Review on Software-Defined Vehicular Networks (SDVN)

Badiea Abdulkarem Mohammed[1†],
b.alshaibani@uoh.edu.sa
University of Ha'il, College of Computer Science and Engineering, Ha'il 81481, Saudi Arabia

Abstract
The expansion of new applications and business models is being significantly fueled by the development of Fifth Generation (5G) networks, which are becoming more widely accessible. The creation of the newest intelligent vehicular networks and applications is made possible by the use of Vehicular Ad hoc Networks (VANETs) and Software Defined Networking (SDN). Researchers have been concentrating on the integration of SDN and VANET in recent years, and they have examined a variety of issues connected to the architecture, the advantages of software-defined VANET services, and the new features that can be added to them. However, the overall architecture's security and robustness are still in doubt and have received little attention. Furthermore, new security threats and vulnerabilities are brought about by the deployment and integration of novel entities and a number of architectural components. In this study, we comprehensively examine the good and negative effects of the most recent SDN-enabled vehicular network topologies, focusing on security and privacy. We examine various security flaws and attacks based on the existing SDVN architecture. Finally, a thorough discussion of the unresolved concerns and potential future study directions is provided.
Keywords:
SDN, VANET, SDVN, Security.

1. Introduction

Vehicular communications are specified as technologies that make use of the latest wireless network generation to enable vehicle-to-vehicle communication via a wireless network [1-6]. Just a few of the benefits of vehicular ad hoc network (VANET) include increased in-vehicle entertainment, improved road safety, and emergency warnings. Due of issues with road mobility, an increasing many of human are getting interested in vehicular communications. The main application of VANETs is in systems of intelligent transportation (ITS) [7-8]. The two main kinds of ITS applications are those for entertainment and transportation safety.

Avoidance of congestion, management of traffic, routing, transfer of data, and control of traffic signal are a few examples of the former [9-10].

The latter offers, among other things, gaming and Internet access. The development of reliable and effective vehicle traffic data transmission is the subject of the most important study in the VANET field [11–14]. Due to its success in applications like traffic safety, many researchers are looking into the usefulness of VANET and routing based on position using routing of geocast [15-16].

The rest of the paper is arranged as follows. Section II provides the background of this paper. Section III describes SDVN technology in details. Section IV reviews the related SDVN research. Section V disuses future research direction. Finally, this paper is concluded in Section VI.

2. Related Literature

2.1 Software-Defined Networking (SDN) Technology

Simply said, Software Defined Networks (SDN) refers to an architecture that makes networks more manageable, affordable, dynamic, and flexible, making it the best choice for applications used today [17-18]. SDN offers a solution to such problems in contrast to the drawbacks and restrictions of existing network typologies. The first solution is that SDN separates the data plane, or the underpinning switches and routers that pass on traffic, from the control plane, or the network's control logic [19-20].

The second option is to separate from the data plane to the control plane, which reduces network switches to simple data-forwarding devices that can be used to apply control logic through a logically centralised controller. While network routers and switches only forward traffic in accordance with the controller's installed rules, this controller defines how traffic will flow in a network [21-22]. The SDN design makes network management simpler by allowing for communication between the control plane and the data plane and application plane, respectively. Northbound Interface (NBI) and Southbound Interface (SBI) are used for this.

2.1.1 SDN Architecture

The core idea of the SDN system is presented in Figure 1. This requirement helps the deployment of modern routing

Manuscript received September 5, 2022
Manuscript revised September 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.9.50

management and protocols without imposing any policies or protocols on all of the network's connected devices, which aids in the introduction of new routing protocols and management [23-24].

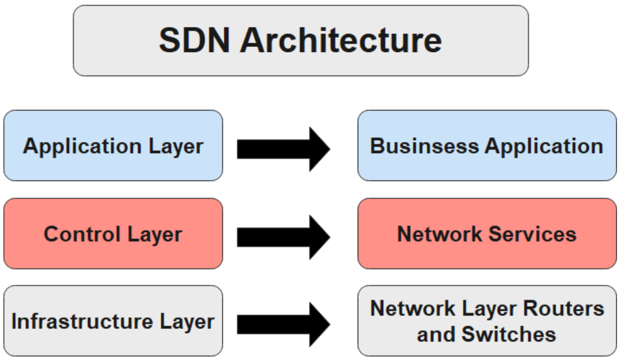

Figure 1 Structure of SDN.

- Infrastructure Layer: Devices that forward and filter packets, including routers, firewalls, switches, intrusion detection systems (IDS), computers, and other internetworking devices, are housed under the infrastructure layer. One of the key duties of the data layer is data transfer. Other duties include surveillance of local network, filtering of information packet and statistics of flow.

- Control Layer: The forwarding plane's configuration is handled by this layer. The data layer identifies the network components of the southbound interface. It determines and makes decisions on the programming, flow tables, and transmission logic on the data layer. Because it serves as the network's central nervous system, it is often referred to as a network operating system.

- Application Layer: Network applications that add modern characteristics and requirements, such as numerous new security regulations and standards of network performance, reside in this layer. The control layer can configure the network to achieve these needs with the use of these features. The application layer has comprehensive visibility into the entire global network, which aids it in making recommendations for a range of various application regulations and rules.

2.1.2 SDN Characteristics

Many of the problems associated with traditional networks are solved by SDN. It contains a number of traits and features that make network operation and design easier. The key SDN characteristics that affect its operation and security are described as follows.

- Control that is logically centralised and network-wide visibility: A controller that is conceptually centralised but physically dispersed is a crucial functionality offered by SDN. The standard southbound interface is used in the SDN architecture to distribute all network control capabilities from the forwarding plane. Older controller versions include NOX [25], Floodlight [26], [27], and Beacon [28]. They carried out the role of an OpenFlow [29] driver. On the other hand, more recent controller implementations, such as OpenDaylight [27] and OpenContrail [30], offer an update on the necessary abstractions for the network services. To manage the various forwarding devices, they now support a variety of programming interfaces.

- Abstraction: One of the most notable features of the SDN network is abstraction through the various layers. An SDN arrangement lessens the burden on the programmer when the layers are interfaced using APIs. Using high level policy languages like Voellmy and Hudak [31] network software and apps can change the network's behaviour based on their specifications. Some of the most widely used abstraction tools are frenetic [32] and pyretic [33].

- Network Dynamism and Automation: SDN provides adaptability to manage complicated transitions, enhancing dynamicity. Data layer devices are easily reconfigurable based on the shifting network status and conditions. In data centres and across the network of service providers, it enables the implementation and deployment of ondemand network and security applications.

- Virtualization: The sharing and adaptation of physical infrastructures between numerous users in distinct networks is a requirement for SDN virtualization. Multi-tenancy in the network architecture is supported by virtualizing the SDN framework's component parts. The majority of SDN networks use VMware's Networking Virtualization Proxy (NVP) [34] and IBM's SDNVE [35].

- Flow Management: The fundamental unit of traffic in the network is the flow. An item in the flow table of an SDN switch is known as a flow rule or flow entry. An SDN device's main data structure is the flow table. A flow rule, which is separated into several categories, can be used to regulate the birds in a network.

  - Flow match fields: utilised as identifiers to differentiate between various flows.

  - Flow priority: utilised to establish the sequence in which the flow rules will be carried out.

- Flow action: a series of procedures that either change or forward the flow.

- Anomaly Detection: The main area of worry in any network is security. It is considerably simpler to attack the controllers in the case of SDN and its centralised control feature employing attacks such as DOS (denial of service) assaults, phoney packet insertion, running unauthorised programmes on the centralised SDN controller, malicious traffic insertion, etc. Attacks today are more sophisticated.
- Switch Management Protocol (SMP): The southbound interface must be used to programme any switches that are part of the data layer because they all forward network traffic. Through a standardised interface, the SDN controller configures these switches. The SDN controller must have a companion interface that serves as a programmable interface in order to talk to the network switches.
- Open Programmable Interfaces (OPI): The control layer and the data layer are not separate in conventional networks. The control layer and data layer are closely connected in conventional networks. The SDN architecture offered this feature. SDN networks separate the aforementioned two layers. This functionality was primarily developed to make forwarding devices simpler and enable autonomous network software evolution within the SDN controller. This feature boosts the likelihood of innovation and makes it simple to integrate new solutions into the network. The controller's applications are in charge of controlling the data layer's devices.

2.1.3 SDN Attacks

Any network's primary concern should be security. Any network's security is evaluated according to how well it can both stop and mitigate security risks in the event of a successful intrusion. Numerous threats that can be categorised as scanning attacks, malware, social engineering attacks, spoofing attacks, network-level DoS attacks, sniffng attacks, web application assaults, and others are present in SDN networks.

- DDoS: SDN networks have a number of benefits, but they also have certain security issues. Attacks using distributed denial of service (DDoS) are quite capable of affecting network components like the controller or switch.

- IP Spoofing: An attacker uses IP spoofing to target a victim by sending erroneous packets to them. In order to get access to the victim's network or system, the attacker must trick and persuade the targeted network that the packets are secure, reliable, and allowed.

- Drive-by-Download: Internet users click on various links and visit a range of web pages while they browse. An attacker attempting to exploit the drive-by-download attack model could create any of these links. Such a perpetrator intends to introduce harmful and unsafe scripts into unsafe and illegal websites.

- Vulnerability Scanner: A vulnerability scanner, as the name implies, creates tools that scan networks, find potential security holes, and attack those holes. The attacker sends these scanning packets straight to the network. If the targeted network has no protections against these vulnerabilities, the vulnerability scanner starts maliciously exploiting it.

- Malware Controller: Malware is defined as any piece of source code, file, application, or software that seeks to carry out harmful tasks like secretly opening backdoors, erasing crucial files, impersonating a DDoS agent, downloading additional malware, spying, etc. Such malicious software is already installed on the victim network utilising C&C servers.

- Phishing: In the case of phishing, the attacker makes advantage of channels like emails, SMS, and tweets and presents them falsely as coming from a reliable source. These communications occasionally contain malicious attachments that, when opened by the recipient, cause malware to be installed on the recipient's device.

- Eavesdropper: Networks are inherently static. This makes it much simpler for an attacker to use the eavesdropper attack model to compromise the victim's security and privacy. An eavesdropper attack is a popular option for attackers due of its simplicity.

2.2 Vehicular Ad-hoc Network (VANET) Technology

Ad hoc networks, VANETs are highly dynamic, have limited access to the network infrastructure, and provide a variety of services. The three types of communication in the VANET depicted in Figure 2 are Vehicle to Infrastructure (V2I), Vehicle to Vehicle (V2V) and Hybrid. The communication medium utilised in V2V is distinguished by its minimal latency and high transmission rate. This architecture is utilised in cooperative driving situations as well as various broadcasting alarm scenarios (emergency braking, accident, deceleration, etc.). The vehicular network in V2I considers the applications that make use of the RSUs that multiply the services provided by internet portals. In hybrid mode, the two earlier methods are combined.

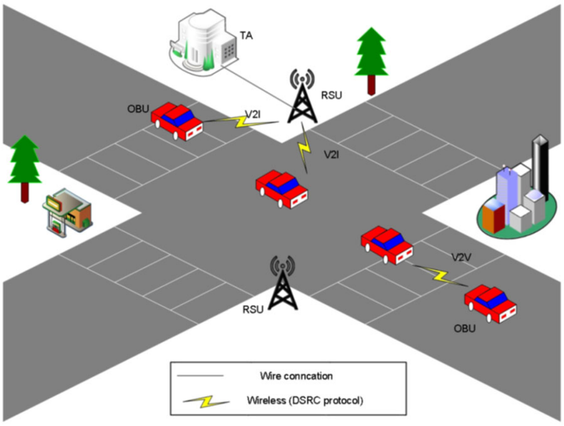

Figure 2 Structure of VANET.

A particular kind of mobile ad-hoc network called VANET has pre-established routes (roads). Roadside units (RSUs) and On-Board units, which are specific authority for registration and control, are used (OBUs). To provide specialised services, RSUs are widely dispersed around the boundaries of the roads, and OBUs are installed in the vehicles using VANET. All vehicles are travelling freely and communicating with each other, with RSUs, and with specific authorities on the road network.

VANET Characteristics: The characteristics of the VANET discussed in [36–40]. VANET discussion was categorised as either: (I) Network architecture and communication mode, or (II) Vehicles and drivers.

(I) Network architecture and communication mode 2.2 SDN Characteristics:

- Unbounded and scalable network: One or more cities, or even entire nations, can utilise VANET. Consequently, management and coordination are needed for security requirements [41-42].
- Wireless communication: Wireless channels are used for the nodes' connection and data exchange, hence necessitates safer communication [43-44].
- High mobility and rapidly changing network topology: It is more difficult to forecast node positions and network topology because of the nodes' high/random speed movement. Increasing node privacy while producing frequent disconnections, instability, and handshake impossibilities [45-46].
- It is advised to support real-time and multimedia applications in addition to dependability and cross-layer communication between the transport and network layers [47-48].

(II) Vehicles and drivers [49].

- High processing power and sufficient energy: Energy and computing resources are not a concern for VANET nodes. They are self-powered by batteries and have powerful computers that can do intricate cryptographic calculations.
- Better physical protection: VANET nodes are more physically secure. Physical compromise is more difficult to come by. Consequently, mitigate the impact of infrastructure attacks.
- Known time and position: Due to the fact that many applications depend on location and geographic addressing or area, the majority of automobiles are GPS-equipped. In order to safeguard the location of nodes from attackers, a tamper-proof GPS is deployed.
- The majority of participants are honest: Most drivers are believed to be honest and helpful in locating the enemy.
- Existing law enforcement infrastructure: They can apprehend the enemy who attacked the system by using the law enforcement personnel.
- Central registration with periodic maintenance and inspection: Vehicles have unique identifiers and are registered with the central authority (license plate). Firmware and software updates are part of routine vehicle maintenance.

2.3 SDN Integration with Emerging Technologies

This section provide a summary of many of the technologies is given along with recommendations for further SDN study to enhance at least one part of their usefulness [50–52].

- Internet of Things: Because it opens up new possibilities, IoT is a crucial technology for vehicle networks [53], [54]. It has been successful to combine network resources with the Internet of Things (IoT) [55]. The scenario [56], which made use of a pilot set of users, combined the SDN prototype with IoT.

- Blockchain: Blockchain technology has been mentioned as a key component of Bitcoin [57]. Cryptocurrency Blockchain technology is a crucial component of Bitcoin. An open-access chain of blocks is produced in a blockchain using a cryptographic hashing method. A perfect blockchain is kept up to date by a select few people, as stated in [58]. This method allows users to maintain track of the transactions they have performed. For instance, this kind of technology is used to implement SDVNs [59], 5G [60], and the Internet of Things [61]. [62–64] provides an explanation of blockchain technology.

- 5G/6G: Vehicle networks might leverage ML applications like quick channel equalisation and flexible resource allocation [52, 65, 66]. On the other side, SDN enables a more adaptable use of the 5G and 6G technologies. To accomplish the 6G goals, five generations of novel strategies are offered, including NFV, reactive vehicle system control, and cognitive radios. The first of these to be applied are NFV, reactive vehicular system control, and cognitive radios.

3. Software-Defined Vehicular Networks (SDVN) Technology

Regarding the potential of SDN to redesign automotive network infrastructure, some are hopeful. In recent years, SDN has established itself as a dependable method of network management. OpenFlow is used by SDN (softwaredefined networking) to communicate across the control and data planes. The versatility of SDN performs admirably in VANET applications. Ad hoc wireless networks of the present are centralised, rigid, and unprogrammable. Applying SDN principles to VANETs is one option to ease the restrictions placed on them. Network organisation, new V2V and V2I services, and easier network management are all benefits of VANET networks, which are built on SDN. The disconnectivity brought on by vehicle movement is reduced by the SDNVN architecture, and overall connectivity is enhanced. Three key components of an SDN-integrated VANET are described in the sections that follow (Figure 3).

Appropriate path: More precise routing decisions can be made with SDN in VANET. Data flow may slow down or get crowded in VANET settings. When all nodes seek to take the shortest path, some nodes get incredibly crowded. The controller can restart the process that is currently executing as soon as it recognises one of the aforementioned instances, improving the network's efficiency and lowering blockages.

- Channel/frequency: Different wireless interfaces or adjustable radios are now available thanks to SDN integration in VANET (e.g., cognitive radios). The controller will decide on the fly, for example, in the case of the radio interface. It enables the run-time selection of radio frequencies for various sorts of traffic. In this endeavour, emergency services are the main priority.

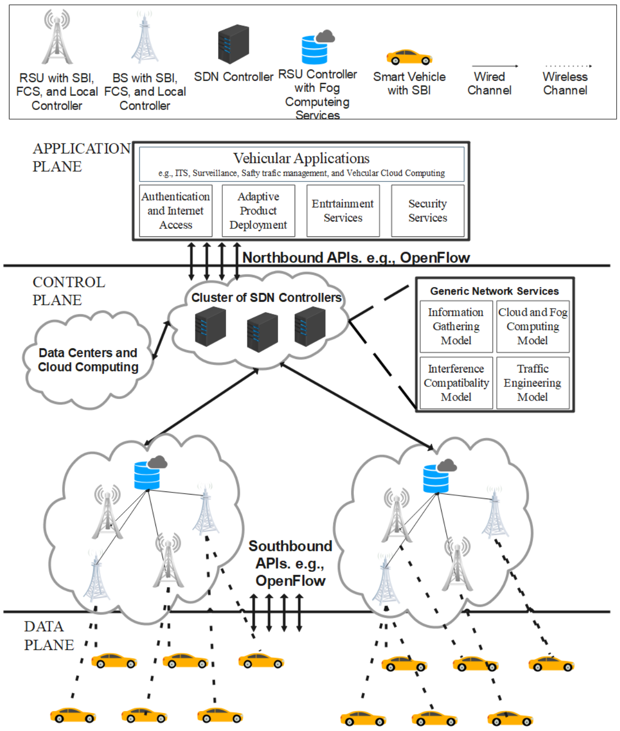

Figure 3 Methodological approach of the present study

- Transmission power: The success of your VANET depends on your ability to select the appropriate energy level and transmission range for your wireless interfaces. A controller in a VANET scenario gathers data from moving objects about their immediate environment (wireless nodes). The information gathered can be used to calculate the number of vehicles on a route or the space between them. The controller adjusts to the requirements of each node to maximise packet delivery.

3.1 Architectures of SDVN

The SDVN research that is currently being done is summarised in this section. Future SDVN designs are grouped according to whether they employ various paradigms (such as NDN, edge computing, cloud computing, and 5G). Following are the two broad categories in which we group the SDVN architectures we surveyed:

- Constructing SDN-based networks for specialised vehicles: Through the use of SDN, they are attempting to improve VANET characteristics such network delay, QoS, access control, routing integrity, and security. Additional technologies, such as SDN, might be needed to boost a certain parameter, like system performance.

- Developing general-purpose SDN-based vehicle networks: They want to boost VANET performance by utilising SDN and additional technologies like 5G and named data networking (NDN).

3.2 Advantage and Issues

We shall go through some of the primary benefits of SDVNs below.

- Optimized resource utilization: The global topology view is a tool that SDVN network managers can use to manage network resources more effectively. For instance, when there are several wireless interfaces or tunable radios available, controllers can more effectively coordinate channel/frequency selections.

- Quick and versatile network configuration: SDVNs' control and logic planes allow for quick and adaptable network design. The topology of the network will be adaptable to the mobility of the vehicles. Because video traffic uses a lot of bandwidth, several forwarding nodes are now overloaded.

- Heterogeneous network integration: SDVNs can thus integrate networks of heterogeneous (wireless and wired), as well as technologies of communication (5G, LTE, Wi-Fi, DSRC, etc.), at the data plane level. Using a communication protocol like OpenFlow makes it simpler for entities in control plane and the data plane to communicate with one another.

- Minimizing service latency: Utilizing SDN at network edge routers can drastically reduce service latency. For applications that are sensitive to delays, this reduces service latency.

3.3 SDVN Attackers

A breach may start from within or outside the organisation, be purposeful or accidental, and take either an active or passive form. Outside attackers are invaders and so unauthenticated, but inside attackers are network users and are therefore authenticated. These strangers are seeking financial gain. Those who wish to harm the network do so purely out of malice and with no thought of personal advantage. A passive attacker, on the other hand, just detects the network's presence. The deployment of SDN controllers in networks makes it challenging to establish an independent communication system.

- Hijacking of session: The authentication procedure is started and finished when a session starts. Once the link has been made, this is simple to accomplish. They gather comprehensive session data and serve as the hub node for the other nodes.

- Identity revealing: Most of the time, the owner of the car will give personal information to verify the driver. Attackers therefore find it simple to access the system.

- Location tracking: You can monitor the vehicle using its location to learn more about the driver and occupants.

- Listening: It goes after the layer of network, enabling access to private data.

- DoS attack: These kinds of attacks happen most frequently. The attackers prevent nodes from using services.

3.4 SDVN Attackers

We outlined the SDVN applications in this section.

- Comfort Technologies: The majority of individuals use comfort apps to learn about the weather, traffic, and the closest restaurants, hotels, hospitals and gas stations. If they have Internet connectivity, drivers and passengers can communicate online [67].

- Safety: It gathers information from sensors and other moving vehicles. The most crucial safety and security aspects are determined by the number of sensors used to gather data and the programme used to process it [68, 69].

- Avoiding Intersection Collisions: It is utilised at junctions to provide drivers options. The RS gathers data when vehicles are moving next to it and processes it in case of an alert or an accident. A warning message is sent so that cars close to the changing area can decide how best to stop their car [70].

- Motion Stopped as a Warning: Put Up a Sign: These are intended to warn drivers not to cross the intersection since there may be dangerous situations nearby. This is required for communication to occur between the RSU and the car's sensors. Since of this programme, the driver must occasionally stop because other cars are rapidly approaching the intersection. Once he has reached the turning point, the signal is green for him to proceed across [71].

- Job Areas on High Alert: Using this arrangement, vehicles close to the work area would be warned to slow down, as described in [68].

4. EXISTING SDVN RESEARCH

4.1 Security Analysis of SDVN

This section reviews the limitation of existing security schemes based on SDVN against major security attacks.

- Control Plane Resource Consumption. The majority of SDVN architectures mentioned in the literature [72–74], [74], [75] were not built with security in mind. In particular, they are subject to control plane resource consumption, which is a significant flaw in SDN. When there are several demands made of the control plane by the data plane, this attack is launched.

- Network Topology Poisoning. The majority of the topological information is connected to upper-layer applications including packet routing, network virtualization and optimization, and mobility tracking [76–78].

- Distributed Denial of Service Attacks. DDoS attacks can be used to cause a distributed denial of service (DDoS) on SDVN architectures [79–81]. The infrastructure layer (vehicles, RSU), the control layer (RSU controllers), and the application layer are the three main functional layers that make up SDVNs designs, hence potential DDoS attacks could be launched against any one or more of these layers.

- Rule conflicts. In OpenFlow applications, rule conflicts could lead to terrible attacks. For instance, a loadbalancing application may decide to ignore specific rules that are intended to quarantine a server because it thinks the targeted host is the least-loaded server [17, 82, 83].

- Privacy. Different user related information, such as the licence plate, the position, and the driver's identity, must be secured in SDVN-based architectures; however, the authorities must be able to divulge the names of the users in the event of an accident or a disagreement [84-85]. It is possible to apply conditional privacypreserving methods to automotive software architectures. The authors of [86] put up GSIS as a solution that combines group-based signatures and ID-based signatures and provides mechanisms for maintaining security and privacy between various OBUs and between OBUs and RSUs. The authors of [87] suggest a blind signaturebased authentication system that protects location privacy.

- Forgery. The goal of this attack is to poison significant areas of highways by fabricating and disseminating fake warning messages [84, 88-89].

- Tampering. The communication of other vehicles may be interfered with by a vehicle acting as a relay, which could result in in-transit tampering. Consequently, the car may delete, alter, or corrupt messages.

- Jamming. Even without compromising cryptographic methods, a jamming attack allows the attacker to divide the network [74, 90-91].

- Impersonation. An assailant can pose as a police officer in this kind of attack to trick other drivers into slowing down or changing lanes [85, 90-91].

- Application-based attacks. The following examines two specific vehicle uses, including platoon management and smart grid. Smart grid application and platooning vehicular application.

- Malware Attack Injection. A maliciously injected piece of software that replicates itself through various controllers, switches, and vehicles is a possibility in SDVN-based infrastructures [92]. By using a trust group structure to authenticate CAN bus communications, the authors of [93] suggest a framework for automotive systems.

- Routing based Attacks. The sinkhole, sybil, and replay attacks are discussed in the sections that follow. This attack can be carried out by an RSU in a sinkhole assault to direct some vehicles to direct all traffic to it. This harmful RSU acts like a hostile gateway. In [94], the authors suggest a centralised method for employing a geostatistical model to identify contaminated areas in the network. Additionally, the authors suggest a distributed monitoring strategy to investigate nearby nodes in order to find malicious nodes. A sybil assault involves creating many bogus vehicle identities to provide the appearance of heavy traffic on the road. Methods like [95-96] examine the signal strength distribution to find sybil attacks. The authors of [97] suggest a statistical technique for determining the origin of a vehicle. This method uses statistical analysis over time to increase the detection's precision. According to [98], sybil node detection is carried out passively by fixed sites in the route. In a replay attack, the attacker sniffs a message to gain access to a closed network, then reuses it. In this situation, methods for message authentication and authorization like might be used [99].

Table I presents the main attacks that vulnerable SDN, VANET and SDVN.

Table 1 Attacks With SDN, VANET And SDVN.

Requirements	SDN	VANET	SDVN
Forgery	Yes	Yes	Yes
Attacks based on application		Yes	Yes
Impersonation		Yes	Yes
Network topology poisoning	Yes		Yes
Malware attack injection	Yes	Yes	Yes
DDoS attack	Yes	Yes	Yes
Control plane resource consumption	Yes		Yes
Jamming		Yes	Yes
Rule conflicts violating security polices	Yes		Yes
On-board tampering		Yes	Yes
Sybil attack	Yes	Yes	Yes
Sinkhole attack	Yes	Yes	Yes
Privacy violation	Yes	Yes	Yes
Replay attack	Yes	Yes	Yes

4.2 SDVN architectural

Table II shows an overview of this SDVN research and highlights the positive and negative aspects of each study.

5. FUTURE RESEARCH DIRECTION

Despite SDVN's rapid development, there are still many unanswered problems regarding its effectiveness, scalability, and dependability (trustworthiness). Thud, this section discusses some future research direction of the SDVN as follows.

Security aspect: The security of SDVN, which is still a serious worry, is a significant barrier to its wider use. The main component in many SDVN programmes that is in charge of running the entire network is the SDN controller. A single controller attack has the potential to bring down the entire network. An unauthorised person could access the system and make choices in place of the controller. Such invasions may endanger the safety of users.

Scalability: The capacity of current SDVNs to scale is crucial given the expanding size of the automotive sector. It is impossible to know whether there may be sudden changes or unforeseen impediments while travelling. The performance of SDVN may be impacted by a number of variables, such as technical advancements, intricate road typologies, infrastructure damage, etc. An increase in the number of cars and communications may also have an impact on SDVNs with low scalability.

Control of quickly transforming: The network architecture of SDVNs is subject to sudden and abrupt changes because of the high mobility of nodes (vehicles). For SDN controllers or RSUs, controlling cars in real-time while dealing with erratic communication connections is difficult. Links being broken are more likely to occur in V2V infrastructure with poor DSRC or WAVE connectivity. However, this procedure is manageable with the aid of an effective modifications and routing algorithm to the infrastructure, although they are expensive.

Process for revocation, misconduct discovery, and evaluation of credibility: The issue of determining which VANET nodes are reliable has not yet been resolved. Errors in vehicle appraisal might put users' lives at danger. We still lack definite standards by which to evaluate the dependability of any given vehicle.

Latency control: When using an unprotected wireless connection, you cannot predict when data will become available. To cut down on latency, other areas of network performance can be improved. Resource management and latency control are clearly related. Cloud computing is becoming increasingly popular since it is more efficient. Costs for cloud computing in VANETs rise as the number of cars grows.

6. Conclusions

This paper aims to improve readers' understanding of SDVN systems. Several SDVN research are compiled in this chapter as a summary. The paper introduces these architectures and explains their benefits and drawbacks. The risks and security precautions related to SDNV are then explored. The incorporation of new technologies into SDNV and pertinent applications of SDNV are then examined. Lastly, a thorough discussion of the unresolved concerns and potential research directions follows.

Table 2 Analyses Of Current SDVN Architectural Types.

Authors	Objective	Strengths	Limitations
Sudheera et al. [100]	Minimal travel time/routing protocol	Quick packet delivery, low latency, and overhead	upkeep of the global system's (or SDN controller's) overview
Tang et al. [101]	Routing with delay reduction for prediction of mobility and SDVNs	To direct trucks along the route	Since there has been no security analysis, there will be no fix if the connection to the controller breaks.
Soua et al. [102]	Enhancing bandwidth and latency using SDN-based VANETs and 5Gassisted VANETs	Using advantages including lower network latency, scalability, and flexibility	A representation of performance in the real world
Qi et al. [103]	A socially conscious clustering protocol is used to provide a 5G-VANET system based on SDN.	Improving the speed of Internet connections and reducing packet delivery	When testing and evaluating the central controller, these challenges are not taken into account.
Huang et al. [104]	5G V2V data off-loading using MEC architecture with SDN capabilities	Using contextual knowledge and V2V off-loading, descriptive route finding	Locating reliable contextual information, maintaining privacy while driving

References

[1] Mahmood A Al-Shareeda, Mohammed Anbar, Iznan Husainy Hasbullah, and Selvakumar Manickam. Survey of authentication and privacy schemes in vehicular ad hoc networks. IEEE Sensors Journal, 21(2):2422–2433, 2020.

[2] Mahmood A Al-Shareeda, Mohammed Anbar, Selvakumar Manickam, and Ali A Yassin. Vppcs: Vanet-based privacy-preserving communication scheme. IEEE Access, 8:150914–150928, 2020.

[3] [3] Mahmood A Al-Shareeda, Mohammed Anbar, Iznan Husainy Hasbullah, Selvakumar Manickam, and Sabri M Hanshi. Efficient conditional privacy preservation with mutual authentication in vehicular ad hoc networks. IEEE Access, 8:144957–144968, 2020.

[4] Mahmoud Al Shareeda, Ayman Khalil, and Walid Fahs. Realistic heterogeneous genetic-based rsu placement solution for v2i networks. Int. Arab J. Inf. Technol., 16(3A):540–547, 2019.

[5] Mahmood A Al-shareeda, Mohammed Anbar, Selvakumar Manickam, and Iznan H Hasbullah. An efficient identity-based conditional privacypreserving authentication scheme for secure communication in a vehicular ad hoc network. Symmetry, 12(10):1687, 2020.

[6] Mahmood A Al-Shareeda, Mohammed Anbar, Murtadha A Alazzawi, Selvakumar Manickam, and Ahmed Shakir Al-Hiti. Lswbvm: A lightweight security without using batch verification method scheme for a vehicle ad hoc network. IEEE Access, 8:170507–170518, 2020.

[7] Felipe Cunha, Leandro Villas, Azzedine Boukerche, Guilherme Maia, Aline Viana, Raquel AF Mini, and Antonio AF Loureiro. Data communication in vanets: Protocols, applications and challenges. Ad Hoc Networks, 44:90–103, 2016.

[8] Wei-Hsun Lee, Kuo-Ping Hwang, and Wen-Bin Wu. An intersection-to-intersection travel time estimation and route suggestion approach using vehicular ad-hoc network. Ad Hoc Networks, 43:71–81, 2016.

[9] Ahmed Nazar Hassan, Omprakash Kaiwartya, Abdul Hanan Abdullah, Dalya Khalid Sheet, and Ram Shringar Raw. Inter vehicle distance based connectivity aware routing in vehicular adhoc networks. Wireless Personal Communications, 98(1):33–54, 2018.

[10] Chakkaphong Suthaputchakun and Zhili Sun. Routing protocol in intervehicle communication systems: a survey. IEEE Communications Magazine, 49(12):150–156, 2011.

[11] Mustafa Maad Hamdi, Lukman Audah, Sami Abduljabbar Rashid, and Mahmood Al Shareeda. Techniques of early incident detection and traffic monitoring centre in vanets: A review. J. Commun., 15(12):896–904, 2020.

[12] Mahmood A Al-shareeda, Mohammed Anbar, Iznan H Hasbullah, Selvakumar Manickam, Nibras Abdullah, and Mustafa Maad Hamdi. Review of prevention schemes for replay attack in vehicular ad hoc networks (vanets). In 2020 IEEE 3rd International Conference on Information Communication and Signal Processing (ICICSP), pages 394–398. IEEE, 2020.

[13] Mahmood A Al-shareeda, Mohammed Anbar, Selvakumar Manickam, and Iznan H Hasbullah. Review of prevention schemes for man-in the middle (MITM) attack in vehicular ad hoc networks. International Journal of Engineering and Management Research, 10, 2020.

[14] Mahmoud Al Shareeda, Ayman Khalil, and Walid Fahs. Towards the optimization of road side unit placement using genetic algorithm. In 2018 International Arab Conference on Information Technology (ACIT), pages 1–5. IEEE, 2018.

[15] Naserali Noorani and Seyed Amin Hosseini Seno. Routing in vanets based on intersection using sdn and fog computing. In 2018 8th International Conference on Computer and Knowledge Engineering (ICCKE), pages 339–344. IEEE, 2018.

[16] Baraa T Sharef, Raed A Alsaqour, and Mahamod Ismail. Vehicular communication ad hoc routing protocols: A survey. Journal of network and computer applications, 40:363–396, 2014.
[17] Mattia Fogli, Carlo Giannelli, and Cesare Stefanelli. Software-defined networking in wireless ad hoc scenarios: Objectives and control architectures. Journal of Network and Computer Applications, page 103387, 2022.
[18] Dimitrios Kafetzis, Spyridon Vassilaras, Georgios Vardoulias, and Iordanis Koutsopoulos. Software-defined networking meets softwaredefined radio in mobile ad hoc networks: State of the art and future directions. IEEE Access, 2022.
[19] Maroua Abdelhafidh, Nadia Charef, Adel Ben Mnaouer, and Lamia Chaari Fourati. Software-defined networking for flying ad-hoc network security: A survey. In 2022 2nd International Conference of Smart Systems and Emerging Technologies (SMARTTECH), pages 232–237. IEEE, 2022.
[20] Shanu Bhardwaj and Surya Narayan Panda. Performance evaluation using ryu sdn controller in software-defined networking environment. Wireless Personal Communications, 122(1):701–723, 2022.
[21] Alfred Raju M and Narendran Rajagopalan. A survey on various architectural models using software-defined networks. In Mobile Computing and Sustainable Informatics, pages 641–657. Springer, 2022.
[22] G Kirubasri, S Sankar, Digvijay Pandey, Binay Kumar Pandey, Vinay Kumar Nassa, and Pankaj Dadheech. Software-defined networking-based ad hoc networks routing protocols. In Software Defined Networking for Ad Hoc Networks, pages 95–123. Springer, 2022.
[23] Martin Casado, Tal Garfinkel, Aditya Akella, Michael J Freedman, Dan Boneh, Nick McKeown, and Scott Shenker. Sane: A protection architecture for enterprise networks. In USENIX Security Symposium, volume 49, page 50, 2006.
[24] Martin Casado, Michael J Freedman, Justin Pettit, Jianying Luo, Nick McKeown, and Scott Shenker. Ethane: Taking control of the enterprise. ACM SIGCOMM computer communication review, 37(4):1–12, 2007.
[25] Natasha Gude, Teemu Koponen, Justin Pettit, Ben Pfaff, Mart´ın Casado, Nick McKeown, and Scott Shenker. Nox: towards an operating system for networks. ACM SIGCOMM computer communication review, 38(3):105–110, 2008.
[26] Floodlight Controller. Floodlight documentation, for developers, architecture.
[27] Hui Liu, Jie Li, Yan-Qing Zhang, and Yi Pan. An adaptive genetic fuzzy multi-path routing protocol for wireless ad-hoc networks. In Sixth International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing and First ACIS International Workshop on Self-assembling Wireless Network, pages 468–475. IEEE, 2005.
[28] G Santhi and Alamelu Nachiappan. Fuzzy-cost based multiconstrained qos routing with mobility prediction in manets. Egyptian informatics journal, 13(1):19–25, 2012.
[29] David Erickson. The beacon openflow controller. In Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking, pages 13–18, 2013.
[30] Vipul Narayan and AK Daniel. Rbchs: Region-based cluster head selection protocol in wireless sensor network. In Proceedings of Integrated Intelligence Enable Networks and Computing, pages 863–869. Springer, 2021.
[31] Martin Casado, Nate Foster, and Arjun Guha. Abstractions for software-defined networks. Communications of the ACM, 57(10):86–95, 2014.
[32] Stephen Gutz, Alec Story, Cole Schlesinger, and Nate Foster. Splendid isolation: A slice abstraction for software-defined networks. In Proceedings of the first workshop on Hot topics in software defined networks, pages 79–84, 2012.
[33] Mark Reitblatt, Nate Foster, Jennifer Rexford, and David Walker. Consistent updates for software-defined networks: Change you can believe in! In Proceedings of the 10th ACM workshop on hot topics in networks, pages 1–6, 2011.
[34] Ken Barr, Prashanth Bungale, Stephen Deasy, Viktor Gyuris, Perry Hung, Craig Newell, Harvey Tuch, and Bruno Zoppis. The vmware mobile virtualization platform: is that a hypervisor in your pocket? ACM SIGOPS Operating Systems Review, 44(4):124–135, 2010.
[35] Diego Kreutz, Fernando MV Ramos, Paulo Esteves Verissimo, Christian Esteve Rothenberg, Siamak Azodolmolky, and Steve Uhlig. Software-defined networking: A comprehensive survey. Proceedings of the IEEE, 103(1):14–76, 2014.
[36] Georgios Karagiannis, Onur Altintas, Eylem Ekici, Geert Heijenk, Boangoat Jarupan, Kenneth Lin, and Timothy Weil. Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. IEEE communications surveys & tutorials, 13(4):584–616, 2011.
[37] Ram Shringar Raw, Manish Kumar, and Nanhay Singh. Security challenges, issues and their solutions for vanet. International journal of network security & its applications, 5(5):95, 2013.
[38] Nirbhay Kumar Chaubey. Security analysis of vehicular ad hoc networks (vanets): a comprehensive study. International Journal of Security and Its Applications, 10(5):261–274, 2016.
[39] Mohamed Nidhal Mejri, Jalel Ben-Othman, and Mohamed Hamdi. Survey on vanet security challenges and possible cryptographic solutions. Vehicular Communications, 1(2):53–66, 2014.
[40] Bassem Mokhtar and Mohamed Azab. Survey on security issues in vehicular ad hoc networks. Alexandria engineering journal, 54(4):1115–1126, 2015.
[41] Mahmood A Al-shareeda, Mohammed Anbar, Selvakumar Manickam, and Iznan H Hasbullah. Review of prevention schemes for modification attack in vehicular ad hoc networks. International Journal of Engineering and Management Research, 10, 2020.
[42] Mustafa Maad Hamdi, Ahmed Shamil Mustafa, Hussain Falih Mahd, Mohammed Salah Abood, Chanakya Kumar, and Mahmood A Alshareeda. Performance analysis of qos in manet based on ieee 802.11b. In 2020 IEEE international conference for innovation in technology (INOCON), pages 1–5. IEEE, 2020.
[43] Murtadha A Alazzawi, Hasanain AH Al-behadili, Mohsin N Srayyih Almalki, Aqeel Luaibi Challoob, and Mahmood A Alshareeda. Id-ppa: robust identity-based privacy-

preserving authentication scheme for a vehicular ad-hoc network. In International Conference on Advances in Cyber Security, pages 80–94. Springer, 2020.

[44] Mahmood A Al-Shareeda, Mohammed Anbar, Selvakumar Manickam, Ayman Khalil, and Iznan Husainy Hasbullah. Security and privacy schemes in vehicular ad-hoc network with identity-based cryptography approach: A survey. IEEE Access, 9:121522–121531, 2021.

[45] Jalawi Sulaiman Alshudukhi, Zeyad Ghaleb Al-Mekhlafi, Badiea Abdulkarem Mohammed. A lightweight authentication with privacy-preserving scheme for vehicular ad hoc networks based on elliptic curve cryptography. IEEE Access, 9: 15633-15642, 2021.

[46] Jalawi Sulaiman Alshudukhi, Badiea Abdulkarem Mohammed, Zeyad Ghaleb Al-Mekhlafi. Conditional privacy-preserving authentication scheme without using point multiplication operations based on elliptic curve cryptography (ECC). IEEE Access, 8: 222032-222040, 2020.

[47] Jalawi Sulaiman Alshudukhi, Badiea Abdulkarem Mohammed, Zeyad Ghaleb Al-Mekhlafi. An efficient conditional privacy-preserving authentication scheme for the prevention of side-channel attacks in vehicular ad hoc networks. IEEE Access,8: 226624-226636, 2020.

[48] Mahmood A Al-Shareeda, Mohammed Anbar, Selvakumar Manickam, and Iznan H Hasbullah. A secure pseudonym-based conditional privacy-preservation authentication scheme in vehicular ad hoc networks. Sensors, 22(5):1696, 2022.

[49] Mahmood A. Al-Shareeda, Selvakumar Manickam, Badiea Abdulkarem Mohammed, Zeyad Ghaleb Al-Mekhlafi, Amjad Qtaish, Abdullah J. Alzahrani, Gharbi Alshammari, Amer A. Sallam, and Khalil Almekhlafi. Provably secure with efficient data sharing scheme for fifth-generation (5g)-enabled vehicular networks without road-side unit (rsu). Sustainability, 14(16):9961, 2022.

[50] MAASM Mahmood A Al-shareeda, Mohammed Anbar, Murtadha A Alazzawi, Selvakumar Manickam, and Iznan H Hasbullah. Security schemes based conditional privacy-preserving in vehicular ad hoc networks. Indonesian Journal of Electrical Engineering and Computer Science, 21(1), 2020.

[51] Mahmood A Al-Shareeda, Mohammed Anbar, Selvakumar Manickam, and Iznan H Hasbullah. Password-guessing attack-aware authentication scheme based on chinese remainder theorem for 5g-enabled vehicular networks. Applied Sciences, 12(3):1383, 2022.

[52] Mahmood A Al-shareeda, Murtadha A Alazzawi, Mohammed Anbar, Selvakumar Manickam, and Ahmed K Al-Ani. A comprehensive survey on vehicular ad hoc networks (vanets). In 2021 International Conference on Advanced Computer Applications (ACA), pages 156–160. IEEE, 2021.

[53] Mahmood A Al-Shareeda, Selvakumar Manickam, Badiea Abdulkarem Mohammed, Zeyad Ghaleb Al-Mekhlafi, Amjad Qtaish, Abdullah J Alzahrani, Gharbi Alshammari, Amer A Sallam, and Khalil Almekhlafi. Cm-cppa: Chaotic map-based conditional privacypreserving authentication scheme in 5g-enabled vehicular networks. Sensors, 22(13):5026, 2022.

[54] Mahmood A Al-Shareeda and Selvakumar Manickam. Security methods in internet of vehicles. arXiv preprint arXiv:2207.05269, 2022.

[55] Samya Muhuri, Debasree Das, and Susanta Chakraborty. An automated game theoretic approach for cooperative road traffic management in disaster. In 2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS), pages 145–150. IEEE, 2017.

[56] Sabeen Javaid, Ali Sufian, Saima Pervaiz, and Mehak Tanveer. Smarttraffic management system using internet of things. In 2018 20th international conference on advanced communication technology (ICACT), pages 393–398. IEEE, 2018.

[57] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, page 21260, 2008.

[58] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. In Proceedings of the thirteenth EuroSys conference, pages 1–15, 2018.

[59] Lixia Xie, Ying Ding, Hongyu Yang, and Xinmu Wang. Blockchainbased secure and trustworthy internet of things in sdn-enabled 5gvanets. IEEE Access, 7:56656–56666, 2019.

[60] Boubakr Nour, Adlen Ksentini, Nicolas Herbaut, Pantelis A Frangoudis, and Hassine Moungla. A blockchain-based network slice broker for 5g services. IEEE Networking Letters, 1(3):99–102, 2019.

[61] Chao Qiu, F Richard Yu, Haipeng Yao, Chunxiao Jiang, Fangmin Xu, and Chenglin Zhao. Blockchain-based software-defined industrial internet of things: A dueling deep q -learning approach. IEEE Internet of Things Journal, 6(3):4627–4639, 2018.

[62] Mauro Conti, E Sandeep Kumar, Chhagan Lal, and Sushmita Ruj. A survey on security and privacy issues of bitcoin. IEEE Communications Surveys & Tutorials, 20(4):3416–3452, 2018.

[63] Zhaojun Lu, Wenchao Liu, Qian Wang, Gang Qu, and Zhenglin Liu. A privacy-preserving trust model based on blockchain for vanets. IEEE Access, 6:45655–45664, 2018.

[64] Florian Tschorsch and Bj¨orn Scheuermann. Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3):2084–2123, 2016.

[65] Mahmood A Al-shareeda, Mohammed Anbar, Selvakumar Manickam, Iznan H Hasbullah, Ayman Khalil, Murtadha A Alazzawi, and Ahmed Shakir Al-Hiti. Proposed efficient conditional privacypreserving authentication scheme for v2v and v2i communications based on elliptic curve cryptography in vehicular ad hoc networks. In International Conference on Advances in Cyber Security, pages 588–603. Springer, 2020.

[66] Mahmood A Al-Shareeda, Selvakumar Manickam, Badiea Abdulkarem Mohammed, Zeyad Ghaleb Al-Mekhlafi, Amjad Qtaish, Abdullah J Alzahrani, Gharbi Alshammari, Amer A Sallam, and Khalil Almekhlafi. Chebyshev polynomial-based scheme for resisting sidechannel attacks in 5g-enabled vehicular networks. Applied Sciences, 12(12):5939, 2022.

[67] Mukesh Saini, Abdulhameed Alelaiwi, and Abdulmotaleb El Saddik. How close are we to realizing a pragmatic vanet solution? a metasurvey. ACM Computing Surveys (CSUR), 48(2):1–40, 2015.
[68] Hammad Shafiq, Rana Asif Rehman, and Byung-Seo Kim. Services and security threats in sdn based vanets: A survey. Wireless Communications and Mobile Computing, 2018, 2018.
[69] N Fares and Shavan Askar. A novel semi-symmetric encryption algorithm for internet applications. Journal of University of Duhok, 19(1):1–9, 2016.
[70] Sulaiman M Sulaiman and Shavan K Askar. Investigation of the impact of ddos attack on network efficiency of the university of zakho. Science Journal of University of Zakho, 3(2):275–280, 2015.
[71] Muhammad Arif, Guojun Wang, Oana Geman, Valentina Emilia Balas, Peng Tao, Adrian Brezulianu, and Jianer Chen. Sdn-based vanets, security attacks, applications, and challenges. Applied Sciences, 10(9):3217, 2020.
[72] Tolga O Atalay, Dragoslav Stojadinovic, Angelos Stavrou, and Haining Wang. Scaling network slices with a 5g testbed: A resource consumption study. In 2022 IEEE Wireless Communications and Networking Conference (WCNC), pages 2649–2654. IEEE, 2022.
[73] Zongjian He, Jiannong Cao, and Xuefeng Liu. Sdvn: Enabling rapid network innovation for heterogeneous vehicular communication. IEEE network, 30(4):10–15, 2016.
[74] Karima Smida, Hajer Tounsi, and Mounir Frikha. Intelligent and resizable control plane for software defined vehicular network: a deep reinforcement learning approach. Telecommunication Systems, 79(1):163–180, 2022.
[75] Ali Hussein, Imad H Elhajj, Ali Chehab, and Ayman Kayssi. Sdn vanets in 5g: An architecture for resilient security services. In 2017 Fourth international conference on software defined systems (SDS), pages 67–74. IEEE, 2017.
[76] Gagangeet Singh Aujla, Sahil Garg, Kuljeet Kaur, and Biplab Sikdar. Software defined internet of everything, 2022.
[77] Wuqiang Qi, Rui Chen, Minghui Chen, Meng Zhao, and Mingzhao Wang. Evaluation analysis of the nephrotoxicity of tripterygium wilfordii preparations with consort harms statement based on deep learning. Journal of Healthcare Engineering, 2022, 2022.
[78] Richard Skowyra, Lei Xu, Guofei Gu, Veer Dedhia, Thomas Hobson, Hamed Okhravi, and James Landry. Effective topology tampering attacks and defenses in software-defined networks. In 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pages 374–385. IEEE, 2018.
[79] Yuchuan Deng, Hao Jiang, Peijing Cai, Tong Wu, Pan Zhou, Beibei Li, Hao Lu, Jing Wu, Xin Chen, and Kehao Wang. Resource provisioning for mitigating edge ddos attacks in mec-enabled sdvn. IEEE Internet of Things Journal, 2022.
[80] Qiao Yan and F Richard Yu. Distributed denial of service attacks in software-defined networking with cloud computing. IEEE Communications Magazine, 53(4):52–59, 2015.
[81] Esha Agarwal. A review on vanet security attacks. Call for Papers, page 45, 2022.
[82] Seung Won Shin, Phillip Porras, Vinod Yegneswara, Martin Fong, Guofei Gu, and Mabry Tyson. Fresco: Modular composable security services for software-defined networks. In 20th annual network & distributed system security symposium. Ndss, 2013.
[83] Ming Mao, Peng Yi, Jianhui Zhang, Liang Wang, Yuan Gu, and Guanying Zhang. Roadside units plane optimization scheme in softwaredefined vehicular networks. Transactions on Emerging Telecommunications Technologies, page e4499, 2022.
[84] Xiaoyu Zhang, Hong Zhong, Chunyang Fan, Irina Bolodurina, and Jie Cui. Cbacs: A privacy-preserving and efficient cache-based access control scheme for software defined vehicular networks. IEEE Transactions on Information Forensics and Security, 2022.
[85] Xiaoyu Zhang, Hong Zhong, Jie Cui, Chengjie Gu, Irina Bolodurina, and Lu Liu. Ac-sdvn: An access control protocol for video multicast in software defined vehicular networks. IEEE Transactions on Mobile Computing, 2022.
[86] Xiaodong Lin, Xiaoting Sun, Pin-Han Ho, and Xuemin Shen. Gsis: A secure and privacy-preserving protocol for vehicular communications. IEEE Transactions on vehicular technology, 56(6):3442–3456, 2007.
[87] Chenxi Zhang, Rongxing Lu, Pin-Han Ho, and Anyi Chen. A location privacy preserving authentication scheme in vehicular networks. In 2008 IEEE Wireless Communications and Networking Conference, pages 2543–2548. IEEE, 2008.
[88] Wafa Ben Jaballah, Mauro Conti, Mohamed Mosbah, and Claudio E Palazzi. Fast and secure multihop broadcast solutions for intervehicular communication. IEEE Transactions on Intelligent Transportation Systems, 15(1):433–450, 2013.
[89] Wafa Ben Jaballah, Mauro Conti, Mohamed Mosbah, and Claudio E Palazzi. The impact of malicious nodes positioning on vehicular alert messaging system. Ad Hoc Networks, 52:3–16, 2016.
[90] Lokendra Vishwakarma, Ankur Nahar, and Debasis Das. Lbsv: Lightweight blockchain security protocol for secure storage and communication in sdn-enabled iov. IEEE Transactions on Vehicular Technology, 2022.
[91] Maxim Raya and Jean-Pierre Hubaux. Securing vehicular ad hoc networks. Journal of computer security, 15(1):39–68, 2007.
[92] Usman Ahmed, Jerry Chun-Wei Lin, Gautam Srivastava, Unil Yun, and Amit Kumar Singh. Deep active learning intrusion detection and load balancing in software-defined vehicular networks. IEEE Transactions on Intelligent Transportation Systems, 2022.
[93] Qiyan Wang and Sanjay Sawhney. Vecure: A practical security framework to protect the can bus of vehicles. In 2014 International Conference on the Internet of Things (IOT), pages 13–18. IEEE, 2014.
[94] Hosein Shafiei, Ahmad Khonsari, Hazhir Derakhshi, and Payam Mousavi. Detection and mitigation of sinkhole attacks in wireless sensor networks. Journal of Computer and System Sciences, 80(3):644–653, 2014.
[95] Haonan Yang, Yongchao Zhong, Bo Yang, Yiyu Yang, Zifeng Xu, Longjuan Wang, and Yuqing Zhang. An overview of sybil attack detection mechanisms in vfc. In

2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSNW), pages 117–122. IEEE, 2022.

[96] Mustafa Maad Hamdi, Majeed Dhafer, Ahmed Shamil Mustafa,Sami Abduljabbar Rashid, Ahmed Jamal Ahmed, and Ahmed Muhi Shantaf. Effect sybil attack on security authentication service in vanet. In 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), pages 1–6. IEEE, 2022.

[97] Bo Yu, Cheng-Zhong Xu, and Bin Xiao. Detecting sybil attacks in vanets. Journal of Parallel and Distributed Computing, 73(6):746–756, 2013.

[98] Tong Zhou, Romit Roy Choudhury, Peng Ning, and Krishnendu Chakrabarty. P2dap—sybil attacks detection in vehicular ad hoc networks. IEEE journal on selected areas in communications, 29(3):582–594, 2011.

[99] Dhia Eddine Laouiti, Marwane Ayaida, Nadhir Messai, Sameh Najeh, Leila Najjar, and Ferdaous Chaabane. Sybil attack detection in vanets using an adaboost classifier. In 2022 International Wireless Communications and Mobile Computing (IWCMC), pages 217–222. IEEE, 2022.

[100] Kalupahana Liyanage Kushan Sudheera, Maode Ma, and Peter Han Joo Chong. Link stability based optimized routing framework for software defined vehicular networks. IEEE Transactions on Vehicular Technology, 68(3):2934–2945, 2019.

[101] Yujie Tang, Nan Cheng, Wen Wu, Miao Wang, Yanpeng Dai, and Xuemin Shen. Delay-minimization routing for heterogeneous vanets with machine learning based mobility prediction. IEEE Transactions on Vehicular Technology, 68(4):3967–3979, 2019.

[102] Ahmed Soua and Samir Tohme. Multi-level sdn with vehicles as fog computing infrastructures: A new integrated architecture for 5gvanets. In 2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), pages 1–8. IEEE, 2018.

[103] Weijing Qi, Qingyang Song, Xiaojie Wang, Lei Guo, and Zhaolong Ning. Sdn-enabled social-aware clustering in 5g-vanet systems. IEEE Access, 6:28213–28224, 2018.

[104] Chung-Ming Huang, Meng-Shu Chiang, Duy-Tuan Dao, Wei-Long Su, Shouzhi Xu, and Huan Zhou. V2v data offloading for cellular network based on the software defined network (sdn) inside mobile edge computing (mec) architecture. IEEE Access, 6:17741–17755, 2018.

Badiea Abdulkarem Mohammed received his BSc in Computer Science from Babylon University, Iraq in 2002, M.Tech in Computer Science from University of Hyderabad, India in 2007 and PhD from Universiti Sains Malaysia, Malaysia in 2018. He is currently an Assistant Professor in the College of Computer Science and Engineering at University of Hail, KSA. He is permanently Assistant Professor at Hodeidah University, Yemen. His research focuses on Wireless Networks, Mobile Networks, Vehicle networks, WSN, Cybersecurity, and Image Processing. He is an IEEE member, Member, IAENG member, and ASR member. In his research area, he has published many papers in reputed journals and conferences.