Software-Defined Vehicular Networking Security: Threats and Security Opportunities for 5G

Marc Lacoste, David Armand, Franck L'Hereec,
Frédéric Prévost, Yvan Rafflé, and Sébastien Roché

Orange
{firstname.lastname}@orange.com

Abstract. The complexity of the 5G vehicular ecosystem, the multiplicity of automotive use cases, and the diversity of the security requirements calls for a simple and yet flexible paradigm to manage security. This is the promise of Software-Defined Vehicular Networking (SDVN) that applies the benefits of Software-Defined Networking (SDN) to vehicular systems and networks. This paper provides an overview of the SDVN approach and architectures, and assesses its security impact for 5G automotive systems, in terms of security benefits, threats, and opportunities for cyber-security services for telcos.

Keywords: vehicular networks · security · software-defined vehicular networking · 5G · SDN · connected and autonomous vehicles

1 5G Connected and Autonomous Vehicles

Connected and autonomous vehicles (CAV) are now turning into a reality, with many benefits in terms of safety, efficiency, and QoS. Their evolutions are structured by two mega-trends. First, rising levels of *autonomy*: vehicles are already partly automated today with many x-assists (e.g., smart parking, cruise control). This trend is expected to grow, both for individual vehicles and for cooperative driving. Second, sprawling *connectivity*: vehicles sense and react to their environment through many network channels. They become "connected to everything" (V2X), including other vehicles (V2V), telco networks, and smart road infrastructures (V2I). Two prominent families of networking technologies are cellular-based connectivity (e.g., 5G such as C-V2X) and WLAN-based connectivity (derived from Wi-Fi), for long-range communications between vehicles and base stations, and nearer interactions in ad hoc networks of vehicles (VANETs).

CAV is a core 5G vertical, but also a complex multi-tier ecosystem composed of vehicles, network and edge, and cloud back-end systems. Such complexity induces multiple security, privacy, and resilience challenges. The great variety of automotive use cases (e.g., lane merging, remote driving) highlights mandatory requirements for integrity and authentication with a high level of robustness, the need for solutions to manage secure software or credential updates, and often confidentiality and privacy guarantees. All those elements call for a simple and yet flexible paradigm to manage security in this complex system-of-systems.

Software-Defined Vehicular Networking (SDVN) applies the benefits of Software-Defined Networking (SDN) to vehicular systems and networks [11]. This approach emerged as a smoother manner to manage security of such increasingly virtualized systems. It may however introduce additional risks. A clear picture of SDVN benefits and limitations will help to better understand 5G vehicular security, in terms of threats, counter-measures, and service opportunities.

This paper provides an overview of the SDVN approach and architectures, and how they may help to meet the CAV diversity of security requirements and ecosystem complexity. We assess the SDVN security impact, in terms of benefits and risks. We finally discuss some security service opportunities for telcos.

2 SDVN: Software-Defined Vehicular Networking

2.1 VANET Deployment Challenges

Vehicular networks face multiple challenges for practical deployment such as *scalability* (number of connected vehicles), *QoS* for connectivity (low-latency, vehicle mobility), variability of *network conditions* (rapidly changing topology, non-uniform network coverage depending on density of vehicles), *heterogeneity* of networking technologies, *lack of flexibility and programmability* of network intelligence (resource allocation, prediction, and use), *security*, and *reliability*.

2.2 Approach

The intuition behind SDVN is to represent vehicles and elements of the road infrastructure such as Road Side Units (RSU) as *network switches* in the data plane. *SDN controllers* monitor the vehicular network in the control plane. Applying SDN principles to VANETs is foreseen to bring the programmability and flexibility lacking in today's distributed wireless substrate, while simplifying network management and enabling new V2V and V2I services [13].

2.3 Architecture

Overview. Motivated by the concept of network virtualization, SDVN [11,17] proposes to exploit SDN to tackle VANETs challenges. A typical architecture is shown in Figure 1:

- ***Data plane*:** This plane includes all data transmission network devices. It features an overlay network to eliminate the heterogeneity of existing vehicular networks. All vehicles, RSUs, and base stations are abstracted as *SDN switches*. These switches can be further categorized into a *mobile data plane* and a *stationary data plane*, according to their mobility. Roadside units and base stations belong to the stationary data plane, while vehicles are in the mobile data plane. Different management policies are applied to the two planes [11].

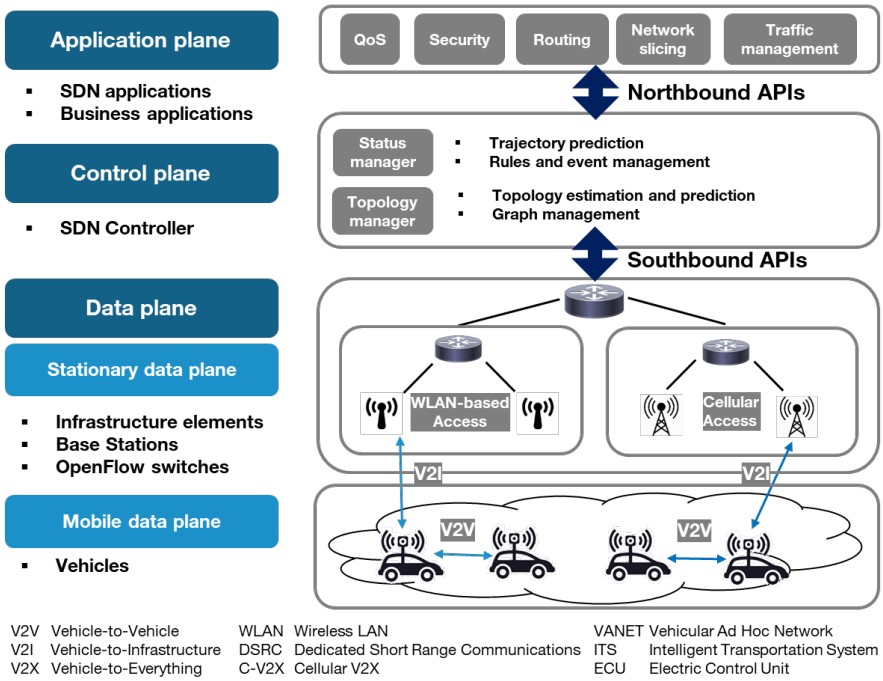

Fig. 1. SDVN architecture

- ***Control plane*:** This plane maintains the status of all the switches and is responsible for making packet-forwarding decisions based on it. The control plane is logically centralized. Control of the networks is transferred from individual switches to the controller. Switch status includes vehicle location, velocity, and network connectivity. This plane also maintains the current network topology state information. Almost all vehicles are now equipped with positioning devices like GPS that can provide such information [11].
- ***Application plane*:** This plane contains network services and applications.
- ***Communication interfaces*:** Control and data planes communicate through a unified interface (a.k.a. Southbound API), which includes some predefined control and notification messages. *Standard OpenFlow needs to be extended to adapt to vehicular requirements.* Different types of cellular or wireless links abstract V2V and V2I communications. The application plane uses Northbound APIs to communicate with the control plane. Unfortunately, there is currently no standardized interface for Northbound APIs.

Application plane modules. Several modules or services compose the application plane such as broadcast storm prevention, network slicing, adaptive protocol deployment, security, QoS, or multi-hop routing. Those services enable to enhance the SDVN functionalities.

Control plane functions. The following components of the architecture have key functions [11]:

- ***Status manager*:** To support logically centralized control of the data plane, the control plane must collect and maintain status information of all SDN switches, including vehicles and RSUs. The status manager is designed for this task. Trajectory prediction is its key function, tackling two important challenges of applying SDN to mobile networks: reachability and mobility. An intuitive way to address this issue is to fall back to the decentralized ad hoc communication while disconnected with the control plane [13].
- ***Topology manager*:** The control plane also needs to maintain the network topology information based on SDN switch status. For a *stationary data plane* with wired communication, the network topology seldom changes. Hence, the topology is considered as stationary. For a *mobile data plane*, the collected status includes neighbor information, which can be used to construct the network topology. If the vehicle position is obtained via *trajectory prediction*, there is no neighbor information available. The topology manager will then estimate the network topology using mean transmission range.

Operational modes. Three main levels of control may be distinguished to operate an SDN-based vehicular network [13]:

- ***Central control mode*:** The SDN controller controls all actions of underlying SDN wireless nodes and RSUs. All the actions performed by SDN data plane elements are explicitly defined by the controller, that will push down all the flow rules describing how to treat traffic.
- ***Distributed control mode*:** Wireless nodes and RSUs do not operate under any guidance from the SDN controller during data packet delivery. This control mode is very similar to self-organizing distributed networks without any SDN features, except that the local agent on each SDN wireless node controls the behavior of each individual node.
- ***Hybrid control mode*:** The SDN controller exerts an intermediate level of control. It can delegate control of packet processing to local agents. Control traffic is exchanged between all SDN elements. Instead of sending complete flow rules, the controller sends out policy rules defining general behavior: SDN wireless nodes and RSUs are instructed to run a specific routing protocol with certain parameters. Nodes and RSUs then use local intelligence for packet forwarding and flow level processing.

An interesting example of complex control mode is the *Hierarchical Software-Defined VANET (HSDV)* [5]. HSDV leverages the flexibility and programmability brought by SDN into vehicular networks while improving overall system performance in case of connection loss between vehicles and the SDN controller. It uses *clustering* concepts to create an infrastructure that maintains a network functional state regardless of central coordination by the SDN controller.

2.4 Benefits for CAV Deployment

SDVN addresses several VANET deployment challenges such as *scalability* and *variability of network conditions*. For instance, it provides better management of heterogeneous vehicular communications by reducing transmission interference and optimizing packet routing. It also allows predicting trajectories to optimize high vehicle mobility. Other benefits include enhancing safety, e.g., emergency traffic gets priority over the remaining traffic.

2.5 Ecosystem

Automotive cyber-security is a rich and growing ecosystem [15]. It involves multiple players such as OEMs, telcos, connectivity providers, chipmakers, AI startups, private sector companies, government agencies, and regulatory authorities. It also includes different areas of security such as protection of system ECUs, anomaly detection, or data protection. Within that ecosystem and beyond, the SDVN impact has been growing. A number of directions may be mentioned.

Machine learning. SDVN is a first step on the path toward the vehicle becoming fully *software-defined*. This vision enables context-aware and continuous adaptation of functionality and protection, depending on requirements of drivers, OEMs, and infrastructure and network providers [16].

Machine learning is a core SDVN-related adaptation technology that has been explored by the V2X ecosystem players for more than a decade, notably through *vehicular Intrusion Detection and Prevention Systems (IDPS)*. Many products are now available, such as Security Information and Event Management (SIEM), threat intelligence, malware mitigation, on-board system anomaly detection, and forensics.

Most systems are based on *anomaly detection*. This approach enables not to be limited to known attacks and is well adapted to the highly-changing vehicular context. Such systems allow detecting violations of system isolation between increasingly virtualized ECUs, or protecting network segments against a wide variety of attacks. They may also use both fleet and vehicle data to identify anomalous driving behaviors [24]. However, most systems remain limited to pure monitoring, reporting, or forensics with few solutions for mitigation.

Network slicing. Another important class of SDVN applications is end-to-end network isolation and anomaly detection. The SDVN controller then manages *slices* by enforcing a routing policy in data plane nodes.

Different types of slices may be defined, e.g., for vehicles, for each driving direction, to optimize broadcast of safety messages [11]. Different architectures have been proposed, either centralized, hierarchical, or based on multiple distributed controllers. However, there is still a lack of specification to extend OpenFlow to the vehicular setting, and of agreement for Northbound APIs.

Safety. SDVN also presents promising perspectives to improve the safety of Legacy In-Vehicle Networks (LIVN) that command many safety-critical features of the vehicle. Unfortunately, resilience remains so far complex and costly. It usually requires major evolutions of the hardware architecture to support new features (e.g., bus re-design, replicating ECUs).

SDVN programmability benefits may help to avoid hardware re-design: in the NIST *Software-Defined In-Vehicle Networking (SDIVN)* [10], upon failure occurrence, the in-vehicle ECU network topology may be reconfigured rapidly with the SDN controller to introduce self-healing capabilities.

European projects and testbeds. Many collaborative projects are exploring V2X use cases and security architectures. For instance, the 5G-PPP 5GCAR project selected five relevant and representative CAV use cases capturing their impact (e.g., societal, safety-related, business opportunities), occurrence in future highways or urban environments, and challenges for the communication system [1]. Those use cases (lane merging, see-through, network-assisted vulnerable pedestrian protection, HD local map acquisition, remote driving for automated parking) enabled to derive key CAV security and privacy requirements [2], and a first 5G V2X architecture addressing both the needs of car manufacturers and network operators.

One key takeaway is that security and privacy for C-V2X needs to be considered across multiple domains (both within a domain, and at domain external interfaces), which includes SDN / NFV management plane, control plane and data plane domains – hence the interest of the SDVN approach.

In continuity of 5GCAR, experiments are also being performed in several other European collaborative projects such as 5GCroCo [3] (in which Renault and PSA are also partners), with a 5G automotive testbed in Linas-Montlhéry (France), jointly operated by Orange and Ericsson.

2.6 Extension to Other Verticals: SDVN and Edge Technologies

SDVN is also applicable for more flexible security in new ecosystems such as drones [9], with potential synergies with automotive [19]. More broadly, identified roadblocks, services, and stakeholders are part of the current very rich set of reflections on the relation between *edge computing* and *security*, in terms of threats and benefits [18].

Indeed, CAV share with other verticals (e.g., smart cities, smart home, smart grids, smart agriculture) a number of networking and computing challenges such as *scalability* or *real-time constraints* that may be captured through the concept of *Smart and Connected Community (SCC)* [21].

SCCs features include context- and locality-awareness (e.g., ambient connectivity), low-latency requirements, promoting safety, security (e.g., safer driving), better quality of life (e.g., optimizing traffic or demand of electric supply), and new business models.

Architectures combining SDVN and edge technologies [20] help meeting such challenges, SDVN from the network side, and edge approaches from the computing side. Sample benefits include: scalable video streaming for environment and traffic data, high-performance Internet services and on-board entertainment systems, real-time roadside computing (accident detection, traffic information), and smarter energy management and mobility support.

Broader geographical zones for vehicular communication between vehicles may for instance be defined with the notion of *fog cells*, using multiple hop relays in the cells. This approach improves scalability, flexibility, throughput, and handover management compared to traditional ITS systems [12,22].

2.7 SDVN and 5G

Several challenges of vehicular networks become magnified for 5G networks. First, *low-latency and network performance*, including also scalability. Second, *mobility and highly dynamic topology*: a high-level of mobility and irregular distribution patterns of vehicles make V2X network management daunting. Third, *resilience*: intermittent connectivity of wireless networks implies to handle frequent disconnections. High signaling overheads also increase outage probability. And fourth, *network heterogeneity*: diverse cellular networks technologies and protocols and vendor equipments make interconnection, information sharing and dynamic adaptation difficult in so-called *HetNet architectures*.

The SDVN-based context-aware approach to traffic management may help supporting the dynamic nature of vehicular networks, simplifying hardware and software management, and finding the right trade-offs between performance, radio coverage, and vehicle density.

A typical 5G SDVN system includes vehicles, users, RSUs, BSs, partitioned into fog cells [8].

- The *data plane* includes vehicles, Base Stations, and RSUs. It collects information about vehicles (speed, direction), the environment (adjacent vehicles, users, traffic and road status), with positioning information, and includes high-speed wireless communications modules. A gateway vehicle communicates directly with the RSU using a multi-hop relay approach.
- The *control plane* includes RSU SDN controllers for edge data and network resource allocation and for management of fog clusters (e.g., mobility of vehicles in the cell, handover management between vehicles and RSUs). All vehicles can maintain communication with the RSU while moving along the road for a vehicle group. An overall SDN controller manages the 5G SDVN system and interfaces with remote clouds.
- The *application plane* includes features such as security, services efficiency, entertainment services, and overall policies.

This design enables adaptive vehicle clustering to reduce network overhead: vehicles communicate with the cellular network through a vehicle *cluster head (CH)* acting as a mobile gateway to support varying traffic conditions. It also supports beamformed transmission, aggregating CH traffic towards the base station to reduce signaling overhead, provide a high-capacity link, and improve communication quality [7]. Finally, centralized control over the HetNet and possible cooperative communication allow reducing latency.

2.8 Open Challenges

Mobility management, *internetworking in heterogeneous networks* and *security* remain vital challenges. The high mobility of vehicles causes dynamic topology and unstable wireless channels. It is thus hard for controllers to collect vehicle and network information in real-time. Distribution of commands from the controllers is also delayed. Current solutions are based on a hierarchical control layer, or predict results of vehicle behaviors. The lack of standardization of SDVN APIs, often poorly designed, and the prevalent open development environments may create opportunities for skilled adversaries to launch severe attacks on various layers of SDVN systems.

3 Security Impact

3.1 SDVN Security Challenges

Security remains a major challenge, as propagation of misinformation from unauthorized entities can lead to serious accidents. The key points of vigilance from a security standpoint are the following [4]. First, *the SDN controller* remains the central decision-making point, and should be strongly protected. A defense-in-depth approach is recommended, similarly to securing traditional SDN systems. Second, *tightly coupled SDN layers* facilitate propagation of threats between layers. APIs between layers should thus be hardened and standardized. Third, *vehicle mobility and openness in the lower data plane* amplify SDN threats to control and application layers. Thus, both layers of the data plane should be secured, with need for real-time authentication.

Some of those challenges may also impact *both CAV security and safety*. As CAV are tightly integrated systems-of-systems, failures on a sub-system may propagate to other sub-systems, and cascade, making recovery very difficult. *cyber-threats on the vehicle decision-making logic* also remain critical: vulnerabilities of machine-learning algorithms (e.g., to noise injection attacks), "brain" of the autonomous vehicle, can cause catastrophic outcomes in terms of safety if data integrity is compromised.

3.2 Security Threats

Several threats compromise forwarding, control, and application layers [23]. *Man-in-the-middle attacks* between a switch and the controller are caused by the lack of transport-layer security. Such attacks can be mitigated by strengthening physical network security. *Denial-of-service attacks* can saturate flow tables and buffers. Such attacks are caused by the insertion of reactive rules instead of adopting a proactive approach. They can be prevented by using multiple controllers. Other threats may come from distributed multi-controllers, applications, illegal access, or conflicts of security rules or configurations.

Despite existing solutions, high mobility requires security mechanisms that can perform *real-time authentication*. Otherwise, latency can cause traffic congestion that impedes the realization of SDVNs. This real-time factor increases difficulty in strengthening security.

Application-level. *Malicious applications* may corrupt the SDN controller and cause violations of authorization, privilege escalation, exhausting available resources, violations of service chains, or injecting malicious control messages in the network which can have catastrophic consequences in the network behavior (e.g., packet dropping, re-routing, and SDN controller termination). *Third party applications* may pose also serious threats due to vendor heterogeneity, lack of interoperability in security policies, and trust issues.

Control plane. *Compromised switches* may lead to poisoning of the SDN controller view of the network or of the network topology, or to creating fake links. *Control messages* may be manipulated for spoofing network resources or obtaining sensitive information. More general attacks include violating authorizations in the SDN controller, compromising network isolation, or threatening controller availability. The controller being the sole point for decision-making makes the control plane particularly vulnerable to attacks and failures. Its knowledge of the network may also be used to *launch new attacks*. Interoperability issues between multiple controllers may also be source of vulnerabilities.

Communication APIs. Major threats are insecurity of APIs and lack of standardization. The Southbound API is generally exposed to man-in-the-middle, eavesdropping, or availability attacks. SDVN lacks standardized customized OpenFlow API and Northbound APIs. Eastbound/Westbound APIs between controllers are also not standardized.

Upper data plane. Malicious programmable switches can advertise fake network topologies, or disrupt traffic (rerouting, hijacking, DoS), or the controller. Threats also include exhausting network resources, or performing side-channel attacks to extract sensitive information.

Lower data plane. Threats come from *vulnerabilities* of the multiple, heterogeneous *wireless communication protocols*, and from *software-defined radio*, as new applications and features may be downloaded through wireless links with reconfiguration capabilities, possibly causing integrity violations in different software layers. Threats also include device cloning (*Sybil attacks*) enabling unauthorized access to a service from another device (i.e., another vehicle). *Heterogeneity of device and networks* is a major source of vulnerability and failures. Factors such as mobility, dynamic topology, low-latency violations (e.g., for emergency services) may also complexify network security monitoring, or lead to road accidents.

3.3 SDVN Security Benefits

Benefits of SDN for security management are well-known thanks to centralization and greater programmability [6]. For instance: increased control capabilities, global network view, self-healing capabilities, enhanced resilience. With applications such as either network-wide or fine-grained intrusion detection, forensics, DoS mitigation, or access control.

Consistently, SDVN contributes to smoother management of vehicular security and safety. Applications include for instance handling failures through network reconfigurations, within the vehicle and beyond.

As such, SDVN is a promising enabler for a wide range of automotive cybersecurity services, such as in-vehicle security (intrusion detection, firewalling, vehicular device management, e.g., OTA updates), 5G connectivity security (network isolation and slicing, network anomaly detection), or orchestration-level services for networks of vehicles (safety, data protection).

4 Telco Benefits and Outlook

As vehicles are increasingly interfaced to the outside world, telcos fully become part of the vehicular ecosystem. SDVN opens a number of opportunities for telcos through value-added security services.

A first area for SDVN-based cyber-security services is *in-vehicle security* and its *extension outside the vehicle* to prevent long-range attacks. For instance, the in-vehicle hardware bus (e.g., CAN bus) remains highly vulnerable, with critical isolation stakes between core vehicle systems (ECUs): with telecommunication units plugged both on the bus and on the cellular network, all critical systems become easily accessible from outside the vehicle. Other examples of services include network attack detection, secure update and vehicle management – leveraging the eSIM card to protect secrets and guarantee secure outbound connectivity. Services involving autonomic security loops are particularly relevant – for instance, security monitoring to detect and react to threats, and guarantee in-vehicle, vehicle-to-network, or 5G end-to-end security.

Improving safety and resilience is another key area for services. SDVN-based monitoring may help bridging the safety-security gap, and to ensure monitoring and reaction to both accidental and malicious faults threatening the autonomous vehicle behavior.

Overall, SDVN provides insight of the potential of *machine learning and artificial intelligence* to address the challenges of future smart vehicular networks, where a wide spectrum of approaches, techniques and tools are increasingly receiving attention to tackle issues such as high mobility, strong network dynamics, stringent and heterogeneous QoS requirements, security and safety [14]. This should be also placed in the broader context of research on modelling and advanced simulations for cyber-physical systems.

Finally, the vehicular ecosystem is tightly integrated with other verticals. A horizontal, cross-vertical approach to security and safety management leveraging SDVN may therefore also be explored.

References

1. 5GCAR Project: Deliverable D2.1. 5GCAR Scenarios, Use Cases, Requirements and KPIs (2017), `https://5g-ppp.eu/5gcar/`
2. 5GCAR Project: Deliverable D4.1. Initial Design of 5G V2X System Level Architecture and Security Framework (2018), `https://5g-ppp.eu/5gcar/`
3. 5GCroCo: Fifth Generation Cross-Border Control: `https://5gcroco.eu/`
4. Akhunzada, A., Khan, M.K.: Toward Secure Software Defined Vehicular Networks: Taxonomy, Requirements, and Open Issues. IEEE Communications Magazine **55**(7), 110–118 (2017)
5. Correia, S., Boukerche, A., Meneguette, R.I.: An Architecture for Hierarchical Software-Defined Vehicular Networks. IEEE Communications Magazine **55**(7), 80–86 (2017)
6. Dabbagh, M., Hamdaoui, B., Guizani, M., Rayes, A.: Software-Defined Networking Security: Pros and Cons. IEEE Communications Magazine **53**(6), 73–79 (2015)
7. Duan, X., Liu, Y., Wang, X.: SDN Enabled 5G-VANET: Adaptive Vehicle Clustering and Beamformed Transmission for Aggregated Traffic. IEEE Communications Magazine **55**(7), 120–127 (2017)
8. Ge, X., Li, Z., Li, S.: 5G Software Defined Vehicular Networks. IEEE Communications Magazine **55**(7), 87–93 (2017)
9. Guerber, C., Larrieu, N., Royer, M.: Software Defined Network Based Architecture to Improve Security in a Swarm of Drones. In: International Conference on Unmanned Aircraft Systems (ICUAS). pp. 51–60 (2019)
10. Halba, K., Mahmoudi, C., Griffor, E.: Robust Safety for Autonomous Vehicles through Reconfigurable Networking. In: International Workshop on Safe Control of Autonomous Vehicles (SCAV) (2018)
11. He, Z., Cao, J., Liu, X.: SDVN: Enabling Rapid Network Innovation for Heterogeneous Vehicular Communication. IEEE Network **30**(4), 10–15 (2016)
12. Khan, A., Abolhasan, M., Ni, W.: 5G Next Generation VANETs using SDN and Fog Computing Framework. In: IEEE Annual Consumer Communications Networking Conference (CCNC). pp. 1–6 (2018)
13. Ku, I., Lu, Y., Gerla, M., Gomes, R.L., Ongaro, F., Cerqueira, E.: Towards Software-Defined VANET: Architecture and Services. In: 13th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET). pp. 103–110 (2014)
14. Liang, L., Ye, H., Li, G.Y.: Toward Intelligent Vehicular Networks: A Machine Learning Framework. IEEE Internet of Things Journal **6**(1), 124–135 (2019)

15. Lu, Z., Qu, G., Liu, Z.: A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy. IEEE Transactions on Intelligent Transportation Systems **20**(2), 760–776 (2019)
16. Mahmood, A., Zhang, W., Sheng, Q.: Software-Defined Heterogeneous Vehicular Networking: The Architectural Design and Open Challenges. Future Internet **11**(3), 1–17 (2019)
17. Mosharaf Kabir Chowdhury, N.M., Boutaba, R.: Network Virtualization: State of the Art and Research Challenges. IEEE Communications Magazine **47**(7), 20–26 (2009)
18. Roman, R., Lopez, J., Mambo, M.: Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. Future Generation Computer Systems **78**, 680–698 (2018)
19. Shi, W., Zhou, H., Li, J., Xu, W., Zhang, N., Shen, X.: Drone Assisted Vehicular Networks: Architecture, Challenges and Opportunities. IEEE Network **32**(3), 130–137 (2018)
20. Shrestha, R., Bajracharya, R., Nam, S.: Challenges of Future VANET and Cloud-Based Approaches. Wireless Communications and Mobile Computing **2018**(05), 1–15 (2018)
21. Shukla, R.M., Sengupta, S., Chatterjee, M.: Software-Defined Network and Cloud-Edge Collaboration for Smart and Connected Vehicles. In: 19th International Conference on Distributed Computing and Networking Workshops (ICDCN) (2018)
22. Truong, N.B., Lee, G.M., Ghamri-Doudane, Y.: Software defined networking-based vehicular Adhoc Network with Fog Computing. In: IFIP/IEEE International Symposium on Integrated Network Management (IM). pp. 1202–1207 (2015)
23. Yaqoob, I., Ahmad, I., Ahmed, E., Gani, A., Imran, M., Guizani, N.: Overcoming the Key Challenges to Establishing Vehicular Communication: Is SDN the Answer? IEEE Communications Magazine **55**(7), 128–134 (2017)
24. Zhang, M., Chen, C., Wo, T., Xie, T., Bhuiyan, M.Z.A., Lin, X.: SafeDrive: Online Driving Anomaly Detection From Large-Scale Vehicle Data. IEEE Transactions on Industrial Informatics **13**(4), 2087–2096 (2017)