of home area network using SDN or combination of SDN with slicing and network function virtualization. [77] gives SDN based fast failure detection and fault recovery mechanism for 5G core networks. [78] presents a software-defined cognitive routing for the internet of vehicles using reinforcement learning.

3. Software defined networking based vehicular ad hoc network

Due to the advantageous characteristics of SDN as flexibility, programmability, and logically centralized control, it can be acquired in various kinds of wireless access networks. These aspects of SDN can be convenient to VANET in order to overcome the challenges and issues in VANET environment [4]. SDN architecture can be implemented in VANET in diverse ways. SDN enables separation of control from the underlying infrastructure. The controller provides network intelligence, programmability with a highly adaptive and scalable environment [60]. By adding programmability to external applications into VANET, SDN brings new capabilities into the vehicular environment and improves network efficiency. SDN based VANET provides independent deployment of processing entities, control, and traffic forwarding. It allows for efficient and dynamic resource allocation, network management, and inclusion of new services through programmability. It allows for adapting changes in dynamic network topology by using different operational modes.

3.1. Architecture of SDN based VANET

SDN can be integrated efficiently with VANET and for this integrated SDN based VANET, different architecture designs were proposed. A general layered architecture of SDN based VANET with communication is explained in Fig. 4. Architecture is divided into three planes as application, control, and data plane. Each plane comprises various components which can be described as follows:

1. **Data plane:** SDN based VANET has decoupled data plane from the control plane. The data plane consists of data forwarding devices of VANET, such as OBU equipped vehicles, OpenFlow enabled RSU, switches, and different network access components. These components can be narrated as follows:
   - **SDN wireless node:** In the case of VANET, vehicles are data plane elements. Vehicles are controlled through the control instructions given by SDN controller. Control messages are received through RSU or wireless access points. Vehicles perform actions accordingly and collect the data required for monitoring also [60,11]. Usually, the hardware of OBU is designed and implemented differently to support various capabilities and functions, such as packet forwarding, channel selection, transmission mode, interface, and power control. The internal components of an SDN wireless node are depicted in Fig. 5. The wireless node has all the properties as OpenFlow enabled switches to comprise. It uses the LTE communication standard for interaction through the control channel and uses Wi-Fi channels for data transmission. Data transmission is based on configuration and type of services. Each node has an SDN module, which takes input from the control plane. Each of the data packets, i.e. all network traffic is processed through SDN module before being forwarded ahead. SDN node acts like both a host and a router or a data forwarding element simultaneously. The node also comprises a local agent, which is able to perform functions based on features installed into the wireless node. It can work as a backup in case of connection loss with the central SDN controller or can provide intelligence to SDN module while receiving input from the controller. The local agent has active participation only when communication with the controller is lost. In that case, it provides some routing and fall-back mechanisms otherwise it shows minimal intelligence [14].
   - **SDN infrastructure components:** SDN infrastructure comprises RSU, network access points, and network devices, such as switches, routers etc. RSUs are stationary elements at the edge of the data plane. These are established along the road side or with cellular base station [79]. Infrastructure components provide wireless access to vehicles. Their behavior or functionalities are controlled by SDN controller. But, SDN controller cannot approach all the vehicles and RSUs. Therefore, 4G/LTE base stations are used to provide long-range connections for control plane communication and high bandwidth connections for data plane communication [14]. RSUs are also OpenFlow enabled and have a compatible interface with wireless, wired, and LTE communication standard. There are two types of approaches followed to provide communication which is V2V and V2I. Vehicles perform vehicle feature monitoring and then the collected data from the monitoring process are forwarded to the local controller. V2I communication occurs between vehicles, stationary RSU, and other infrastructure elements to forward the monitored data and extend the communication range. [18] proposed architecture for SDN based VANET in which OpenFlow enabled RSUs to work as RSU local controller for a

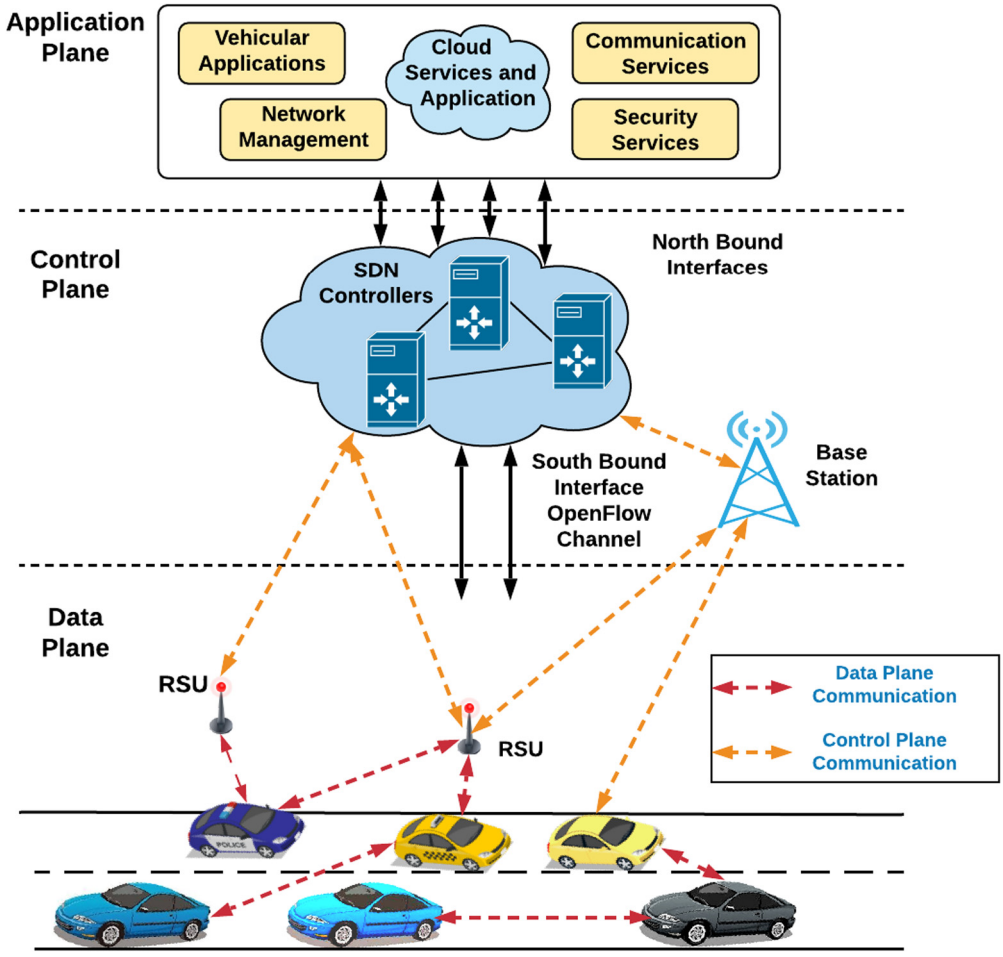

Fig. 4. Software defined networking based vehicular ad hoc network architecture.

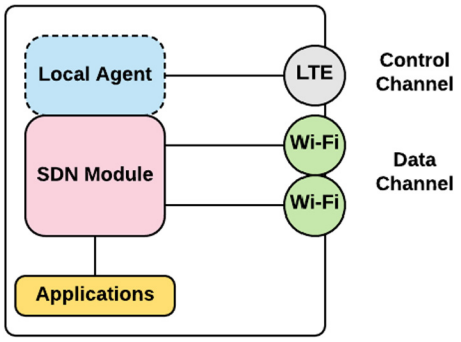

Fig. 5. SDN wireless node [14].

group of RSUs. RSU controllers gather information from their local area and then forward it to SDN controller.

- **SDN enabled switches:** In the data plane, a switch network exists where the switches follow the forwarding rules sent by SDN controller. The switches can forward the data packet on the specified path to the destination vehicle if a matching flow rule is found. Otherwise, the switch can send a request to the controller for providing the corresponding flow rule or it can drop the packet [79].

Thus, the data plane consists of various components and all of them have different functionalities and properties, which together provide data plane services.

2. **Control plane:** Control plane is the core part of SDN based VANET where all the controlling elements, such as SDN controller, protocols, network modules exist. This is an essential part, enabling the centralized view and logical control in VANET. The control plane also provides interfaces to communicate with other control plane elements.

- **SDN controller:** SDN controller is a software program that executes at the centralized and logical server of SDN based VANET. The controller is responsible for the performance of the whole network and it has a global view of the network. It collects information from the infrastructure plane to process the requirements of the application layer. It exploits SDN architecture and infrastructure to provide storage and computation potential. Flow rules construction, mobility management, resource allocation, and network function virtualization are the key functions of the SDN controller. Some more functions, such as data preprocessing and analysis are also performed by the controller. The functionalities of one controller can be distributed among the group of controllers in a hierarchy [79]. The controller can be placed in two types of control plane. First is a fixed control plane where the controller resides at a fixed place in the infrastructure. It can be situated at a centralized fixed server or a cloud server. The local controller also remains at RSU and base stations and is responsible for collecting the network data. Second is the mobile control plane where the controller does not reside at a fixed place. Here global controller is the central entity, which performs the complex operations and functions, and serves the requests for resource allocation, bandwidth allocation etc. Local controllers are equipped in

the vehicle itself which is active only when the vehicle is the cluster head of a group.

3. **Application plane:** As shown in Fig. 4, the application plane consists of various applications used in the network intended for providing specific services. Services include security, cloud computing, management, load balancing, recovery, monitoring, QoS, virtualization, communication, business-related applications, and vehicular applications like vehicle location prediction and suspicious network activity detection.

SDN enables the separation of control from the data plane and this feature makes VANET more dynamic. Data plane elements do not work according to predefined routing decisions as in traditional VANET. Therefore, their forwarding decisions depend on the flow of network traffic and kind of incoming packets. Decisions are taken by the centralized controller in accordance with present topology and traffic conditions.

3.2. Operation modes

SDN based VANET has decoupled data plane and control plane where the data plane works according to the control plane instructions. But the degree of control by SDN controller differs for the various operation modes. These operation modes are classified into three categories, which can be expressed as follows [14]:

1. **Centralized control mode:** In this mode, network performance and actions of underlying components, such as SDN wireless node, OpenFlow enabled switch, and RSU are controlled by SDN controller. Forwarding and all the networking decisions are determined by the centralized controller. SDN controller sends the flow rules to the data plane that defines how to treat a particular packet.
2. **Distributed control mode:** In this mode, SDN elements are not under the control of SDN controller. The local agent in SDN wireless nodes, i.e. vehicle remains active to determine the behavior of the nodes and make the forwarding decisions during packet delivery. This mode is somehow similar to a self-organizing network without SDN features.
3. **Hybrid mode:** This mode comprises both the operational modes. The centralized controller can control the network at different levels from zero levels to full control level. SDN controller does not hold all the control with it, but it consigns the packet processing to the local agent within SDN wireless node. Afterward, forwarding and control details are exchanged between all SDN elements. As in one situation, the SDN controller assigns the policies regarding flow rule generation to SDN wireless nodes and RSUs. According to those policies, the nodes construct flow rules and packet forwarding decisions using local intelligence.

As explained above, different operation modes of SDN based VANET can be deployed in the network environment according to network scenario.

3.3. Use cases and applications

ITS enables various applications in the vehicular environment in urban areas or smart cities. These applications related to communication and network resources are dynamic in nature. So infrastructure should be adaptable to the variation in requirements to serve various applications constantly. These applications range from safety, non-safety, and data dissemination to network virtualization applications [80]. Here different use cases are depicted as follows where SDN continuously cooperates with network infrastructure to satisfy the requirements of applications.

1. **Smart parking:** Smart parking system is a well-known application in smart cities. This application makes use of sensors and integrated devices to detect the parking space and to forward detected information to the central server. So that the server can disseminate the gathered and processed parking information to the citizens for utilization. For the transmission of information, multi-hop mesh networking could be used. But it becomes complex to use this technology for a wide-area network. Often in current systems, a low-power wide-area network approach is applied, which facilitates integration with cloud applications. If SDN controller is included in the infrastructure, the distribution of parking availability information can be achieved using V2V and V2I communication between peers. Using the floating content approach, information can be disseminated in a geographical area in a distributed fashion [15,81].
   In this application, devices are connected in IoT (Internet of Things) infrastructure. SDN enables the network to overcome the critical IoT issues, such as the arrangement of network resources, traffic congestion control, circumvent the network clash, and serve various kind of services concurrently with flexibility and scalability. Nokia proposed “Nuage Networks” [82] which is based on SDN framework and it is capable to provide Virtualized Cloud Services (VCS), Virtualized Security Services (VSS) and Software-Defined Wide Area Networking (SD-WAN) [4,11].
2. **Smart grid of electric vehicles:** Electric Vehicles (EV) are the future active elements, intended to improve energy efficiency and reducing emissions in the transport sector. According to the original concept of the smart grid, electric vehicles are utilized to distribute and produce energy from renewable sources by integrating information and power network. Electric vehicles are movable parts and power supply networks, i.e. Electric Vehicle Supply Equipment (EVSE) is a static part of the Electric Vehicle Infrastructure (EVI). Communication technologies, such as Wi-Fi, ZigBee, and Power Line communication used here are vulnerable to security threats as in the case of VANET. Applying SDN into the smart grid can be a beneficial idea, which can overcome the challenges and avail of a secure, reliable, and robust power system. An electric vehicle can be provided with the smart charging schedule under energy constraints and security enabled mechanisms [15].
3. **Platooning:** Platoon is a formation of driving vehicles that maintain an inter-vehicular distance and follow a leader vehicle. The leading vehicle is responsible to adjust the distance and maintain the stability of the platoon. It also forwards the information to followers in the platoon and other following vehicles. It exchanges information using V2V communication. Platoon decreases human involvement and can intensify the driving safety. Cooperative Adaptive Cruise Control (CACC) is a platooning application where radar technology is used to sense the neighboring vehicle’s position and speed. The chain made in platoon includes humans, vehicles, environments, such as infrastructure, traffic, and roads together with a leading vehicle. But there should be a central entity to choose the appropriate leader, which can arrange the platoon and decide the action profile based on dynamic conditions in a city. In smart city transportation, a central infrastructure unit RSUC is being used to instruct the vehicles in a data plane. Vehicles are instructed with the rules for a lane change, change in acceleration, merge and split according to real-time traffic conditions. This controller keeps the platooning secure and robust against various attacks as it supports the leader for the detection of jamming and replay attack [15].
4. **Emergency and safety services:** Emergency services in the smart cities, such as medical, fire safety, and police have vary-

ing requirements for communication and network resources. SDN controller can provide the resources in accordance with their requirement, type of information sent, and urgency of the service. Resources are provisioned on a priority basis also so that the emergency services can be executed primarily. SDN helps to distribute the emergency messages regarding the event occurred in VANET environment. It provides minimum resources pro-actively and increased scale of provisioning according to requirements. It can also mitigate the security attacks, such as Sinkhole attack and DDoS attack on emergency services by using trust approaches. In SDN enabled VANET, some frequency channels are reserved for emergency and other important services. It also provides road safety by using consistent V2V and V2I communication for transmission of road alert messages and safety messages [11].

As explained above, there are various cases, where SDN concept provides easiness and security to the applications. Apart from this, there are some other applications of SDN based VANET where the integration of SDN increases the capabilities of VANET. These applications [4] are explained as below:

1. **5G network implementation:** 5G networks require a reliable and flexible run of applications in VANET. SDN can fulfill the requirements of 5G networks, such as latency control, scalability, and dynamic provisioning with re-adjustment of data flow and routing of traffic. SDN can respond to dynamic latency requirements for real-time applications and topology. SDN ensures the availability of routing links, which have a low latency path and controlled jitter for real-time and safety-related applications. The consistent growth in data flow requires high bandwidth utilization. OpenFlow enabled SDN provides Bandwidth-on-Demand (BoD) services [4]. These services are cost-effective and allow users to resize the bandwidth usage dynamically as per their needs and pay only for their usage. SDN in the 5G network ensures the dynamic QoS and efficient data dissemination by providing low latency, flexibility, bandwidth requirement through DSRC of 75 MHz for the safety and non-safety applications.
2. **Wireless network virtualization:** SDN enables virtualization of large scale wired and wireless networks by dividing them into small, logical, and isolated networks. Different network elements can share network resources, infrastructure, and spectrum in an efficient manner. It also sanctions the virtualization of interfaces and forwarding devices among numerous users.
3. **Traffic control, road monitoring, and management:** The huge amount of traffic in the cities is continuously managed and controlled by SDN controller. For this, the controller keeps track of moving vehicles' information and provides communication with multi-hop routing simultaneously. SDN controller collects monitoring data from sensors related to road conditions, such as emergency and traffic congestion. Accordingly, the controller changes routing and forwarding decisions dynamically, and exchanges monitored data and flow rules with the vehicle in the data plane. Traffic accident detection techniques can also be applied as in [4] based on the monitored data, such as speed, acceleration, coordinates of vehicle etc. In this approach, the behavior of vehicles is analyzed based on the collected data set and using machine learning approaches, such as support vector machine, artificial neural network, and random forest [83]. SDN controller has a global view on the network, so it can suggest lane change assistance to vehicles on request by taking decisions based on gathered data from RSU.
4. **Miscellaneous applications:** SDN supports heterogeneity of network resources. Here different communication technologies and interfaces are exploited, such as DSRC, Wi-Fi, WiMAX to achieve efficient V2V and V2I communication. SDN also serves the network with efficient bandwidth, resource utilization, and QoS. Along with these, some more applications are provided by SDN based VANET.

   SDN environment makes available the surveillance data on-demand through an authorized requester like police for investigation purposes. On receiving a request, SDN creates flow rules for surveillance data to reach the requester.

   To provide infotainment services to vehicles, such as audio and video streaming, SDN uses the best path flow with the help of the shortest path algorithm over Multi Protocol Label Switching (MPLS) [4]. This gives the optimal solution for the issue of high mobility and delivers the QoS with improved performance.

   SDN can also enable interoperability between in-vehicle data sources. In a vehicle, heterogeneous data is generated by different Electronic Control Modules (ECUs). Therefore, interoperability between the ECUs is needed that allows different technologies to collaborate for achieving complex tasks in a vehicle. In [84], an SDN-based approach was proposed enabling in-vehicle data sources interoperability and allows ECUs to share a medium.

Fig. 6. Challenges in SDN based VANET.

SDN exploits its unique characteristics into VANET, to provide VANET services with improved performance. Thus, there are many applications, which provide services in a better way by using SDN paradigm.

3.4. Challenges in SDN based VANET

SDN based VANET exploits the benefits of SDN in the numerous applications of vehicular environment. Various challenges need to be handled in SDN based VANET as shown in Fig. 6. Among all these challenges, security is a major issue. These challenges [80] can be described as follows:

- **Management of dynamic network topology:** High mobility of vehicles incurs dynamic network topology, channel instability, and the link breaks [11]. These effects can be reduced through advanced vehicle direction and network topology prediction.
- **Security and privacy:** In this type of network, the controller is the central entity that can be imitated by a malicious user to disrupt the network functioning. If the privacy of vehicles and transmitted information in the network is not maintained, it can lead to severe accidents [18]. VANET is also prone to various security attacks, such as DDoS, Sybil, Man-in-the-middle, jamming attack, attacks on hardware and software components, attacks on infrastructure as hijacking and unauthorized access.
- **Latency control:** Latency depends on a variety of factors like data preprocessing operations, location tracking, resource availability etc. Latency can be controlled through the optimization of resources and performance parameters, and network implementation by using cloud infrastructure. But for large scale networks, cloud deployment is an expensive approach [85].
- **Scalability and heterogeneity of architecture:** With the change in network scale, network topology varies and technical upgradation is also needed. In large scale networks, numerous communication technologies require more network resources. Thus, inefficient resource management degrades network performance. Scalability leads to heterogeneity in the network. Incorporating coordination and communication between heterogeneous elements increases controller overhead and affects the performance. Inter-networking mechanisms based networking architecture can overcome the issues arising due to heterogeneity [11].
- **Resource scheduling:** Resource scheduling is a complex process due to the heterogeneous components, communication modes, computation, and scalability issues. Effective scheduling can be obtained through network optimization by using network availability vector and network cost vector. In Cooperative Data Scheduling (CDS) [86], the total weighted gain of the network is maximized because each vehicles' weight is inversely proportional to the remaining dwell time.
- **Heterogeneous wireless technology of VANET:** Vehicles can access the Internet via different wireless technologies like 3G, Wi-Fi, WAVE, WiMAX, 4G/LTE etc. The utilization of such types of technologies increases heterogeneity in the network. Wireless technologies have different network performance, communication costs, and a variety of resources required. Thus, it leads to the issues of interoperability and resource utilization in the network. However, software-defined vehicular network makes use of multiple wireless interfaces for multi-hop communication for better performance at low cost [87]. Author in [88] discusses that in the case of multiple wireless interfaces vehicles consider various parameters to choose one of the wireless technologies. Moreover, a vehicle can choose multiple interfaces simultaneously for example Wi-Fi and UMTS that increase overall bandwidth. The author utilizes SDN as the unified resource manager and designs a novel centralized resource scheduling solution. It allows SDN based VANET to choose the optimal network technologies from all available interfaces. [89] proposes network selection and data dissemination approach using heterogeneous wireless interfaces in SDN based VANET. A communication model is introduced for heterogeneous wireless networks and a solution is proposed for optimal network selection using two-stage Stackelberg game theory and a data dissemination approach that uses stable links and local controllers.
- **Centralized control of SDN:** Control functionality deployment and control implementation in both logical and physical form is a challenging issue. Due to the dynamic network infrastructure, it is challenging placing a controller at the edge of the network or distribution of its functionality to low-level controllers. In one of the categories of architecture, top-level controllers are established region wise. Whereas bottom level controllers are placed at some specified RSU and base stations, which are in the nearby regions of vehicles. This placement is performed to reduce the communication latency. But it is a challenging task to place controller functionalities based on VANET characteristics. Because VANET is inherently distributed, such as in the case of highways, the network needs to be partitioned. Then it is impractical to control all vehicles through a single controller. In [90], a distributed SDN based VANET architecture was proposed that manages the large scale network in highway scenarios by partitioning network in a distributed manner. Author in [91] proposed a semi-centralized flexible SDN based heterogeneous VANET architecture in which hierarchical multi controllers are installed on the network edge with an efficient fall back recovery mechanism. It is feasible for both covered and uncovered infrastructure-less area in VANET. [92] proposed a hierarchical software-defined VANET (HSDV) that makes use of clustering to create an infrastructure. It helps to maintain network functioning state regardless of central coordination through the controller and improves overall performance in case of a broken connection between vehicles and controller.
- **Connectivity:** Mobility of vehicles affects the wireless connectivity among the controller, infrastructure unit, and vehicles. Short communication time leads to delay in information forwarding related to network management, resource allocation, and network changes. The controller can deal with connectivity issues by minimizing the mobility effect on SDN based VANET. But such specific mechanisms are quite complex due to privacy and deployment issues [18].
- **Misbehavior of elements from different technologies (e.g. cloud, 5G, and ICN) involved:** Integrated technologies with SDN and controller can have security and other kinds of vulnerabilities that influence VANET operations functionality and performance also [18]. Such technology integration can introduce a new threat vector in VANET environment which is difficult to detect and prevent.
- **Trustworthiness evaluation, misbehavior detection, and revocation process:** Trusted vehicle reduces the security vulnerabilities in SDN based VANET. For misbehavior detection, active mechanisms should determine vehicle trustworthiness by using their behavioral and structural parameters. Certificate Revocation List (CRL) [93] can be used for the revocation process of a vehicle. But some more effective and fast detection and trust-based approaches should be designed [94].
- **Wider flow rule definitions and policies:** For VANET applications, flow rules have to be wider according to the application requirement. SDN controller should offload itself by sending the policy for flow rule making instead of directly sending the flow rules. In this way, the local controllers can determine the packet forwarding path based on the policy [18]. But it causes a new issue that which flow rules should be decided by the controller and for which the local controller should process in accordance with application need.

SDN based VANET can provide various services and benefits to ITS, but implementation of these types of architectures has to face a variety of challenges. These challenges should be dealt with precisely by integrating SDN with VANET before its deployment in a realistic environment.

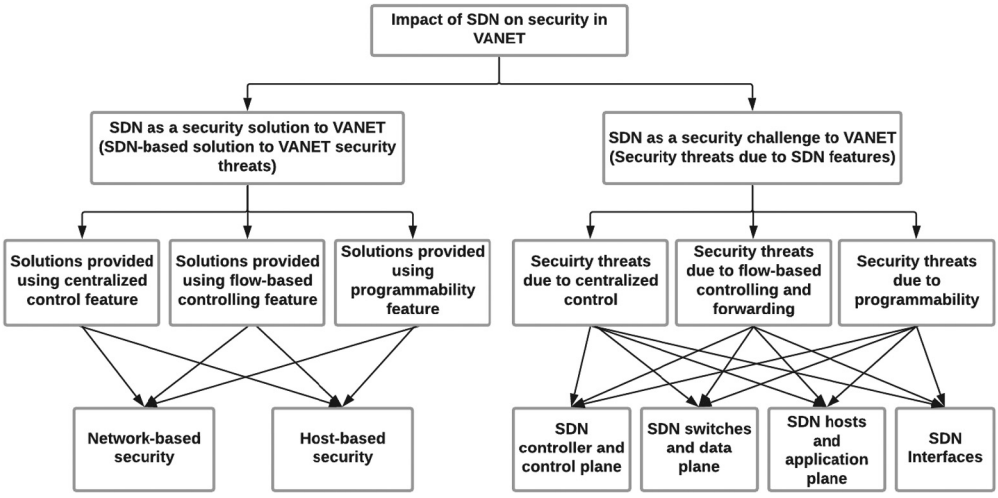

Fig. 7. Role of SDN in security of VANET.

3.5. Services provided to VANET by SDN

Besides applications described in the above sections, SDN serves with the different services in VANET which are essential from the security and efficiency point of view [17,95]. These are depicted as follows:

1. **Network forensic:** SDN controller keeps a global view of ongoing activities in the network and flow of traffic. The controller constantly monitors traffic flow and gathers information about traffic flow and current activities. Malicious nodes can modify the configuration of a node to disturb its functionality. These changes can be detected through the forensic analysis of gathered data and can be kept as network-based evidence. Through these forensics, the effect of undetected attacks can be found, so that some defensive mechanisms can be developed for these attacks. Compromised nodes can also be identified through the traceback in network forensic together with the detection of nodes responsible for these attacks [96]. Whereas in traditional networks, Network Forensic Analysis Tools (NFATs) and different advanced approaches are used.
2. **Self healing:** Self healing services provide automatic recovery to the network system in case of an attack. SDN controller defines the rules for each of the devices in the network. These rules define the limitations of the devices. Whenever the condition for a particular rule is reached, devices react in accordance with actions defined in the rules. Self healing process keeps monitoring the network and if some malicious activity is detected, diagnosis is also performed. Then self-healing mechanisms provide the solution to the network to get back into its native state.
3. **Frequency or channel selection**: Data transmission in VANET requires wireless channels with different frequencies. SDN controller dynamically selects the frequency channels appropriate for a specific data transmission from the available channels. Devices are not bounded to transmit through a specific frequency spectrum. As per the requirement, the devices are allotted with the channels dynamically. For emergency services, special channels are assigned.
4. **Route selection**: In SDN based VANET systems, SDN controller works to provide an efficient, secure, and optimal route for the data traffic. It provides the shortest route for transmission. But in case of bandwidth consumption or traffic congestion, SDN controller reroutes the traffic to a new route where the congestion probability is decreased.

As explained above, SDN provides a variety of services that facilitate the efficiency and secure transmission of data.

4. Impact of software defined networking on security of vehicular ad hoc network

The integration of SDN into VANET turns the network into a programmable and flexible network. SDN controller is a centralized entity that controls the whole network with efficiency and effectiveness. SDN controller in centralized mode is a single point of failure. If it fails, the whole vehicular environment becomes disrupted. SDN and VANET have some security challenges and these challenges make them prone to security attacks that violate the security requirements. Security is the premier concern for SDN based VANET applications, such as smart city, smart parking, platooning, infotainment services, safety, and non-safety applications. If the user is satisfied with the security policies and regulations related to kinds of vehicular applications, the demand and utilization of new prominent applications can increase. Security policies should ensure that the user's private information would be kept secret, and data exchanges will be not threatened and will remain secure. The key point to be considered is how the integration of SDN into VANET affects the security of VANET environment. SDN consists of features as global awareness of network, programmability, and flow-based forwarding which bring the advantages of enhancing security services in SDN-based VANET environment. Whereas these features also come with some disadvantages as vulnerabilities that originate security threats [97,98].

As shown in Fig. 7, SDN affects the security of SDN based VANET in two ways [19]. In first, SDN features help to detect and mitigate security attacks. Various security solutions provided using SDN features ensure network-based security and host-based security. And in the second way, SDN can be a challenge when new security threats occur due to SDN features. These security threats affect all of the three planes and interfaces in SDN based VANET. A detailed description of these forms is presented in the next subsections.

4.1. SDN as a solution to security threats in VANET

SDN controller has a global view of the whole network area. SDN characteristics, such as logical centralization, continuous monitoring of node and information in transit, and management can provide various benefits like uninterrupted services and security to VANET applications.

Table 3
VANET security attacks and affected security requirements: Authentication (A), Availability (B), Confidentiality (C), Data Integrity (D), Non-repudiation (E), and layers: Physical (1), Data Link (2), Network (3), Transport (4), Session (5), Presentation (6), Application (7).

Attacks	Security requirements	Layers
Brute Force Attack	A, C	7
GPS Spoofing	A, B	1
Illusion Attack	A, B, C, D	7
Bogus Information Attack	A, B, D	7
Replay Attack	A, E	1
Masquerading Attack	A, D	1, 2, 3, 4
Sybil Attack	A	1
Tunneling Attack	A, C	2, 3
Man in the Middle Attack	A, C, D, E	1, 2, 3, 4, 5, 6, 7
Routing Attack	A, C	3
DoS Attack	B, D	3, 4, 7
DDoS Attack	B, D	3, 4, 7
Repudiation	B, E	1, 7
Spamming	B	1
Malware	B, C	1
Black Hole Attack	B	3
Jamming	B, D	2, 3
Snooping Attack	C	1, 2, 3, 4
Traffic Analysis	C	1, 2, 3, 4
Sinkhole Attack	C, D	1, 3, 4
Eavesdropping	C	1, 2, 3, 4
Tampering Hardware Attack	D	2, 4, 7
Timing Attack	D	1, 3
Misbehavior	A, B, D	1, 3, 7

To understand how SDN can work as a solution to security attacks in VANET, first we describe the security threats in VANET. Afterward, the solutions and approaches to overcome VANET attacks by using the properties of SDN are depicted.

4.1.1. Security threats in VANET

All the applications in vehicular environments depend on exchanged data. If the exchanged data is compromised, it can create the worst consequences for the safety of drivers and vehicles. During the transmission, data can be falsified, modified, stolen, and misguided by some malicious node. This results in accidents, traffic congestion, resources unavailability etc. and can be more dangerous in an emergency. Applications of the intelligent transportation system should be provided with the security approaches that ensure the protection of data as well as the privacy of the user identification information [99].

VANET environment is highly dynamic where the connection between two vehicles remains for a very short time and network topology also varies instantly. In these situations, the implementation of security solutions is a critical task. In this subsection, VANET attacks are classified on the basis of affected security requirements and affected layers. Table 3 lists various security threats, which occur in VANET, and shows which security requirements and layers of the OSI network model are affected by a particular attack.

1. **Classification of VANET security attacks on the basis of security requirements:** To ensure the security of each VANET application, some requirements should be accomplished, which are called security requirements. These are Authentication, Availability, Confidentiality, Data Integrity, and Non-repudiation mainly. Security attacks in VANET can be classified according to various security requirements, which are threatened of that particular attack [3,37,60,18,100–103,42,104]. The security requirements and related attacks can be summarized as below:
   - **Attacks on authentication:** Authentication is a major security requirement for any network. It ensures that any malicious and unidentified node is not present in the network and messages should be generated only through a legitimate user. On the joining of the network by a node and before accessing ITS services, authentication of the node is required. Otherwise, an attacker node can violate these requirements and the network becomes vulnerable to security attacks, such as brute force attack, Sybil attack, GPS spoofing, illusion attack, bogus information attack, replay attack, masquerading attack, impersonation, tunneling attack, Man-in-the-middle attack, routing attack etc.
   - **Attacks on availability:** VANET applications are constantly utilized by the users. Therefore, VANET components and functionality should be available throughout time to provide services. Any violation of availability can disrupt network functionality and delay in information transmission. There are several attacks that affect the availability of network resources. Attacks can be Denial of Service (DoS) attack, Distributed Denial of Service (DDoS) attack, spamming, jamming, GPS spoofing, illusion attack, bogus information attack, repudiation attack, malware, black hole attack etc.
   - **Attacks on confidentiality:** Messages transmitted during the communication can contain sensitive information. In that case, to ensure confidentiality, the message should not be accessed by an illegitimate user. Confidentiality is concerned with some rules and restrictions that limit access to resources and sensitive information. But still, it is threatened by some attacks, such as tunneling attack, snooping attack, Man-in-the-middle attack, brute force attack, illusion attack, traffic analysis, malware, routing attack, sinkhole attack, eavesdropping etc.
   - **Attacks on data integrity:** Integrity ensures that the data in transit will not be altered, modified, or deleted. There are various attacks on the integrity of data as illusion attack, masquerading attack, sinkhole attack, impersonation, bogus information attack, DoS attack, Man-in-the-middle, tampering hardware attack, jamming attack, timing attack etc.
   - **Attacks on non-repudiation:** On receiving of a message, the receiver cannot deny from receiving, if it is sent through a legitimate user. As well as the sender cannot deny from sending a message. This is called non-repudiation, and this requirement is also induced by Man-in-the-middle, replay attack, repudiation etc.

Thus, different kinds of VANET attacks can disrupt the security requirements and can cause severe consequences for vehicles and the safety of drivers.

2. **Security attacks at different layers of network architecture:** According to the OSI model, VANET layered communication architecture comprises seven layers, such as physical, data link, network, transport, session, presentation, and application. Security attacks on VANET can be categorized on the basis of the target layer also [101]. Mainly, threats in session and presentation layers are not focused in VANET. Threats in different layers are as follows:
   - **Threats in physical layer:** Physical layer should be adaptable to changes in link characteristics of a network. The link radio signals are easy to eavesdrop and jam. Therefore, it causes security threats in the physical layer, such as jamming, DoS attack, interference, and eavesdropping etc.
   - **Threats in data link layer:** Link layer is based on the cooperation of the IEEE 802.11 Medium Access Control (MAC) and IEEE 802.11 Wireless Equivalent Privacy (WEP) protocol. MAC provides regular communication and WEP is responsible for providing security in the wireless local area network (WLAN). Both protocols are prone to security attacks, as MAC is vulnerable to DoS attacks and WEP is exposed to probabilistic cipher key recovery attack, message integrity attack, and message privacy attack etc.
   - **Threats in network layer:** Due to the varying topology of the network, it is a challenging task to maintain an efficient connection and route between vehicles. Different routing approaches are used for the establishment of an optimized and efficient route to spread and transfer the information to all the nodes in the network. But one security attack on the network layer can disrupt the whole communication in the network. There are kinds of attacks, which are performed on the network layer. They consist of routing code poisoning attack, routing table overflow attack, resource consumption, attacks on routing protocol, black hole attack, rushing attack, wormhole attack, Byzantine attack, and location disclosure.
   - **Threats in transport layer:** Transport layer is dedicated to providing secure end to end connection, communication establishment, encryption, authentication and to handle packet delay and packet loss. The functionality of this layer is also compromised due to attacks, such as session hijacking, SYN flooding, and TCP ACK storm.
   - **Threats in application layer:** Above the transport layer, session layer controls sessions, and connections in the network. The presentation layer handles data encryption and the presentation of data in a usable format. The application layer is concerned with the sensitive data related to vehicles. We primarily focus on the threats in the application layer. The attacker can acquire the control to handle some applications to capture the information about vehicles and their characteristics, such as their location, speed, acceleration etc. Repudiation attack and malicious code attacks are the foremost attacks performed in the application layer.

   As explained above, layers of VANET architecture are influenced by a variant of attacks. While communication and functionalities in the network are dependent on these network layers. Therefore, attacks on these layers can cause drastic consequences in the network.

4.1.2. SDN approaches to overcome security challenges in VANET

SDN has the ability to manage the transmission in the whole network together, without configuring network devices individually [62]. SDN has a global view of the network. Thus, it can control all the network components and flow using a centralized SDN controller. The traditional network requires lots of information exchange to secure the network. While SDN controller is capable of gathering and processing all the information simultaneously. The principle features of SDN provide security advantages to VANET. With the help of these features, SDN based architectures and networks are able to counteract prominent security attacks in VANET [105,106].

However, if the controller itself is compromised or impersonated by a malicious node, the network will be the most vulnerable to security threats. Through the compromised controller, the attacker can instruct network devices to perform malicious activities. Attackers can create fake and incorrect flow rules to disrupt communication and tamper the devices and software through the programmability. These malicious activities can cause resource unavailability, accidental situations, traffic congestion, and communication delay in the network. The next subsection covers these harms occurring in SDN based VANET. There is a trade-off between these two concepts: Whether SDN is a security advantage to VANET or it is a security challenge to VANET. Table 4 shows the taxonomy of VANET security threats according to SDN features that provide solutions to these attacks. In the last category, this table shows the attacks for which solutions are not provided using SDN. This table also gives a brief discussion of threats along with the proposed solutions in the literature to counteract those attacks.

1. **Attacks countered through centralized control and global awareness of network:** Centralized SDN controller is able to keep track of each of the ongoing activity and transmission. The controller can communicate with all the components of the network. Hence, through the gathered information from the network components, the controller dynamically takes the decision and instructs the network devices to perform accordingly. Various security attacks can be countered with the help of this SDN feature.

   In a masquerading attack, the attacker impersonates a benign vehicle through identity theft or by stealing the vehicle credentials. The attacker is intended to get access to some services and exchanged information in place of a compromised vehicle. SDN controller keeps track of suspicious activities in the network globally. If some doubtful is detected, SDN controller can do further inspections through identity confirmation or it can isolate the impersonating vehicle. The controller blocks the data flows and access to data transmitted by the impersonating vehicle until further scans are performed. This approach can be applied in an electronic vehicle smart grid to overcome masquerading attack [15].

   In a replay attack, the attacker captures and resends the messages in a later time, which was sent previously in the network. These replayed messages contain expired information that has no use in the current scenario. Uses of these messages can originate hazardous results for safety and non-safety applications. Sometimes, replay attacks are not easy to be identified because they do not create such situations to be detected. Besides this, some messages can be replayed intending to flooding at the target node. They can be replayed to consume the network resources, such as bandwidth, buffer memory, and processing power so that legitimate nodes would be unable to use resources in an emergency. To overcome this attack, a variant of approaches can be furnished using SDN. In one mechanism, as a centralized SDN controller has a global view so every message in the network can be assigned with a globally synchronized time with respect to the controller. Thus, if the old messages are replayed, they will be identified through their expired time. In another approach, each data packet can be assigned with a sequence number. If the same packet is replayed after some time, it can be detected easily, and then it

Table 4
Taxonomy of VANET attacks with respect to provided solution (using SDN and without SDN), and their existing solution.

Attack category	VANET attacks	Attack description	Existing solutions
Attacks whose solutions are provided using centralized control SDN feature	Masquerading Attack/Sybil Attack	A legitimate user is impersonated by attacker through providing false ID, and then attacker tries to get exchanged information and send wrong messages	Use sequence number and digital signature [107], validate entities using signature, timestamp and temporary certificates [108–110]
	Replay Attack	Attacker intercept and keep the copy of warning and other messages, and then replay them by impersonating legitimate user	ARIADNE [111,112]
	Sinkhole Attack	Traffic is routed through a malicious gateway to intercept information and then retransmitted	Sinkhole detection using RMHSD [113], Sinkhole detection using MD5 [114]
	Black Hole Attack	A malicious node who does not exist in the network, pretend itself as the shortest route for the packets, so packets are directed to that route where node can intercept the data, and drop or forward to desired node	[111,115], secure routing process [116]
Attacks whose solutions are provided using flow-based Controlling and Forwarding SDN feature	Malware	A malicious software is injected into the network and multiple copies of this software are created	Attack detection using authentication mechanism [117]
	DDoS Attack	DoS attack performed in a distributed fashion	Suspect a greedy behavior and identify responsible nodes [118], Redundancy Elimination Mechanism [119]
	Bogus Information Attack	Bogus or incorrect information is transmitted intentionally to divert the target vehicle's direction	Truthfulness of reported data should be computed [120,121], use signature to check authenticity of data [122] and monitoring to identify unusual changes in vehicle location [123]
Attacks whose solutions are provided using programmability SDN feature	Jamming	Channel frequencies are interfered by the interfering signal to prevent communication through the channel	Frequency hopping or switch the transmission channel [119], anti-jamming [124]
	Snooping (Eavesdropping)	Passive attack intended to extract information without modification through eavesdropping	VANSEC protocol [125], [37]
	Intrusion Attacks	Performed to get access the system without valid credential and compromise the system security	Lightweight intrusion detection mechanism [126]
	DoS Attack	The victim is attacked by sending service requests in large amount to make resources unavailable for benign users	Apply digital signature and authentication method [127], use secure routing protocols with one way hash function and symmetric cryptography [111]
Attacks whose solutions are not provided using SDN features	Repudiation Attack	Attacker denies of sending or receiving of messages, and causes retransmission and delay	SAODV [128], detect compromised nodes [129]
	Tunneling Attack	Through misguidance, the vehicle is sent into a tunnel path in order to disrupt network consistency	[37]
	Man-in-the-Middle Attack	A malicious node listens to ongoing communication and may insert false information	Authentication using digital certificates [115], lightweight authentication scheme [130], misbehaving node detection via RSU [131]
	Tampering Hardware	Vehicle hardware and sensors are tampered physically during the manufacturing, to get and put the data or to alter the working of hardware	Control at manufacturing
	Routing Attack	Network layer functionality is disrupted either by packet drop or routing alteration	Verify vehicles [132], identify malicious vehicles [133]
	Timing Attack	Messages are delayed intentionally in order to make them useless and induce the reliability in network	[119,115]
	Misbehavior	Active entity misbehaves by transmitting false information in order to disrupt the network intentionally or it can be unintentional due to malfunctioning	Misbehavior detection mechanism [134], machine learning based misbehavior detection [71]

is discarded. These approaches can be employed in platooning [15].

Through the sinkhole attack, the attacker route the data flow to an adversary node that acts as a convenient gateway for the data flow. But at that gateway, the attacker can intercept the data or can stop the data from being forwarded to the actual recipient. The impact of this attack can be more crucial in the case of emergency services. SDN provides an authorization mechanism based on trust calculated for the relay infrastructure or relay node. Before forwarding the data to the next intermediate vehicle of infrastructure through V2V communication, the sender node asks the controller for the reliability of the recipient node. The controller receives feedback for the recipient node from the members in the community of the recipient node where that node usually forwards the data. On the basis of obtained positive or negative feedback, SDN controller decides whether the node is reliable or not. If the controller receives positive feedback from the community members, the sender is advised to forward the data to that recipient. This approach can be followed in emergency services [15]. Sometimes it can consume more time to determine the trust value for a relay node. As the connection between vehicles remains for a short duration, the trust computation should be faster to defend from the sinkhole attack. This solution can be applied to defend from the black hole attack also. In this attack, the adversary node advertises and intercepts the forwarded packets to that route.

SDN can provide defense solution from intrusions also. Intrusion can be any doubtful activity, entity, and behavior in the network system, which can trouble network security by causing various security attacks. By centralized control property of SDN, various intrusion detection methods are proposed. One

of them is L-IDS (Learning Intrusion Detection System) [135], which uses SDN features. It can detect a variety of attacks by creating diverse anomaly rules in embedded mobile devices on an institutional site. This approach can be applied in vehicular networks for embedded devices in vehicles within the existing systems without modifications. On detection of attacks, the network can be configured dynamically with the help of an employed mechanism in the IDS for mitigation of attacks through the controller. Thus, countermeasures for various attacks can be implemented by the centralized controller.

2. **Attacks countered through flow-based controlling and forwarding:** This feature of SDN is able to mitigate various kinds of attacks. It grants security at a granular level. Data flow from different devices is analyzed and if they are identified suspicious then those devices are labeled and isolated [15]. The forwarding devices are directed to not process the data flow coming from those labeled devices.

   One of the major threats is malware (a suspicious program) injected into the application programs which can infect one component or the whole. As a result of this attack, the application does not function correctly and shows the dubious behavior. To mitigate this, SDN controller detects suspicious devices on the basis of data flow. Through the analysis of data flow in a network, doubtful devices are detected and isolated from the network. This approach can be applied in an electric vehicle smart grid.

   In DDoS attack, a subset of vehicles (called zombies or bots) is infected to perform maliciously in control of coordinating vehicle (botmaster). The botmaster triggers the botnet to send a large number of fake signals to a victim service provider. In effect of this, the service provider is overloaded with numerous requests and becomes unavailable to provide services to legitimate vehicles. To counter this attack, SDN controller keeps track of ongoing flows for the services, which can be compromised through this attack. If any suspicious traffic flow is detected, the controller identifies sources of the data flow and instructs the data plane elements to drop the data packet coming from those malicious sources. Thus, the malicious traffic flow is not routed further and the occurrence of DDoS attack is prevented. This measure can be applied in emergency services. One lightweight method, Self Organizing Maps (SOM) was proposed in [136] for DDoS detection. SOMs are trained with traffic flow features. They extract features of traffic flow for detection with low overhead and provide detection through the trained traffic flow at a good rate.

   Bogus information attack can be performed to create an accidental situation or divert the vehicle's direction to a different path by transmitting fake information. SDN provides a solution to defend this attack as a collective consensus approach [15]. When an emergency is detected in a particular area, SDN controller contacts the other vehicles in that area by using this mechanism. SDN gathers the details from other vehicles regarding the information provided by the malicious vehicle. If the collected detail is not consistent as the dispersed information regarding emergency, then the controller directs the vehicles by sending new flow rules to drop the data packets coming from that malicious vehicle.

   This mechanism can be deployed in emergencies. But it can also take lots of time for decision-making by the controller if the vehicles do not respond immediately. Some novel approaches can be used where vehicles are provided with the classifier. Vehicles can determine the correctness of information based on keywords and some major features of received information in less time. Thus, through flow-based forwarding, the controller can detect malicious flow and instruct the forwarding devices to behave accordingly by creating new flow rules.

3. **Attacks countered through programmability:** In SDN, the programmability feature allows SDN controller to reconfigure, update and delete the policies to instruct RSU and other forwarding devices (vehicles). Network devices can be directed to perform different tasks and functions, in accordance with behavior recorded and requirements in the network. It also allows creating and deploy robust and flexible approaches to detect and mitigate attacks [19]. In this section, we describe how different types of attacks can be overcome through programmability.

   In a jamming attack, information transmitting signals are interfered with by jamming signals transmitted through a powerful transmitter of an attacker in a particular frequency channel. Thus, the receiver becomes unable to receive sensitive and important information on time due to interference in the effect of a jamming attack. To counter this, RSU gathers information about the quality of used channels for transmission and forward that to the controller. According to the quality, the controller blacklists the channels where the heavy interference is observed. The controller forwards the list of bad channels to RSU and forwarding devices. Then instruct the devices through creating new policies that how to use channels hopping in case of heavy interference [15]. This mechanism can be followed in smart parking, platooning, and other fields, which are vulnerable to jamming attacks. According to this mechanism, the bad channels remain underutilized as they are not allocated to legitimate users in one network. In that case, malicious users can utilize these channels to forward their data to bother the ongoing activities and perform various attacks on other networks.

   In snooping (eavesdropping) attacker analyzes the beacons of vehicles during communication with SDN controller. Through this attack, the attacker tries to obtain the identity, behavior, habits, and path of a target vehicle or a large community of vehicles. To maintain the privacy of vehicle information, their ID's should not be transmitted during the communication. To achieve this, RSU gets the ID's of vehicles in a particular region and creates a list. This list is forwarded to SDN controller. The controller swaps the ID's of vehicles with other temporary IDs according to a predefined policy. Now, the vehicles retransmit their beacons with new IDs, so that the eavesdropper will not be able to identify the correct vehicle information [15]. In the smart parking application, this approach can be used. Obtaining the IDs of vehicles by the attacker is not the only way to eavesdrop the communication. Attackers can acquire behavior and other information related to vehicles. Attackers can do this through continuous monitoring of vehicles, by following the driver or vehicle activities, and by using other ways. Therefore, some unique approaches can be proposed to protect all the sensitive information related to vehicles together with their IDs. So, the adversary would not be able to eavesdrop ongoing communication.

   By using the programmability feature, intrusion detection systems can overcome various threat vectors [19], such as traffic flooding attack, buffer overflow attack etc. [137] gives an anomaly detection method where algorithms are based on SDN programmability. In this method, information is conveyed to Internet Service Provider (ISP) on the detection of an anomaly. ISP can use this information to identify the existence of an attack. One solution SnortFlow was proposed in [138]. This approach uses a combination of the intrusion detection capability of Snort and the reconfiguration property of OpenFlow for intrusion prevention in the cloud environment. The

Table 5
Security threats in SDN based VANET.

Origin of attacks	Attack	Affected plane/interface in SDN based VANET	Proposed countermeasures
Attacks occurring due to centralized control	DDoS Attack	Control plane, data plane, control-plane interface	Use of multiple controller [95], FloodGuard mechanism [140]
	Privacy Violation	Data plane	Group based and ID based signature [141], Identity based Conditional Privacy Preserving Authentication (CCPA) [142]
	Unauthorized Access	Control, data, application plane, control-data, control-application interface	Secure SDN structure with byzantine algorithm [143]
Attacks occurring due to flow-based Controlling and Forwarding	Conflict in rules	Data, control plane	FortNOX [144]
	Routing Attack	Control plane	Statistical method for Sybil detection [132], Geo-statistical hazard model for sinkhole detection [145], message authentication [141]
	DoS Attack	Control plane, data plane, application plane, control-plane interface	[146]
Attacks occurring due to Programmability	Network topology poisoning	Control, data, application plane, control-data, control-application interface	TopoGuard mechanism to detect fake link updates [147], Sphinx [148]
	Malware	Control, data, application plane, control-data, control-application interface	Network behavior based model [149]
Miscellaneous Attacks	Control plane resource consumption	Control, data, application plane, control-data interface	FloodGuard [140], LineSwitch [150], FloodDefender [151]
	Forgery	Data plane, data-control interface	Secure localization method [152], [153]
Attacks inherited from VANET	On Board Tampering	Control, data, application plane, control-data, control-application interface	Anomaly detection [154]
	Jamming	Data, control plane, data-control interface	Bad channel detection [155]
	Impersonation	Data, control plane	Anomaly detection [156]

performance of this approach can vary with different scenarios of deployment.

In DDoS attack, one vehicle node is flooded with multiple packets of different flows simultaneously. The vehicle buffers the packets and asks RSU for the flow rules related to the packet, for which the vehicle does not consist of rules. Vehicles have limited cache space, so some buffered packets may be dropped. In this way, the packets from legitimate users can also be dropped. One SDN application, DefenseFlowTM [139] was developed to counter DoS attacks by Radware, a security solution provider. This application analyzes the traffic flow, collected by the controller from forwarding devices. On analyzing the traffic patterns suggested for DoS attack, if a threat is detected then the suspicious traffic is redirected to a scrubbing center. Traffic is redirected by the mechanism of traffic diversion for detailed investigation through signature detection and neutralization of threats. Thus, the DoS attack can be prevented from occurrence through detection. In this way, SDN controller can reconfigure the network policies through programming to detect and overcome the attacks in VANET.

As explained above, VANET attacks can be defended through mechanisms using SDN features. Their performance can be improved by deploying new capabilities and features into them. Through these capabilities, the mechanisms will be able to consider kinds of factors, such as heterogeneity, speed, accuracy, resource availability, and utilization.

4.2. SDN as a security challenge to VANET

As described in the previous section, foremost attacks in VANET, such as DDoS, jamming, impersonation, sinkhole, replay etc. can be countered by using SDN features. But SDN is also vulnerable to some more attacks, which are inherited into SDN based VANET together with attacks in VANET. In this section, the major attacks of SDN based VANET are described. We have also presented different mechanisms proposed for the detection and prevention of these attacks.

4.2.1. Security threats in SDN based VANET

Security vulnerabilities in SDN based VANET are consequences of SDN vulnerabilities as well as of vulnerabilities in VANET. In this subsection, at first, the threats inherited from SDN are summarized among which some threats are performed in VANET also. After this, some threats are described, which are found only in VANET. Table 5 shows a list of attacks originated from different sources, names of planes, which are affected by the attack, and mechanisms proposed to defend from the respective attack.

- **Security threats inherited from SDN:** Though the adaptation of SDN in various wireless access or wired networks may bring the programmability in the deployment of network and implementation of applications. It comes with lots of vulnerabilities acquired from its architecture with its centralized control and flexibility. SDN controller can reduce conflicts between security policies installed in networks and supply coordination between network components. Opposed to this, it is a single point of failure and principle target to be attacked by malicious users. By spoofing the identity of the controller, network functionality can be altered [157]. Programmability furnishes diversity in SDN security policies, but it can also be affected through malicious programs. Flow-based forwarding is able to isolate and label the doubtful flows. But this is also vulnerable to flow poisoning attack due to lack of intelligence in data plane devices [15]. Thus, the features of SDN supply vulnerabilities as disadvantages to SDN based VANET. Some attacks

of SDN also occur in VANET environment but due to different vulnerability. There are various attacks which can be categorized as follows:

1. **Security attacks due to centralized control:** There are various threats, which can occur due to compromised controller in the control plane. One of them is a DDoS Attack in which multiple attacker nodes send the numerous packets simultaneously to one or more vehicles or switches. Thus, the unavailability of network resources occurs and the network is threatened. For the different kinds of packets, the rules may not be installed at vehicles. Therefore, multiple queries are sent to the controller to generate the rules for the packets. It requires large processing power and many amounts of time. In that situation, the controller can drop queries as it is not capable to serve all of them simultaneously. This attack takes place in the control plane and if the centralized controller is compromised, it can influence the working of the whole network [17]. Thus, a single centralized control can make the network vulnerable and security attacks can happen in the network. DDoS occurs in VANET also where the vehicles, RSU, and base station are targeted. To overcome this attack, multiple controllers should be used in high-density traffic areas where these controllers are logically linked with the centralized controller. The programming in the entire network can be done through the centralized controller which can also manage the overall functionality of the network system [95]. One solution approach is FloodGuard [140], which uses data plane cache to store the packets for which table miss occurs. Then those packets are processed through the packet migration technique. This approach also uses a proactive flow rule analyzer to track the sensitive values of state variables in executing applications. It performs dynamic conversion of path conditions into proactive flow rules and installs them into OpenFlow switches.
   Through the privacy violation attack, the privacy of the vehicles can be violated by the attacker or through an authorized entity, such as SDN controller. The sensitive information of the vehicles, such as user identity, location, license plate number etc. can be leaked. This thing affects network architecture and functionalities. The privacy leakage can be originated from the controller side. But together with protection at the controller side, the south-bound and north-bound communication interface should also be protected [18]. The privacy of VANET application users can be exposed by the adversaries also in VANET. To preserve the privacy of vehicles, a group based and ID-based signature scheme was proposed in [141]. This scheme provides privacy preservation between VANET entities without managing public keys and certificates with low message transmission delay. In [142], the author presents an identity based Conditional Privacy Preserving Authentication (CCPA) scheme for VANET. It provides privacy protection and mutual authentication at the same instant for both types of communication V2V and V2I. It intensifies performance and it has lower computation and communication cost because it does not use bilinear pairing.
   An attacker can gain unauthorized access to network resources and devices by impersonating the centralized controller or any of the applications in the network. Thus, it can manipulate the network operations and policies. To counter this attack, a secure SDN structure is presented in [143] where each network element is under the control of multiple controllers with the help of the Byzantine mechanism. Together with this, an algorithm for controller assignment is also proposed. This algorithm securely assigns a minimized number of controllers to switches with Byzantine fault tolerance.
   As explained above, a single centralized controller can be threatened by various attacks. For those attack, a variety of solutions was also proposed.
2. **Security attacks due to flow-based controlling and forwarding:** Whole communication and services in a network are controlled on the basis of flow rules. By creating conflicts in flow rules and modifying flow rules, network control and communication can malfunction. Some of those types of threats are explained here.
   Conflict in rules is one of the major threats in SDN. Flow rules regarding the data packets are installed in the forwarding devices by the network controller. These flow rules can be overridden by some non-secure rules, which can produce the rule conflicts and vulnerabilities for harmful attacks on applications of SDN based VANET. FortNOX [144] is one of the proposed solutions that detect the conflicts in rules, which can originate contradiction in existing security policies. FortNOX expands the NOX controller by using digitally signed authorization roles to solve rule conflicts. It does not allow any OpenFlow application to override the once inserted rules, with the rules that can cause conflicts in rules.
   SDN and VANET both have vulnerabilities that can proceed to routing attacks, such as Sybil, replay, and sinkhole attacks. Thus, SDN based VANET also has routing threats produced through flow rule modification. It affects the forwarding of messages and their routing path in the network. In the Sybil attack, the attacker generates fake identities to create the illusion of traffic congestion. To overcome this attack, one solution was given in [132]. It specifies a statistical method and analyzes the signal strength distribution for the detection of Sybil attack. It also verifies the physical location of the vehicle. In [145], a centralized approach was proposed for sinkhole attack detection using the geostatistical hazard model. This model detects sinkhole by finding the energy holes in every region of the network. A distributed monitoring approach explores the neighbors to detect energy holes. The mitigation scheme in this model prevents the flow of data packets towards the suspicious region of sinkhole attack. In a replay attack, the attacker acquires a copy of a message and resends to cause hazardous situations in the network. A mechanism for authentication of the message proposed in [141] can be applied here to overcome the replay attack on receiving a message.
   When the DoS attacks are performed, vehicles are flooded with multiple packets by the attacker. Vehicle nodes have limited cache space for buffering the incoming packets for which flow rules are not available to the vehicle. When the cache reaches its limit, the vehicle may drop the packets. Thus, the data packet coming from some legitimate users can also be dropped. The resources become unavailable for legitimate users and their services are also denied. This attack is performed at the forwarding plane of SDN based VANET [17]. One solution to this attack is, the vehicle should have a large capacity to store the multiple rules that belong to various kinds of packets. Thus, it will be easier to make the forwarding decision, and the overall throughput of the network will be increased [146].
   As described above, flow-based forwarding and control can also cause vulnerabilities to principle attacks in SDN based VANET. These attacks can be countered through different mechanisms as explained above.
3. **Security attacks due to programmability:** Whole working of SDN based VANETs is configured and controlled through

programming. Adversaries can insert malicious program, to alter network processing and functionalities. In this way, various attacks can be performed, such as network topology poisoning. SDN controller maintains the topology of the network and controls the routing of packets by allocating flow rules to upper layer applications and services. If the controller is hijacked, then false link information can be injected through the programming to create the black holes. Where all the data packets are forwarded to a malicious route, and packets can be altered and dropped. Thus, topology poisoning persists in SDN based VANET. This can threaten safety applications by producing black holes in the network. In [147], a mechanism TopoGuard can detect fake link update information through behavioral profiling. This mechanism can validate the updates in the network topology on the basis of information given by the Port Manager and Host Tracker module. One more mechanism Sphinx [148] provides network topology poisoning detection by monitoring the deviation in network states through regular exploitation of flow graph.

Programmability can cause the insertion of malicious codes and unauthenticated messages into the vehicle, controllers, RSU, and applications. These malicious codes can replicate themselves into different layers of SDN based VANET to disorder network activities. One approach is proposed in [149], which is a network behavior-based model to detect the malware. It observes the suspicious activities in the network by using detection algorithms at the time of connection request in the controller. These algorithms include connection rate, connection success ratio, and IP blacklisting. This approach does not extract the information from the packets. Thus, the privacy of devices remains unaffected.

Thus, attacks explained above can be performed through the modification in programming. These attacks influence the whole processing of the network. Some solutions were also presented in this part that can prevent these attacks.

4. **Miscellaneous attacks**: There are some more attacks that do not fall in the above categories, such as control plane resource consumption and forgery attack. In most of SDN architectures, the control plane is vulnerable to resource consumption attack. If the required flow rules are not available at RSU and switches then many requests for flow rules are sent to the controller from the data plane. The controller is overwhelmed with multiple requests. Sometimes the packets in RSU have to wait for the flow rules until it deletes the old flow rules. This happens because the RSU and the controller do not have enough resources. Thus, it causes resource consumption at the control plane and data plane.

   SDN approaches can be used for SDN based VANET also, such as FloodGuard [140]. It uses data plane cache to store the table miss packets and then uses the packet migration technique. LineSwitch [150] mechanism is based on blacklisting and probabilistic approach. By using these approaches, the mechanism prevents the traffic flow from reaching the controller. Thus, it can protect from SYN flooding attack, control plane saturation attack, and buffer saturation attack. One approach is given as FloodDefender [151]. This approach can identify attacks and process table miss packets through the three techniques, which are packet filter, flow table management, and table miss engineering. This approach is scalable and independent of protocols and it can be implemented easily without embedding new devices.

   Through the forgery attack, false messages, and rules are transmitted in the network. Forgery attacks include GPS spoofing, Bogus Information attack etc. These attacks can cause serious accidental situations. They can be prevented by using secure localization of a benign vehicle node. [152] presents a validated and secure localization. Here, to determine the location of a node more trusted anchor nodes (Triangular) are used. Thus, location information cannot be fabricated. In one proposed method [153], location is determined for a cheating node, which can cause a Sybil attack. The location is found using the RSSI based trilateration method. Thus, if a Sybil attack is launched, it can be detected easily.

   As shown above, those attacks affect network performance. To counter them, some solution approaches are also given.

- **Security threats inherited from VANET**: When SDN is deployed into a traditional VANET environment, VANET has some key attacks. These attacks are conducted into SDN based VANET. One of them is on board tampering attack. Some of the vehicles can disrupt the communication of other vehicles by modifying, dropping, or corrupting the in-transit data packets during safety and non-safety application. In another way, the attacker can tamper on board sensing in SDN based VANET architecture.

  Anomaly detection behavior can be used to identify the tampered data packets. As in [154], the author proposed a watchdog based scheme. In this scheme, watchdog nodes observe the behavior of nodes in the relay and prevent uncooperative data transmission in the network. Only authentic data packets are allowed to be propagated.

  Through jamming attack, transmitting signals are interfered by the jamming signals which are sent by the powerful transmitter. A jamming signal can cause a disturbance in the sensitive data transmission and can partition the network. As a consequence of this, the controller becomes unable to guide the vehicles and cannot monitor the network correctly. To counter this, RSU monitors the quality of channels and gathers the information [155]. Based on information forwarded by the RSU, the controller can list the bad channels and forward it to all the deployed nodes in the network. And then, those bad channels are not utilized for transmission.

  Through impersonation attack, an attacker can impersonate a legitimate user to change the direction of other vehicles or to distribute false information about road conditions to mislead the vehicles and to cause an accidental situation.

  In SDN based VANET, the anomaly (impersonator) can be detected during the link discovery by the controller. To counter this, one approach is proposed in [156]. It traces back the sources of an anomaly in the network and uses this method to identify the switches creating the routes for the anomaly.

Thus, SDN based VANET suffers from a variety of attacks. SDN can provide solutions to threats to some extent. But still, there are various vulnerabilities for which novel mechanisms should be developed to defend those attacks. Some approaches are defined below.

4.2.2. Novel security approaches in SDN based VANET

In the previous section, we have described various security threats occurring in SDN and VANET. The provided solutions for the threat vector were also discussed in the above section. This section narrating security solutions using different novel techniques. These techniques include machine learning, deep learning along with trust computation techniques. They overcome the major attacks and provides effective performance, accuracy, and secure routing. These approaches are as follows:

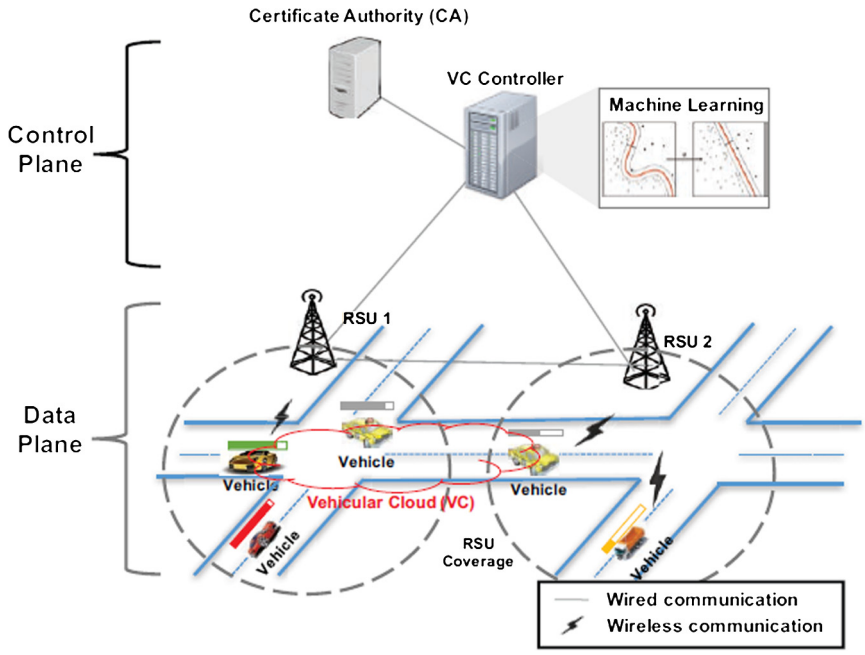

Fig. 8. Software Defined Vehicular Cloud (SDVC) architecture [158].

- **Security attack detection approaches in SDN based VANET:** At present a number of security approaches utilize machine learning algorithms and blockchain-based approaches to detect the major attacks. One of the approaches is collaborative security attack detection. Due to the characteristics of VANET, it has vulnerabilities for unexpected attacks which are difficult to be predicted. To overcome these, a collaborative security attack detection approach was proposed in [158]. In this mechanism, the Software-Defined Vehicular Cloud architecture (SDVC) is used where SDVC controller maintains a global view of the network on the basis of information collected from vehicles as shown in Fig. 8. Vehicles can create Vehicular Cloud (VC) to execute the resource-intensive services by using SDVC controller. VC observes the flow information for the incoming packets and sends it to SDVC controller. In a centralized manner, SDVC controller performs the training of multi class Support Vector Machine (SVM) with the collected flow information from VC. After this, SDVC controller originates an SVM classifier and distributes it to all the vehicles in the network. Through this classifier, vehicles can perform the classification of flows for incoming packets and identify the unexpected attacks in advance.
  SDVC controller has enough computation power, storage, and large database. If the number of flow information, i.e. datasets are increased then SDN classifier can perform with increased accuracy, precision, and recall. The vehicle can identify attacks more accurately than the distributed approach.
  Author in [159] proposes Sentinel, a mitigation algorithm for DDoS flooding attacks in highly dynamic SDN based VANET. This algorithm works within the controller that creates new flow rules to prevent attack packet forwarding. It has two phases as detection of attack and mitigation of the attack. In the detection phase, flooding attack is detected on the basis of time series analysis of packet flow. On the detection of an attack, a flow tree is constructed to find the source of the spoofed packet in the mitigation phase. This approach is able to mitigate attacks in all density scenarios and various parameters. It is an efficient method and has better mitigation rate. [160] proposes a framework for securing the vehicular social network. A centralized controller is a single point of failure. Therefore, together with SDN, this framework uses a blockchain concept that certifies transactions and gives data anonymity in a distributed way by-passing the centralized approach. In this framework, three levels of controllers as Principal Controller (PC), RSU, and miners are used. Local controllers act as minor which are selected using the proposed Distributed Miners Connected Dominating Set algorithm (DMCDS). DMCDS is a single-phase algorithm and supports dynamic topology. Miners are selected based on a minor score which depends on a trust parameter and network parameters. The performance is measured in various scenarios using parameters, such as trust metric, node mobility, node density, and radio range. This framework is resistant to security attacks also including identity-based attacks, eavesdropping attacks, and service-based attacks.
- **Trust based secure routing algorithms in software-defined vehicular ad hoc network:** Various approaches were proposed to enable secure routing in SDN based VANET. These approaches used trust computation techniques with learning mechanisms to provide improved and secure routing. One of the proposed protocols is an Improvised-Trust based Ad Hoc on Demand Distance Vector Routing (I-TAODV) protocol [161]. It offers secure routing in SDN based VANET. This method provides double security checks for the detection of malicious vehicles with the help of two algorithms. Based on the calculated trust value, the first algorithm detects trusted vehicles. Malicious vehicles are identified using the second algorithm. Thus, if in the first algorithm, a malicious vehicle is detected as a trusted vehicle because of algorithm fail. Then it cannot be escaped in the second algorithm where it will be detected as malicious. In this way, through the double security check, this protocol has improved throughput and reduced delay in comparison to existing protocols, such as AODV and TAODV. In [162], the author implemented a deep reinforcement learning algorithm in software-defined vehicular ad hoc networks to evaluate the behavior of neighboring nodes. There are two phases: (a) trust computation phase and (b) path learning phase. In the first phase, a trust model is deployed to calculate the trust of the immediate path for Q-value (maximum long term reward for the best-trusted path in path learning) by using a convolution

neural network. In the next phase, a deep Q-learning algorithm is used to calculate the best routing policy. This scheme is focused to maximize the long term reward value. The vehicles selected in the final route are used more to forward the data packets further than the unselected vehicles.

Thus, there are various approaches that have been proposed based on feature detection by using machine learning, deep learning, neural networks. These features are different vehicle parameters, flow information, and features of transmitted traffic flow in the network.

5. Discussion and future directions

In this section, we explain some findings which are gathered from the review of the presented state of the art and survey on security in SDN based VANET. Then we summarize open issues and challenges that provide possible future directions in order to develop effective and secure SDN based VANET. Some of these open issues are also addressed in subsection 3.4.

5.1. Learning outcomes

The lessons learned from our comprehensive survey are discussed as follows:

- When SDN is integrated with VANET, it can improvise the performance of VANET. It can overcome the issues of mobility, dynamic network topology, and short connection time through network programmability and flexibility. SDN also comes up with the features of centralized control, programmability, and flow-based forwarding and controlling. It can saturate the impact of various issues in VANET, including security threats to VANET, through its unique properties. But these properties also can be the reason for causing security vulnerabilities in a network.
- Each security approach applied to SDN based VANET is based on the working abilities of a centralized controller. It can defeat the diverse security problems by utilizing its characteristics. But the controller is an easy target for adversaries to disorganize the services and performance of the whole network. If the controller is compromised or imitated, the adversary can modify the functionality of the network and reconfigure network policies. An adversary can also perform attacks on various planes in the network. Therefore, the security of the controller is a key issue which is the foremost requirement for the protection of the whole network. However, none of the comprehensive surveys on SDN security has covered this issue that should also be investigated and discussed.
- SDN comes with the concept of a local agent. Each of the vehicles is installed with a local agent that works as a local controller in case of lost communication with the centralized controller. When the single controller fails, local agents provide the flow decision and routing mechanisms to vehicles in order to implement safety and non-safety applications without interruption. Local agents do not have adequate facilities and power so that they can serve the security services also. In that case, one phenomenon of multiple controllers in a network can be utilized. To overcome the issue of a single controller failure, multiple controllers can be placed in a network. These controllers are logically linked and managed by a centralized controller. They can deploy security approaches within their region. But installation and maintenance of these controllers may increase the burden over the network because it requires continuous communication and network resources. This solution comes with the new issues, such as the number of controllers required and where they should be placed. These issues were not discussed extensively in previous researches.
- Through this article, we can infer that SDN provides the security services till the network controller is safe and not compromised since whole network activities and services are based on this central entity. Various security algorithms are proposed that ensure the security of network traffic and user data. But their implementation overhead and accuracy is a serious concern.

5.2. Future research directions

Here we provide a precise roadmap that can be considered for future research in SDN based VANETs.

- **Scalability and heterogeneous network management:** In the scalable network environment, vehicular applications have diverse resource and communication requirements. Although, an approach is proposed in [89] for network management and data dissemination in a heterogeneous network environment that enhances the network performance also. Still, the designing of such network architecture is an open research issue, that can serve the heterogeneous network requirements and upgrade the network performance.
- **Multiple controller placement:** In large scale networks, the concept of using the multiple controllers was proposed for the proper functioning of the network in case of single controller failure. Placement of numerous controllers and to decide the number of required controllers is still questionable. Finding the solution to these issues can be addressed as a promising research problem in the future.
- **Centralized controller security:** In SDN based networks, centralized controller security is essential for protecting the whole network. Most of the researchers emphasize confidentiality and integrity security requirements in the network. To develop such network architectures and security mechanisms that ensure the security of the centralized controller is a possible research direction.

6. Conclusion

The dynamic network architecture of SDN has successfully transformed traditional networks into diverse application oriented networks. SDN based VANET is evolving as SDN provides intelligence in VANETs due to the open, re-configurable interface and flexibility of SDN. In this paper, we explored SDN based VANET and its various aspects through discussions based on available literature and tried to present the relevant understanding of security issues faced in SDN based VANET. We have presented the detail of VANET and SDN with the description of their components. This article highlights the issue of security and privacy which is a major challenge in SDN based VANET. We have presented classifications and a list of threats with their solutions based on various parameters in SDN based VANET. We emphasize the fact that SDN provides security solutions to VANET attacks, but it may bring new security threats to the network. In this paper, we have explored two perspectives: (a) solutions, which are provided to VANET security problems using SDN properties (b) threats, which may occur due to SDN properties. There are numerous issues including controller security, controller placement, heterogeneity, and network security in SDN based VANET on which, work can be extended by both researchers and industries. To the extent of our knowledge, this article presents a systematic and comprehensive survey of security issues of SDN based VANET by a thorough investigation of

every aspect. We finally depict the lessons learned through this survey, open research questions, and future directions relative to this subject to assist researchers and automotive industries.

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.

Acknowledgements

The authors would like to thank the Department of Computer science and Engineering and TEQIP-III, Malaviya National Institute of Technology Jaipur for providing research facilities to carry out the research work.

References

[1] S. Al-Sultan, M.M. Al-Doori, A.H. Al-Bayatti, H. Zedan, A comprehensive survey on vehicular ad hoc network, J. Netw. Comput. Appl. 37 (2014) 380–392.
[2] 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, 2004, pp. 19–28.
[3] M.N. Mejri, J. Ben-Othman, M. Hamdi, Survey on VANET security challenges and possible cryptographic solutions, Veh. Commun. 1 (2014) 53–66.
[4] 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.
[5] W. Liang, Z. Li, H. Zhang, S. Wang, R. Bie, Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends, Int. J. Distrib. Sens. Netw. 11 (2015) 745303.
[6] Q. Ding, B. Sun, X. Zhang, A traffic-light-aware routing protocol based on street connectivity for urban vehicular ad hoc networks, IEEE Commun. Lett. 20 (2016) 1635–1638.
[7] M. Kadadha, H. Otrok, H. Barada, M. Al-Qutayri, Y. Al-Hammadi, A Stackelberg game for street-centric QoS-OLSR protocol in urban vehicular ad hoc networks, Veh. Commun. 13 (2018) 64–77.
[8] M.A. Gawas, S.S. Govekar, A novel selective cross layer based routing scheme using ACO method for vehicular networks, J. Netw. Comput. Appl. 143 (2019) 34–46.
[9] O.A. Wahab, H. Otrok, A. Mourad, A Dempster–Shafer based tit-for-tat strategy to regulate the cooperation in VANET using QoS-OLSR protocol, Wirel. Pers. Commun. 75 (2014) 1635–1667.
[10] T. Halabi, M. Zulkernine, Trust-based cooperative game model for secure collaboration in the internet of vehicles, in: ICC 2019 - 2019 IEEE International Conference on Communications (ICC), IEEE, 2019, pp. 1–6.
[11] J. Bhatia, Y. Modi, S. Tanwar, M. Bhavsar, Software defined vehicular networks: a comprehensive review, Int. J. Commun. Syst. 32 (2019) e4005.
[12] S. Schaller, D. Hood, Software defined networking architecture standardization, Comput. Stand. Interfaces 54 (2017) 197–202.
[13] S. Saraswat, V. Agarwal, H.P. Gupta, R. Mishra, A. Gupta, T. Dutta, Challenges and solutions in software defined networking: a survey, J. Netw. Comput. Appl. 141 (2019) 23–58.
[14] 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), IEEE, 2014, pp. 103–110.
[15] 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 (2016) 2077.
[16] A. Akhunzada, M.K. Khan, Toward secure software defined vehicular networks: taxonomy, requirements, and open issues, IEEE Commun. Mag. 55 (2017) 110–118.
[17] H. Shafiq, R.A. Rehman, B.-S. Kim, Services and security threats in SDN based VANETs: a survey, Wirel. Commun. Mob. Comput. 2018 (2018).
[18] W.B. Jaballah, M. Conti, C. Lal, Security and design requirements for software-defined VANETs, Comput. Netw. (2020) 107099.
[19] D.B. Rawat, S.R. Reddy, Software defined networking architecture, security and energy efficiency: a survey, IEEE Commun. Surv. Tutor. 19 (2016) 325–346.
[20] M.W. Maier, D. Emery, R. Hilliard, Software architecture: introducing IEEE standard 1471, Computer 34 (2001) 107–109.
[21] M.W. Maier, D. Emery, R. Hilliard, ANSI/IEEE 1471 and systems engineering, Syst. Eng. 7 (2004) 257–270.
[22] D. Emery, R. Hilliard, Every architecture description needs a framework: expressing architecture frameworks using ISO/IEC 42010, in: 2009 Joint Working IEEE/IFIP Conference on Software Architecture & European Conference on Software Architecture, IEEE, 2009, pp. 31–40.
[23] T. Kosch, C. Schroth, M. Strassberger, M. Bechler, Automotive Internetworking, vol. 4, John Wiley & Sons, 2012.
[24] R. Naja, A survey of communications for intelligent transportation systems, in: Wireless Vehicular Networks for Car Collision Avoidance, Springer, 2013, pp. 3–35.
[25] J.-P. Hubaux, S. Capkun, J. Luo, The security and privacy of smart vehicles, IEEE Secur. Priv. 2 (2004) 49–55.
[26] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, T. Weil, Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards and solutions, IEEE Commun. Surv. Tutor. 13 (2011) 584–616.
[27] R. Baldessari, B. Bödekker, M. Deegener, A. Festag, W. Franz, C.C. Kellum, T. Kosch, A. Kovacs, M. Lenardi, C. Menig, et al., Car-2-car communication consortium-manifesto, in: IEEE Vehicular Technology Conference, Spring 2007.
[28] R.J. Bates, GPRS: General Packet Radio Service, McGraw-Hill Professional, 2001.
[29] M. Mouly, M.-B. Pautet, T. Foreword By-Haug, The GSM System for Mobile Communications, Telecom Publishing, 1992.
[30] Z. Abichar, Y. Peng, J.M. Chang, WiMAX: the emergence of wireless broadband, IT Prof. 8 (2006) 44–48.
[31] A. Samukic, UMTS universal mobile telecommunications system: development of standards for the third generation, IEEE Trans. Veh. Technol. 47 (1998) 1099–1104.
[32] C.C.C. Consortium, et al., C2C-CC manifesto, in: Overview of the C2C-CC System, 2007.
[33] O. Strobel, Communication in Transportation Systems, IGI Global, 2013.
[34] S.K. Bhoi, P.M. Khilar, Vehicular communication: a survey, IET Netw. 3 (2013) 204–217.
[35] R.F. Atallah, M.J. Khabbaz, C.M. Assi, Vehicular networking: a survey on spectrum access technologies and persisting challenges, Veh. Commun. 2 (2015) 125–149.
[36] Y.L. Morgan, Managing DSRC and wave standards operations in a V2V scenario, Int. J. Veh. Technol. 2010 (2010).
[37] H. Hasrouny, A.E. Samhat, C. Bassil, A. Laouiti, VANET security challenges and solutions: a survey, Veh. Commun. 7 (2017) 7–20.
[38] M. Zhou, L. Han, H. Lu, C. Fu, Distributed collaborative intrusion detection system for vehicular ad hoc networks based on invariant, Comput. Netw. (2020) 107174.
[39] O.A. Wahab, A. Mourad, H. Otrok, J. Bentahar, CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks, Expert Syst. Appl. 50 (2016) 40–54.
[40] D. Kosmanos, A. Pappas, L. Maglaras, S. Moschoyiannis, F.J. Aparicio-Navarro, A. Argyriou, H. Janicke, A novel intrusion detection system against spoofing attacks in connected electric vehicles, Array 5 (2020) 100013.
[41] A. Rasheed, S. Gillani, S. Ajmal, A. Qayyum, Vehicular ad hoc network (VANET): a survey, challenges, and applications, in: Vehicular Ad-Hoc Networks for Smart Cities, Springer, 2017, pp. 39–51.
[42] S. Sharma, B. Kaushik, A survey on internet of vehicles: applications, security issues & solutions, Veh. Commun. 20 (2019) 100182.
[43] A. Buchenscheit, F. Schaub, F. Kargl, M. Weber, A VANET-based emergency vehicle warning system, in: 2009 IEEE Vehicular Networking Conference (VNC), IEEE, 2009, pp. 1–8.
[44] R. Lu, X. Lin, H. Zhu, X. Shen, Spark: a new VANET-based smart parking scheme for large parking lots, in: IEEE INFOCOM 2009, IEEE, 2009, pp. 1413–1421.
[45] J. Zhu, Y. Feng, B. Liu, Pass: parking-lot-assisted carpool over vehicular ad hoc networks, Int. J. Distrib. Sens. Netw. 9 (2013) 491756.
[46] A. Kumar, N. Anusha, B.S.S.V. Prasad, Automatic toll payment, alcohol detection, load and vehicle information using internet of things & mailing system, in: 2017 International Conference on Intelligent Computing and Control (I2C2), IEEE, 2017, pp. 1–5.
[47] M. Barua, X. Liang, R. Lu, X.S. Shen, RCare: extending secure health care to rural area using VANETs, Mob. Netw. Appl. 19 (2014) 318–330.
[48] W. Almobaideen, R. Krayshan, M. Allan, M. Saadeh, Internet of things: geographical routing based on healthcare centers vicinity for mobile smart tourism destination, Technol. Forecast. Soc. Change 123 (2017) 342–350.
[49] N. Kumar, K. Kaur, S.C. Misra, R. Iqbal, An intelligent RFID-enabled authentication scheme for healthcare applications in vehicular mobile cloud, Peer-to-Peer Netw. Appl. 9 (2016) 824–840.
[50] J. Grover, M. Gaur, N. Prajapati, V. Laxmi, RSS-based Sybil attack detection in VANETs, in: Proceedings of the International Conference TENCON2010, IEEE, 2010, pp. 2278–2283.
[51] J. Grover, M.S. Gaur, V. Laxmi, Multivariate verification for Sybil attack detection in VANET, Open Comput. Sci. 1 (2015).
[52] W. Bouksani, B.A. Bensaber, RIN: a dynamic pseudonym change system for privacy in VANET, Concurr. Comput. 31 (2019) e4719.
[53] H.M. Song, J. Woo, H.K. Kim, In-vehicle network intrusion detection using deep convolutional neural network, Veh. Commun. 21 (2020) 100198.
[54] J. Guo, X. Li, Z. Liu, J. Ma, C. Yang, J. Zhang, D. Wu, Trove: a context awareness trust model for VANETs using reinforcement learning, IEEE Int. Things J. 7 (7) (2020) 6647–6662, https://doi.org/10.1109/JIOT.2020.2975084.

[55] J. Kamel, M.R. Ansari, J. Petit, A. Kaiser, I.B. Jemaa, P. Urien, Simulation framework for misbehavior detection in vehicular networks, IEEE Trans. Veh. Technol. 69 (6) (2020) 6631–6643, https://doi.org/10.1109/TVT.2020.2984878.

[56] E. Haleplidis, K. Pentikousis, S. Denazis, J.H. Salim, D. Meyer, O. Koufopavlou, Software-defined networking (SDN): layers and architecture terminology, in: RFC 7426, IRTF, 2015.

[57] OpenFlow Switch v 1.5.1, https://www.opennetworking.org/, 2020.

[58] F. Hu, Q. Hao, K. Bao, A survey on software-defined network and OpenFlow: from concept to implementation, IEEE Commun. Surv. Tutor. 16 (2014) 2181–2206.

[59] M. Mousa, A.M. Bahaa-Eldin, M. Sobh, Software defined networking concepts and challenges, in: 2016 11th International Conference on Computer Engineering & Systems (ICCES), IEEE, 2016, pp. 79–90.

[60] M.S. Todorova, S.T. Todorova, Ddos attack detection in sdn-based vanet architectures, June 2016, 175, http://projekter.aau.dk/projekter/files/239545035/Master_Thesis___DDoS_Attack_Detection_in_SDN_based_VANET_Architectures__group_1097.pdf.

[61] W. Xia, Y. Wen, C.H. Foh, D. Niyato, H. Xie, A survey on software-defined networking, IEEE Commun. Surv. Tutor. 17 (2014) 27–51.

[62] A. Shaghaghi, M.A. Kaafar, R. Buyya, S. Jha, Software-defined network (SDN) data plane security: issues, solutions, and future directions, in: Handbook of Computer Networks and Cyber Security, Springer, 2020, pp. 341–387.

[63] A. Jalili, H. Nazari, S. Namvarasl, M. Keshtgari, A comprehensive analysis on control plane deployment in SDN: in-band versus out-of-band solutions, in: 2017 IEEE 4th International Conference on Knowledge-Based Engineering and Innovation (KBEI), IEEE, 2017, pp. 1025–1031.

[64] R. Masoudi, A. Ghaffari, Software defined networks: a survey, J. Netw. Comput. Appl. 67 (2016) 1–25.

[65] Y. Jarraya, T. Madi, M. Debbabi, A survey and a layered taxonomy of software-defined networking, IEEE Commun. Surv. Tutor. 16 (2014) 1955–1980.

[66] M. Jammal, T. Singh, A. Shami, R. Asal, Y. Li, Software defined networking: state of the art and research challenges, Comput. Netw. 72 (2014) 74–98.

[67] L. Fang, F. Chiussi, D. Bansal, V. Gill, T. Lin, J. Cox, G. Ratterree, Hierarchical SDN for the hyper-scale, hyper-elastic data center and cloud, in: Proceedings of the 1st ACM SIGCOMM Symposium on Software Defined Networking Research, 2017, pp. 1–13.

[68] F. Paolucci, F. Civerchia, A. Sgambelluri, A. Giorgetti, F. Cugini, P. Castoldi, P4 edge node enabling stateful traffic engineering and cyber security, J. Opt. Commun. Netw. 11 (2019) A84–A95.

[69] X. Zhu, C. Chang, Q. Xi, Z. Zuo, Attribute-guard: attribute-based flow access control framework in software-defined networking, Secur. Commun. Netw. 2020 (2020).

[70] T. Zhang, A. Bianco, P. Giaccone, A.P. Nezhad, Dealing with misbehaving controllers in SDN networks, in: GLOBECOM 2017 - 2017 IEEE Global Communications Conference, IEEE, 2017, pp. 1–6.

[71] S. Gyawali, Y. Qian, Misbehavior detection using machine learning in vehicular communication networks, in: ICC 2019 - 2019 IEEE International Conference on Communications (ICC), IEEE, 2019, pp. 1–6.

[72] H. Farhady, H. Lee, A. Nakao, Software-defined networking: a survey, Comput. Netw. 81 (2015) 79–95.

[73] R. Saunders, J. Cho, A. Banerjee, F. Rocha, J. Van der Merwe, P2P offloading in mobile networks using SDN, in: Proceedings of the Symposium on SDN Research, 2016, pp. 1–7.

[74] J.H. Jafarian, E. Al-Shaer, Q. Duan, OpenFlow random host mutation: transparent moving target defense using software defined networking, in: Proceedings of the First Workshop on Hot Topics in Software Defined Networks, 2012, pp. 127–132.

[75] A. Rego, L. Garcia, S. Sendra, J. Lloret, Software defined network-based control system for an efficient traffic management for emergency situations in smart cities, Future Gener. Comput. Syst. 88 (2018) 243–253.

[76] L. Ben Azzouz, I. Jamai, SDN, slicing, and NFV paradigms for a smart home: a comprehensive survey, Trans. Emerg. Telecommun. Technol. 30 (2019) e3744.

[77] S. Panev, P. Latkoski, SDN-based failure detection and recovery mechanism for 5G core networks, Trans. Emerg. Telecommun. Technol. 31 (2020) e3721.

[78] C. Wang, L. Zhang, Z. Li, C. Jiang, SDCoR: Software defined cognitive routing for internet of vehicles, IEEE Int. Things J. 5 (2018) 3513–3520.

[79] C. Jiacheng, Z. Haibo, Z. Ning, Y. Peng, G. Lin, S. Xuemin, Software defined internet of vehicles: architecture, challenges and solutions, J. Commun. Inf. Netw. 1 (2016) 14–26.

[80] L. Nkenyereye, L. Nkenyereye, S. Islam, Y.-H. Choi, M. Bilal, J.-W. Jang, Software-defined network-based vehicular networks: a position paper on their modeling and implementation, Sensors 19 (2019) 3788.

[81] F. Al-Turjman, A. Malekloo, Smart parking in IoT-enabled cities: a survey, Sustain. Cities Soc. (2019) 101608.

[82] Software-defined networking (SDN) | Nuage networks, https://www.nuagenetworks.net/, 2011.

[83] N. Dogru, A. Subasi, Traffic accident detection using random forest classifier, in: 2018 15th Learning and Technology Conference (L&T), IEEE, 2018, pp. 40–45.

[84] K. Halba, C. Mahmoudi, In-vehicle software defined networking: an enabler for data interoperability, in: Proceedings of the 2nd International Conference on Information System and Data Mining, 2018, pp. 93–97.

[85] 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 (2017) 87–93.

[86] K. Liu, J.K. Ng, V.C. 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 (2015) 1759–1773.

[87] Z. He, J. Cao, X. Liu, SDVN: enabling rapid network innovation for heterogeneous vehicular communication, IEEE Netw. 30 (2016) 10–15.

[88] Z. He, D. Zhang, J. Liang, Cost-efficient sensory data transmission in heterogeneous software-defined vehicular networks, IEEE Sens. J. 16 (2016) 7342–7354.

[89] M. Chahal, S. Harit, Network selection and data dissemination in heterogeneous software-defined vehicular network, Comput. Netw. 161 (2019) 32–44.

[90] A. Kazmi, M.A. Khan, M.U. Akram, DeVANET: decentralized software-defined VANET architecture, in: 2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW), IEEE, 2016, pp. 42–47.

[91] A. Alioua, S.-M. Senouci, S. Moussaoui, H. Sedjelmaci, A. Boualouache, Software-defined heterogeneous vehicular networks: taxonomy and architecture, in: 2017 Global Information Infrastructure and Networking Symposium (GIIS), IEEE, 2017, pp. 50–55.

[92] S. Correia, A. Boukerche, R.I. Meneguette, An architecture for hierarchical software-defined vehicular networks, IEEE Commun. Mag. 55 (2017) 80–86.

[93] J.R. Singh, A. Kumar, D. Singh, R.K. Dewang, A single-hop based fast certificate revocation protocol in VANET, in: 2016 2nd International Conference on Computational Intelligence and Networks (CINE), IEEE, 2016, pp. 23–28.

[94] A. Alrawais, A. Alhothaily, B. Mei, T. Song, X. Cheng, An efficient revocation scheme for vehicular ad-hoc networks, Proc. Comput. Sci. 129 (2018) 312–318.

[95] M. Dabbagh, B. Hamdaoui, M. Guizani, A. Rayes, Software-defined networking security: pros and cons, IEEE Commun. Mag. 53 (2015) 73–79.

[96] E.S. Pilli, R.C. Joshi, R. Niyogi, Network forensic frameworks: survey and research challenges, Digit. Investig. 7 (2010) 14–27.

[97] I. Ahmad, S. Namal, M. Ylianttila, A. Gurtov, Security in software defined networks: a survey, IEEE Commun. Surv. Tutor. 17 (2015) 2317–2346.

[98] S. Scott-Hayward, S. Natarajan, S. Sezer, A survey of security in software defined networks, IEEE Commun. Surv. Tutor. 18 (2015) 623–654.

[99] A.K. Malhi, S. Batra, H.S. Pannu, Security of vehicular ad-hoc networks: a comprehensive survey, Comput. Secur. (2019) 101664.

[100] R.G. Engoulou, M. Bellaïche, S. Pierre, A. Quintero, VANET security surveys, Comput. Commun. 44 (2014) 1–13.

[101] B. Mokhtar, M. Azab, Survey on security issues in vehicular ad hoc networks, Alex. Eng. J. 54 (2015) 1115–1126.

[102] M. Kim, A survey of vehicular ad-hoc network security, in: International Conference on Mobile and Wireless Technology, Springer, 2017, pp. 315–326.

[103] M.R. Ghori, K.Z. Zamli, N. Quosthoni, M. Hisyam, M. Montaser, Vehicular ad-hoc network (VANET), in: 2018 IEEE International Conference on Innovative Research and Development (ICIRD), IEEE, 2018, pp. 1–6.

[104] M. Arif, G. Wang, M.Z.A. Bhuiyan, T. Wang, J. Chen, A survey on security attacks in VANETs: communication, applications and challenges, Veh. Commun. (2019) 100179.

[105] A. Akhunzada, A. Gani, N.B. Anuar, A. Abdelaziz, M.K. Khan, A. Hayat, S.U. Khan, Secure and dependable software defined networks, J. Netw. Comput. Appl. 61 (2016) 199–221.

[106] S.T. Ali, V. Sivaraman, A. Radford, S. Jha, A survey of securing networks using software defined networking, IEEE Trans. Reliab. 64 (2015) 1086–1097.

[107] R. Raiya, S. Gandhi, Survey of various security techniques in VANET, Int. J. Adv. Res. Comput. Sci. Softw. Eng. 4 (2014).

[108] M.S. Al-Kahtani, Survey on security attacks in vehicular ad hoc networks (VANETs), in: 2012 6th International Conference on Signal Processing and Communication Systems, IEEE, 2012, pp. 1–9.

[109] A. Rao, A. Sangwan, A.A. Kherani, A. Varghese, B. Bellur, R. Shorey, Secure V2V communication with certificate revocations, in: 2007 Mobile Networking for Vehicular Environments, IEEE, 2007, pp. 127–132.

[110] M. Raya, P. Papadimitratos, J.-P. Hubaux, Securing vehicular communications, IEEE Wirel. Commun. 13 (2006) 8–15.

[111] R.S. Raw, M. Kumar, N. Singh, Security challenges, issues and their solutions for VANET, Int. J. Netw. Secur. Appl. 5 (2013) 95.

[112] Y.-C. Hu, A. Perrig, D.B. Johnson, Ariadne: a secure on-demand routing protocol for ad hoc networks, Wirel. Netw. 11 (2005) 21–38.

[113] Z. Zhang, S. Liu, Y. Bai, Y. Zheng, M optimal routes hops strategy: detecting sinkhole attacks in wireless sensor networks, Clust. Comput. 22 (2019) 7677–7685.

[114] S. Vidhya, T. Sasilatha, Sinkhole attack detection in WSN using pure MD5 algorithm, Indian J. Sci. Technol. 10 (2017) 24.

[115] V.H. La, A.R. Cavalli, Security attacks and solutions in vehicular ad hoc networks: a survey, Int. J. Ad Hoc Netw. Syst. 4 (2) (2014) 1–20, https://doi.org/10.5121/ijans.2014.4201.

[116] N.J. Patel, R.H. Jhaveri, Trust based approaches for secure routing in VANET: a survey, Proc. Comput. Sci. 45 (2015) 592–601.
[117] 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), IEEE, 2014, pp. 13–18.
[118] M.N. Mejri, J. Ben-Othman, GDVAN: a new greedy behavior attack detection algorithm for VANETs, IEEE Trans. Mob. Comput. 16 (2016) 759–771.
[119] A.M. Malla, R.K. Sahu, Security attacks with an effective solution for dos attacks in VANET, Int. J. Comput. Appl. 66 (2013).
[120] J.T. Isaac, S. Zeadally, J.S. Camara, Security attacks and solutions for vehicular ad hoc networks, IET Commun. 4 (2010) 894–903.
[121] M. Sun, M. Li, R. Gerdes, A data trust framework for VANETs enabling false data detection and secure vehicle tracking, in: 2017 IEEE Conference on Communications and Network Security (CNS), IEEE, 2017, pp. 1–9.
[122] L. He, W.T. Zhu, Mitigating dos attacks against signature-based authentication in VANETs, in: 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE), vol. 3, IEEE, 2012, pp. 261–265.
[123] T. ETSI, 102 893 v1.1.1, ITS-Security-Threat, Vulnerability and Risk Analysis, 2010.
[124] Y. Qian, N. Moayeri, Design of secure and application-oriented VANETs, in: VTC Spring 2008 - IEEE Vehicular Technology Conference, IEEE, 2008, pp. 2794–2799.
[125] S. Ahmed, M.U. Rehman, A. Ishtiaq, S. Khan, A. Ali, S. Begum, VANSec: attack-resistant VANET security algorithm in terms of trust computation error and normalized routing overhead, J. Sens. 2018 (2018).
[126] H. Sedjelmaci, S.M. Senouci, M.A. Abu-Rgheff, An efficient and lightweight intrusion detection mechanism for service-oriented vehicular networks, IEEE Int. Things J. 1 (2014) 570–577.
[127] A. Dahiya, V. Sharma, A survey on securing user authentication in vehicular ad hoc networks, Int. J. Inf. Secur. 1 (2001) 164–171.
[128] M.G. Zapata, Secure ad hoc on-demand distance vector routing, ACM SIGMOBILE Mob. Comput. Commun. Rev. 6 (2002) 106–107.
[129] S.S. Tangade, S.S. Manvi, A survey on attacks, security and trust management solutions in VANETs, in: 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), IEEE, 2013, pp. 1–6.
[130] M.-C. Chuang, J.-F. Lee, TEAM: trust-extended authentication mechanism for vehicular ad hoc networks, IEEE Syst. J. 8 (2013) 749–758.
[131] C.D. Jung, C. Sur, Y. Park, K.-H. Rhee, A robust conditional privacy-preserving authentication protocol in VANET, in: International Conference on Security and Privacy in Mobile Information and Communication Systems, Springer, 2009, pp. 35–45.
[132] B. Yu, C.-Z. Xu, B. Xiao, Detecting Sybil attacks in VANETs, J. Parallel Distrib. Comput. 73 (2013) 746–756.
[133] T. Zhou, R.R. Choudhury, P. Ning, K. Chakrabarty, P2DAP—Sybil attacks detection in vehicular ad hoc networks, IEEE J. Sel. Areas Commun. 29 (2011) 582–594.
[134] C. Zhang, K. Chen, X. Zeng, X. Xue, Misbehavior detection based on support vector machine and Dempster-Shafer theory of evidence in VANETs, IEEE Access 6 (2018) 59860–59870.
[135] R. Skowyra, S. Bahargam, A. Bestavros, Software-defined ids for securing embedded mobile devices, in: 2013 IEEE High Performance Extreme Computing Conference (HPEC), IEEE, 2013, pp. 1–7.
[136] R. Braga, E. Mota, A. Passito, Lightweight DDoS flooding attack detection using NOX/OpenFlow, in: IEEE Local Computer Network Conference, IEEE, 2010, pp. 408–415.
[137] S.A. Mehdi, J. Khalid, S.A. Khayam, Revisiting traffic anomaly detection using software defined networking, in: International Workshop on Recent Advances in Intrusion Detection, Springer, 2011, pp. 161–180.
[138] T. Xing, D. Huang, L. Xu, C.-J. Chung, P. Khatkar, SnortFlow: a OpenFlow-based intrusion prevention system in cloud environment, in: 2013 Second GENI Research and Educational Experiment Workshop, IEEE, 2013, pp. 89–92.
[139] R. Meyran, DefenseFlow: the first ever SDN application that programs networks for DoS/DDoS security, Retrieved March 10, 2016.
[140] 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, IEEE, 2015, pp. 239–250.
[141] X. Lin, X. Sun, P.-H. Ho, X. Shen, GSIS: a secure and privacy-preserving protocol for vehicular communications, IEEE Trans. Veh. Technol. 56 (2007) 3442–3456.
[142] 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 (2015) 2681–2691.
[143] H. Li, P. Li, S. Guo, S. Yu, Byzantine-resilient secure software-defined networks with multiple controllers, in: 2014 IEEE International Conference on Communications (ICC), IEEE, 2014, pp. 695–700.
[144] P. Porras, S. Shin, V. Yegneswaran, M. Fong, M. Tyson, G. Gu, A security enforcement kernel for OpenFlow networks, in: Proceedings of the First Workshop on Hot Topics in Software Defined Networks, 2012, pp. 121–126.
[145] H. Shafiei, A. Khonsari, H. Derakhshi, P. Mousavi, Detection and mitigation of sinkhole attacks in wireless sensor networks, J. Comput. Syst. Sci. 80 (2014) 644–653.
[146] Q. Yan, F.R. Yu, Distributed denial of service attacks in software-defined networking with cloud computing, IEEE Commun. Mag. 53 (2015) 52–59.
[147] S. Hong, L. Xu, H. Wang, G. Gu, Poisoning network visibility in software-defined networks: new attacks and countermeasures, in: NDSS, vol. 15, 2015, pp. 8–11.
[148] M. Dhawan, R. Poddar, K. Mahajan, V. Mann, Sphinx: detecting security attacks in software-defined networks, in: NDSS, vol. 15, 2015, pp. 8–11.
[149] T.-H. Nguyen, M. Yoo, A behavior-based mobile malware detection model in software-defined networking, in: 2017 International Conference on Information Science and Communications Technologies (ICISCT), IEEE, 2017, pp. 1–3.
[150] M. Ambrosin, M. Conti, F. De Gaspari, R. Poovendran, LineSwitch: tackling control plane saturation attacks in software-defined networking, IEEE/ACM Trans. Netw. 25 (2016) 1206–1219.
[151] G. Shang, P. Zhe, X. Bin, H. Aigun, R. Kui, FloodDefender: protecting data and control plane resources under SDN-aimed dos attacks, in: IEEE INFOCOM 2017 - IEEE Conference on Computer Communications, IEEE, 2017, pp. 1–9.
[152] 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 & Security in Wireless and Mobile Networks, 2005, pp. 71–78.
[153] 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, IEEE, 2017, pp. 1–6.
[154] 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, IEEE, 2008, pp. 1–6.
[155] 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), IEEE, 2017, pp. 1–7.
[156] J. François, O. Festor, Anomaly traceback using software defined networking, in: 2014 IEEE International Workshop on Information Forensics and Security (WIFS), IEEE, 2014, pp. 203–208.
[157] K. Benzekki, A. El Fergougui, A. Elbelrhiti Elalaoui, Software-defined networking (sdn): a survey, Secur. Commun. Netw. 9 (2016) 5803–5833.
[158] M. Kim, I. Jang, S. Choo, J. Koo, S. Pack, Collaborative security attack detection in software-defined vehicular networks, in: 2017 19th Asia-Pacific Network Operations and Management Symposium (APNOMS), IEEE, 2017, pp. 19–24.
[159] G. de Biasi, L.F. Vieira, A.A. Loureiro, Sentinel: defense mechanism against DDoS flooding attack in software defined vehicular network, in: 2018 IEEE International Conference on Communications (ICC), IEEE, 2018, pp. 1–6.
[160] Y. Yahiatene, A. Rachedi, Towards a blockchain and software-defined vehicular networks approaches to secure vehicular social network, in: 2018 IEEE Conference on Standards for Communications and Networking (CSCN), IEEE, 2018, pp. 1–7.
[161] H. Vasudev, D. Das, A trust based secure communication for software defined VANETs, in: 2018 International Conference on Information Networking (ICOIN), IEEE, 2018, pp. 316–321.
[162] D. Zhang, F.R. Yu, R. Yang, A machine learning approach for software-defined vehicular ad hoc networks with trust management, in: 2018 IEEE Global Communications Conference (GLOBECOM), IEEE, 2018, pp. 1–6.