Artificial Intelligence-Driven and Secure 5G-VANET Architectures for Future Transportation Systems

Murtaja Ali Saare [1], Mohamed Abdulrahman Abdulhamed [2], Mahmood A. Al-Shareeda [3*],
Mohammed Amin Almaiah [4], Rami Shehab [5]
[1,2] Faculty of Computer Science and Information Technology Computer Science Department,
University of Basra, Basra, Iraq
[3] Department of Electronic Technologies, Basra Technical Institute, Southern Technical
University, 61001, Basra, Iraq
[4] King Abdullah the II IT School, Department of Computer Science, The University of Jordan,
Amman 11942, Jordan
[5] Vice-Presidency for Postgraduate Studies and Scientific Research, King Faisal University, Al
Ahsa 31982, Saudi Arabia
Email: [1] murtaja.sari@uobasrah.edu.iq; [2] mohammed@uobasrah.edu.iq,
[3] mahmood.alshareedah@stu.edu.iq, [4] m.almaiah@ju.edu.jo, [5] Rtshehab@kfu.edu.sa
*Corresponding Author

Abstract—**The advent of 5G has opened a new era of intelligent, adaptive and secure VANETs that is envisaged to serve as the backbone network architecture for next generation of vehicular transportation systems. In this work, we present a connected 5G VANETs-to-Edge Computing systems with Artificial Intelligence (AI) infrastructure to improve system adaptability, anomaly detection, trust management, and real-time decision-making. Crucial enabling technologies like Software-Defined Networking (SDN),.Mobile Edge Computing (MEC), and millimeter-wave communication are investigated in detail. We examine key security threats such as identity forgery, data interception, and denial-of-service attacks, and assess the AI-enhanced defense measures such as intrusion detection systems and blockchain-based trust models. Applications, like autonomous platooning, and collaborative vehicle authentication provide additional examples of AI technologies' added value in the context of vehicular communications and safety. The paper concludes by providing open issues and future directions, including quantum-resistant protocols, lightweight AI models and cognitive networking in the context AI-driven 5G-VANET ecosystems.**

Keywords*—*Artificial Intelligence in VANETs; 5G-Enabled Vehicular Networks; Secure VANET Architectures; Intelligent Transportation Systems (ITS); Edge-Assisted AI Computing; Software-Defined Networking (SDN); Blockchain-based Trust Management

I. Introduction

Intelligent transportation systems (ITS) rely on vehicular communication as a backbone technology to enable wireless connectivity among cars, roadside gadgets, passengers, and pedestrians. At present, there are two main schools of thought in the field of vehicular communications: dedicated short-range communications (DSRC) and vehicle-to-everything technologies based on Long Term Evolution (LTE) (i.e., LTE-based V2X or LTE-V) [1]–[6]. The first is based on cellular network technologies specified by the Third Generation Partnership Project (3GPP), while the second is based on standards for Wireless Access for Vehicles Environment (WAVE) and has already been defined by IEEE 802.11p and IEEE 1609 [7]–[10].

Several vehicle communication services, both for safety and non-safety purposes, can be supported by LTE-based V2X communications, which take use of huge cell coverage range, high capacity, and widely distributed infrastructure. The road map for vehicle-to-everything (V2X) services based on 5G has already been prepared by technical organisations such as 3GPP and Qualcomm [11]–[16].

The goal of 5G is to facilitate new air interfaces and access ways using the re-allocated spectrum. Moreover, it will be based on existing wireless technologies such as Wi-Fi, LTE, high-speed packet access, the Global System for Mobile Communications, and others [17]–[20]. Nevertheless, outlining the fundamental components of 5G is crucial for facilitating the coexistence of current technologies [21]–[24]. Among the many essential components of 5G are technologies for discovering and providing services based on proximity information, network slicing techniques, software defined networks (SDNs), mobile edge computing (MEC), and millimeter-wave communications (specifically, in the 28 GHz, 38 GHz, 60 GHz, 71-76 GHz, and 81-86 GHz bands) [25]–[28].

The current standards for vehicular communication, known as IEEE 802.11p, [29]–[31] primarily address issues like reduced latency, extremely reliable transmission of periodic communications, and spectrum scarcity. When it comes to large-scale network deployments, the current standard isn't scalable and doesn't provide guaranteed service delivery. Further research on 5G-enabled vehicle communications is warranted due to the promises made by the successor of LTE, 5G, which has already been the subject of some studies. Gathering varied application requirements and basic standard specifications for 5G rollout until 2020 are current endeavours. We don't know of any other lesson that covers 5G for car communications like this one. The list of main contributions are listed as follows.

- Historical Context, Current Applications, and Service Quality Review: We start by an in-depth background about VANETs describing their evolution from the beginnings until present. This encompasses a review of their founding principles, milestones, and progress. Also, the diverse applications of VANETs with respect to Intelligent Transportation Systems (ITS) including traffic control, improved road safety, and infotainment systems are discussed. This equips with extensive knowledge of the standards of reliability, latency, scalability, and interoperability across services.
- Architecture and 5G Integration with IoT and Heterogeneous Device Support: The architecture of 5G-enabled mobile edge VANETs is proposed that highlights the primary components contributing to strong vehicular communication networks. VANETs interact effortlessly with the Internet of Things (IoT), enabling real-time data sharing, automation, and smart city functionalities. Moreover, we investigate the 5G offerings for supporting heterogeneous devices to enable vehicle to vehicle (V2V), vehicle to infrastructure (V2I), and vehicle to everything (V2X) communication, wherein vehicular systems, roadside units (RSUs), and user devices are efficiently inter-connected making the city networks smart and intelligent.
- Security Analysis in 5G-Enabled VANETs: A separate section examines the security challenges and threats posed by the integration of 5G and VANETs. We analyze critical vulnerabilities, including sensitive data leaks, identity spoofing, and denial-of-service (DoS) attacks, and assess the effectiveness of existing security frameworks in preventing these attacks. Analyzing the introduction of five G infrastructure with sample attack scenarios in VANETs then providing countermeasures for enhancing network security through usage of high end cryptographic algorithms and intrusion detection systems.
- Open Challenges and Future Directions in VANET Security Using 5G: The paper ends with the identification and discussion of unsolved problems in the integration of 5G with VANETs. We highlight key challenges such as enabling privacy, providing ultra-low latency for safety-critical applications, and dealing with the high computational cost of real-time security mechanisms. We further propose future research directions as lightweight security protocols, integration of artificial intelligence (AI) for agile recognition of anomalies, and utilization of blockchain technology for secured and transparent resource sharing.

The rest of this paper is structured as follows. Section II introduces the overview of VANET. Then we present VANET using 5G technology in Section III. As a case study, Section IV investigates the security of VANET using 5G. Section V provides the taxonomy of VANET using 5G. Section VI discusses open challenges and future direction in VANET using 5Gs. Section VII shows results of this paper. Finally, Section VIII concludes this article. Fig. 1 provides the organization work of this paper.

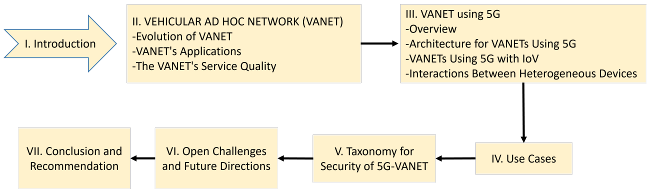

I. Introduction
II. VEHICULAR AD HOC NETWORK (VANET)
-Evolution of VANET
-VANET's Applications
-The VANET's Service Quality
III. VANET using 5G
-Overview
-Architecture for VANETs Using 5G
-VANETs Using 5G with IoV
-Interactions Between Heterogeneous Devices
IV. Use Cases
V. Taxonomy for Security of 5G-VANET
VI. Open Challenges and Future Directions
VII. Conclusion and Recommendation

Fig. 1. Work Organization of Review Paper

II. Vehicular Ad hoc Network (VANET)

A. *Evolution of VANET*

In 2001, VANETs were initially mentioned and introduced. Speed is the hallmark of moving vehicles [32], [33]. If the car travelling in the opposite way is driving at a high speed, the link will be broken after a few seconds. The network would like to transmit only the most important data in order to reduce the likelihood that it would not be received successfully in such a scenario. However, if a cluster of vehicles is travelling at a consistent speed, the network will have plenty of time to transmit any incoming data [34], [35]. This duration could grow substantially for events like parades or vehicle escorts. Because it's crucial to know which intermediate nodes will remain in the network long enough to complete the necessary transfer, multi-hop communication becomes much more challenging due to high mobility [36].

B. *VANET's Applications*

The characteristics, significance, benefits, etc., of VANET applications are covered in this section. Over the years, a number of research have focused on developing applications and use cases for communication in the vein of VANETs. A VANET application is one that prioritises safety and comfort [37], [38].

1) Applications-based Safety Aspect: Preventing traffic fatalities is the goal of these programmes. In order to avoid accidents, these apps primarily aim to send safety-related information to the right person at the right moment [39], [40]. The following are a few of the safety-related applications, which are listed in Table I.

- Information Messages (IM): Instant messages can be sent while driving through areas with work zones, toll booths, or signs restricting speed.
- Assistance Messages (AM): On the road, this kind of information will be useful to the driver. Navigation, lane change, and cooperative collision avoidance (CCA) signals are all part of AM. When it comes to helping the motorist, the CCA message is considered vital because it tells them to slow down so they may avoid uncertain conditions.
- Warning Messages (WM): WMs provide information like toll booths, traffic signal heads, and warnings regarding bad road conditions.

TABLE I. A FEW LITERATURE-BASED SAFETY APPLICATIONS

Applications	Explanation
Turn assistance	Provide assistance to the driver as they manoeuvre the vehicle
Avoiding collisions at intersections	Please provide information about the intersection of the roads.
Warning for blind spots	Warn the motorist that another vehicle is occupying their blind spot.
Curve speed	Signalling impending lane changes in a vehicle
Vehicle for emergency services	Allow passage to emergency vehicles, including ambulances.
Disruption of traffic signals	Warning other drivers in the area of the dangerous situation
Lane change warning	Verify that the designated entryway is free of obstructions.

2) Applications-based Non-Safety Aspect: While this may not be as important as the safety applications, it will help ensure that drivers are comfortable and traffic flows efficiently [41]. Such programmes may also be known as value-added offerings.

Road users should have unified internet access for non-safety uses, since there is a significant demand from those travelling with internet-connected autos [42]. Non-safety uses include things like stress-free driving, traffic flow information, route optimisation alternatives, and sites of interest [43], [44]. There are a variety of applications for this technology, including the automatic collection of tolls, location-based services (such as the exact positions of stores and restaurants), and internet connectivity. Apps that prioritise user comfort are shown in Table II.

C. The VANET's Service Quality

Changes to quality of service apps are covered in this section. Thanks to quality of service, both network efficiency and data sharing are enhanced. Quality of service also refers to the servability of network applications. The quality of service is determined by the support of VANET apps. There may be restrictions on VANET traffic monitoring, user comfort, and security. In terms of road safety and traffic monitoring, the authenticity of real-time data is the biggest challenge. Ongoing dialogue is essential for comfort application development. VANET Quality of Service entails MAC protocol cooperation, QoS routing, and resource reservation. The mechanisms of the routing and network layers provide quality of service. Ensuring VANET QoS requires optimising the routing protocol. According to [45], [46], networks aim towards success.

TABLE II. A FEW LITERATURE-BASED NON SAFETY APPLICATIONS

Applications	Explanation
Navigations	Making available a map that can be used to find the way to any place
Service announcement	Be sure to provide information regarding the restaurant and any other rest stops along the way.
Status update for passengers via remote	Proposal for an ambulance-specific wireless body sensor network. Direct transmission of patient vitals from the ambulance to the hospital allows for more precise diagnosis.
Entertainment	Users can enjoy live video and audio while on the go.
Parking availability	Details regarding available parking spaces, especially in urban areas
Route Alteration	In the event of traffic congestion, it helps drivers save time by modifying their routes.
Map download	Facilitate the downloading of maps for use in planning

Ad hoc networks present challenges for QoS routing due to fast topology changes and inaccurate state information [47]. To achieve QoS routing, a route must meet requirements in addition to connecting a source to a destination [48]. A service's capacity to implement QoS can be determined by applying previously stated requirements, such as minimum bandwidth, maximum delay, and maximum packet loss rate. Therefore, choosing the most accessible route is critical for QoS metrics. Conventional cable routing protocols can disrupt VANET connectivity due to its high mobility, poor link quality, and limited transport distance (28). Researchers have suggested several QoS routing methods to solve reliability and security concerns in VANET networks [49]–[51], while also considering the challenges faced by these networks.

III. VANET USING 5G

A. Overview

It is worth noting that cellular networks are becoming more popular for ITS connectivity services, partly because of their widespread deployment and coverage around the world. To be more precise, the 3GPP standardisation body has defined V2X services for the LTE network (release 14, 15) and improved V2X (eV2X) for the 5G network (release 6) [52], [53]. 5G, short for "fifth-generation wireless," is the most recent innovation in networking for mobile devices. Due to its architecture's compatibility with other new technologies, such as Heterogeneous Networks (HetNet), networking slicing, massive Multiple-Input Multiple-Output (MIMO), device-to-device communications, millimetre wave (mmWave), software defined networking (SDN), and high data rates (up to 20 Gbps) for real-time applications, it guarantees a latency of 1 ms on top of that [54]. 5G is able to accomplish more thanks to these cutting-edge technologies, including increased capacity, ultra-low end-to-end latency, faster data rates, a large number of connected devices, and reliable quality of experience (QoE) delivery [55].

5G technology's network management is just as notable as its increased capacity and decreased latency. With the use of network slicing, this network management may handle many virtual network connections according to the services needed. For instance, CAMs only employ secure, data-only connections, non-safety or multimedia applications necessitate greater capacity rather than high rate, and alert messages and pertinent security services necessitate a quick, low-latency network connection [56]. Existing VANET standards (IEEE 802.11p/DSRC) have flaws that have been previously mentioned, such as inefficient use of the 5.9 GHz band, limited communication range, overhead/delay caused by centralised security, and inefficient protocols for broadcast and acknowledgement. In order to remedy these deficiencies, 5G relies on Device-to-Device (D2D) connections [57]. Discover services and communicate with nearby users directly with D2D. Because of this, it can facilitate V2V and V2I communications directly, bypassing the need for the cellular infrastructure and the conventional uplink/downlink methods of cellular communication. This means that mission-critical automotive applications can benefit from D2D-based vehicular broadcasting, which offers low transmission power, low latency, high data rate, and great spectral efficiency [58].

In terms of safety, 5G offers a number of advantages due to its inherent flexibility. An important part of 5G-based flexible security is software-defined networking (SDN) control and virtual network functions (VNFs). As a result, 5G allows for the modification of security parameters and data encryption through the user plane. With NFV, virtual network functions (VNFs) are deployed and managed on cloud platforms. These VNFs may then be accessed remotely, doing away with the requirement for specialised hardware to run various applications and services offered by different vendors. With SDN, the network control plane and the data forwarding plane are physically separated, which allows for improved network control. Consequently, NFV and SDN both use the properties of the underlying networks to offer dynamic and need-based security [59]. That being said, 5G holds great promise for the commercialization of VANET thanks to SDN's exceptional capabilities in managing a multitude of heterogeneous devices, various network circumstances, improved security, and network flexibility.

Along with other groundbreaking features, 5G solves the issue of supporting a high number of nodes, which is a common difficulty in the Internet of Things (IoT). Additionally, it is not feasible to handle wireless network operations and applications independently due to their strong coupling. Consequently, we must zero in on a communication paradigm that serves various application needs in a heterogeneous, efficient, and scalable manner while also complementing and integrating with current technologies. 5G is an excellent choice for diverse situations in this regard. Similarly, VANET makes use of several networks, including WSN, the Internet of Things (IoT), CC, and others, in addition to the vehicles on the road. Thus, the aforementioned developments in computing, communication, processing, and storage can be utilised to access the capabilities of 5G. In VANETs or the so-called Internet of Vehicles (IoV), it may handle a large number of communication links all at once. in the 45th

B. Architecture for VANETs Using 5G

The 3GPP group has been hard at work standardising LTE-V and developing solutions for vehicle-to-element communications. The Long Term Evolution (LTE-V) standard introduces two modes: the centralised LTE-V-Cell mode and the decentralised TD-LTE Direct mode. A new decentralised design called LTE-V-Direct modifies the TD-LTE physical layer to preserve the short-range direct communication feature, increase reliability, and provide low latency, in contrast to the older DSRC. Both DSRC and LTE-based systems will coexist soon [60]. With the help of Fig. 2, we can see the three levels of 5G-enabled vehicular networks' architecture: vehicle, network, and application.

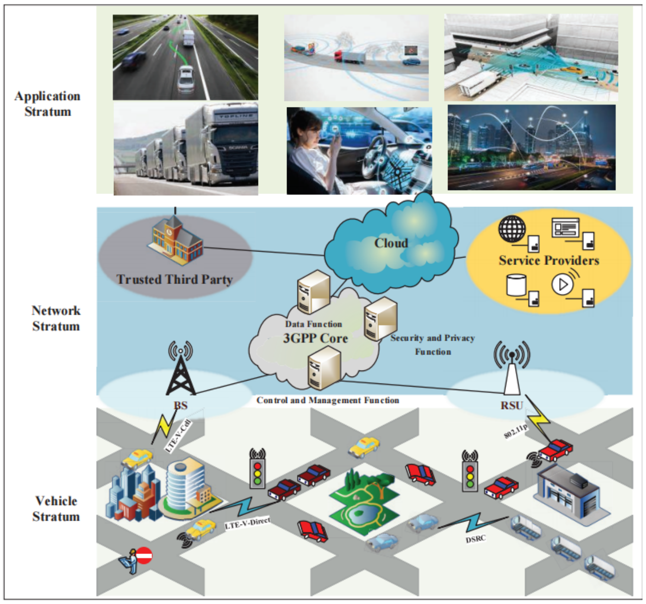


Fig. 2. Architecture for VANETs Using 5G [61]

Working tirelessly, the 3GPP group has standardised LTE-V and created solutions for communications between vehicles and elements. Two new modes, LTE-V-Cell and TD-LTE Direct, are part of the Long Term Evolution (LTE-V) standard. The LTE-V-Direct decentralised design replaces the DSRC with an updated version of the TD-LTE physical layer that maintains the direct communication capability over short distances while also improving reliability and delivering low latency. In the near future, there will be systems that use both DSRC and LTE [60]. The vehicle, network, and application layers make up the architecture of 5G-enabled vehicular networks, as shown in Fig. 2. functions related to policy control, authentication, and authorization (such as carrying out procedures for secure channel formation and access authentication, among others). The primary function of DF is to forward packets. When vehicles access the core network, SPF can store crucial materials and provide security and privacy services. A certificate authority (CA) handles certificate management, and a trusted identity manager (TIM) handles the actual vehicle identities for various uses; these two components make up the trusted third party (TTP). In 3GPP, there are four distinct kinds of vehicle-to-X applications: vehicle-to-infrastructure (V2I), vehicle-to-vehicle (V2V), vehicle-to-network (V2N), and vehicle-to-pedestrian (V2P).

C. VANETs Using 5G with Internet of Vehicles (IoV)

The Internet of Vehicles (IoV) is a hot subject right now, touching on topics like smart cities, data security, and autonomous cars. 5G's low latency, high connection density, and high data speeds are grabbing a lot of attention on VANET. Recent experiments with 5G-enabled VANET have focused on improving data connectivity and traffic safety. 5G makes a huge difference in traffic safety and management thanks to its faster data transfer, real-time vehicle-to-vehicle and vehicle-to-infrastructure connections, and its high resilience and network failure recovery capabilities. These projects are crucial for a better, safer, and more efficient transportation system since they promote advancement in the Internet of Vehicles area. Research on the Internet of Things (IoT) and 5G-enabled VANETs is summarised in the following.

- Higher Data Rates: Faster and more efficient vehicle-to-vehicle communication is possible with 5G's increased data rates. When it comes to enhancing traffic safety, autonomous cars are a major concern because they are able to communicate and share data amongst themselves thanks to sensors and artificial intelligence.
- Low Latency: With 5G's ability to enable low-latency, real-time communication between vehicles and infrastructure, traffic safety can be enhanced. Several aspects of smart city development, including parking, traffic control, energy conservation, and sustainability, can be aided by the Internet of Vehicles.
- Higher Connection Density: More infrastructure and vehicle gadgets may interact at once with 5G's increased connection density. Protecting sensitive information during inter-vehicle communication is a top priority. Data encryption, authentication, and intrusion detection systems are all part of this category of security measures.
- High Reliability: Critical applications like emergency communication and traffic coordination can benefit from 5G's increased reliability in vehicle-to-vehicle communication.
- Network Outage Fix: 5G is designed with specific features that ensure continuous service, even when the network is down.

D. Interactions Between Heterogeneous Devices

The variety of verbal network transactions makes big data, with its high data volume, numerous data picks, and stringent quality of service requirements, challenging to send via the IoV. A issue for contemporary VANETs is the provision of transition requirements for distinct IoV purposes. After that, for each unique application, the transition methods are summarised and placed into categories. We are looking into MAC and routing protocols for state-of-the-art IoV. Fig. 3 shows a high-level paradigm for the creation of such IoV systems in relation to cloud computing, LTE, or 5G.

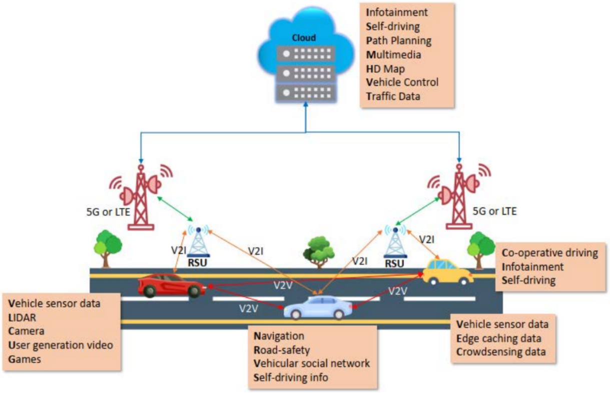


Fig. 3. The scenario of cloud-to-LTE or 5G VANET connectivity and data interchange in the IoV platform [62]

1) Transmission Needs and Applications: In order to sell digital ads, mobile advertising programmes have chosen a variety of small public vehicles, including buses and taxis. It is mandatory for every vehicle to periodically transmit its location, speed, acceleration, and title direction to all other cars in the area. The short size of security messages—typically 200-500 bytes—means that these capabilities require a decreased transmission rate (DSRC Committee, 2009). To draw the attention of drivers operating heavier vehicles, these announcements or advertisements can be transmitted over longer distances than safety warnings. It is possible for commercial records to be continuously released via the network via the link between the seed motor and others in a vast area [63].

2) Challenges with Wireless Channels: Significant and ever-changing factors affecting V2V link performance in scenery include tall buildings, tunnels, overhead bridges, lengthy roadways, and the condition of time-altered traffic. Because of these obstacles and multipath fading, Wi-Fi channels break down [64].

3) Shortage of Spectrum Resources: The DSRC standard includes multiple service channels (SCH) and one control channel (CCH) that offer 10 MHz and 20 MHz bandwidths, respectively, as options. However, the 75 MHz of licenced spectrum that the FCC has given the DSRC is not enough to guide IoV transmission in dense environments for applications that are rich in media [65].

4) High Mobility: Overwhelming traffic frequently interrupted Wi-Fi connections between moving vehicles and under-capacity road infrastructure. In addition, factors such as speed, acceleration, road layout, visitor lights, riding behaviour, and movement connected to site restrictions all impact channel effective resource allocation, routing protocol structure, and message reception [66].

5) The Density of Dynamic Vehicles: Cities and highways often have high vehicle densities, but suburban areas and highways often have extremely low densities [67]. The fundamental and unanswered topic is how processes might adapt to various vehicle densities in a way that prevents channel aid from being squandered at low densities and minimises channel congestion at high densities.

6) Lack of International Collaboration: Due to the vast geographic scope and diverse range of community admissions covered by IoV, the establishment of a central coordinator for the initiative presents unique challenges. In an effort to work around these limitations, IoV transmission systems are spread out.

IV. Use Cases

As shown in Fig. 4, the use case for security of VANET using 5G technology as follows.

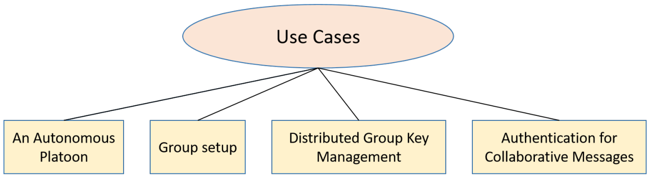

Use Cases
An Autonomous Platoon
Group setup
Distributed Group Key Management
Authentication for Collaborative Messages

Fig. 4. Types of Use Case

A. An Autonomous Platoon

The most important use case for 5G is autonomous driving. Platooning is an effective way to increase road capacity, according to research, as shown in Fig. 5. This is because it reduces the distances between cars or trucks via electronic (and maybe mechanical) linking. The vast majority of autonomous vehicle fleets will use this style of driving [68], [69]. Automated technology in semi-trucks is now being tested by a number of businesses, including Volvo. Vehicle fleet trains, consisting of multiple autonomous vehicles following a predetermined course and led by a platoon leader, greatly enhance vehicular networking performance and pave the way for future cooperative communication applications. Though this driving behaviour will be useful for future intelligent transportation, we must prioritise security and privacy concerns before releasing these technologies to the public.

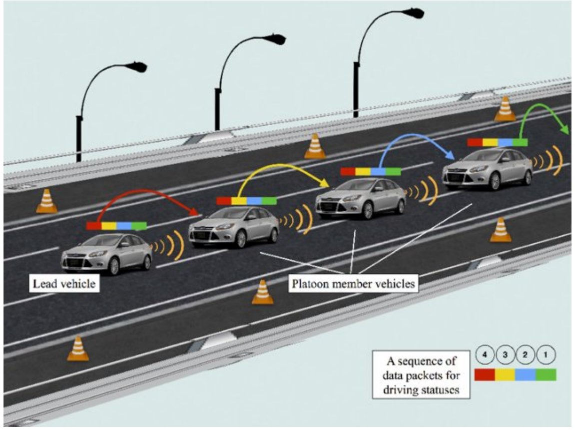


Fig. 5. A platoon of vehicles [70]

Using an autonomous platoon as an example, we look at the privacy and security concerns and offer various solutions. A platoon can be formed in one of two ways: with a fixed trustworthy member or with a dynamic untrusted member. When it comes to vehicles owned by individuals, the former can form weak ties only when they are physically close by, while the latter is more appropriate for vehicles controlled and managed by a company, such as a transportation fleet, where a pre-established trust relationship already exists. As a result, their connection is fleeting and based on mistrust. The focus of this section is on the second scenario.

B. Group Setup

The social aspect is offered by 5G-enabled self-driving cars [71]. A fleet of nearby cars can be formed. Autonomous vehicles with 5G connectivity will encourage passengers to work together by having them run an algorithm to gauge their social skills. Collaboration is essential for group growth and knowledge exchange. The most straightforward way to submit vehicle qualities is through collaborative attribute sets. Every aspect of CAS reflects some aspect of the traveler's history, hobbies, or goals. During neighbourhood discovery, you have the option to manually input vehicle cooperation traits. Examining shared characteristics enables vehicles to work together.There are two drawbacks to this method. Be wary of unfamiliar vehicles. Cooperating vehicles require trust.

Proprietorship of blockchain trust [72]. Chats are validated by a nearby car. Once validated, the vehicle can go on to rate message source vehicles and upload them to BSs or RSUs. BSs and RSUs use car ratings to determine trust and prohibit it. Mine trust blockchains with every BS/RSU. Trust blockchains are maintained by all BSs/RSUs by consensus. Before adopting a vehicle, the entire company verifies its legitimacy. Vehicle characteristics are not known prior to a merger. These qualities are known even by temporary couples. As an illustration, every vehicle possesses ten distinct characteristics. Turn 6 on, and vehicles with more than 6 features will function. Collaborative attribute matching with privacy protection is the goal of multi-party PSI [73]. It is possible for several people to anonymously calculate dataset intersections. According to Fig. 6, secure groups value privacy.

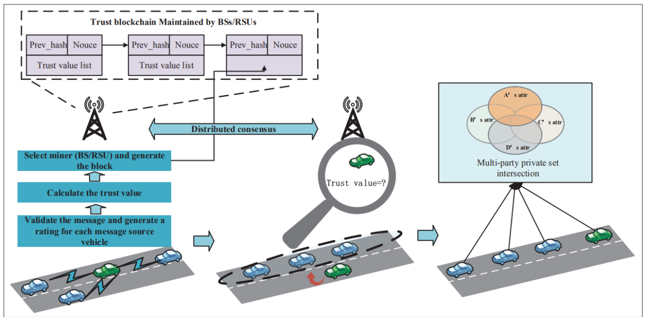
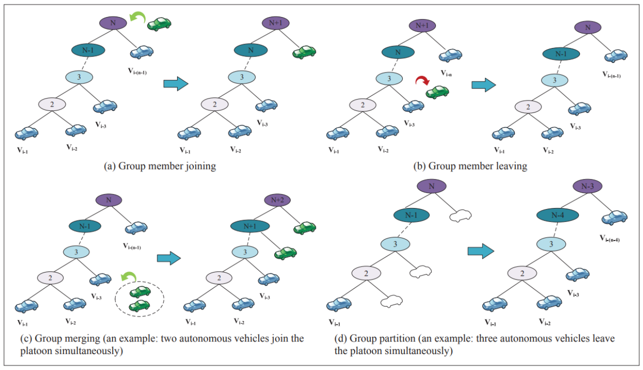

Trust blockchain Maintained by BSs/RSUs
Prev_hash
Nouce
Trust value list
Prev_hash
Nouce
Trust value list
Prev_hash
Nouce
Distributed consensus
Select miner (BS/RSU) and generate the block
Calculate the trust value
Validate the message and generate a rating for each message source vehicle
Trust value=?
A′ s attr
B′ s attr
C′ s attr
D′ s attr
Multi-party private set intersection

Fig. 6. Setup of a secure group while protecting individual privacy [61]

C. Distributed Group Key Management

Two scenarios, SEGM-I and SEGM-II, are taken into account by Lai et al. [74] when they offer a secure group management framework for integrated vehicular ad hoc network (VANET)-cellular networks. In contrast to SEGM-I, which is intended for use with fixed trusted members, SEGM-II is tailored to handle more generic cases, such as those including dynamic untrusted members. According to SEGM-II's inherent topology, an autonomous driving fleet's composition can vary rapidly, and cars can join or exit the fleet at any moment. Consequently, a difficult challenge is how to design dispersed group key management to facilitate flexible autonomous vehicle fleet management. Key generation protocols that contribute (CKGPs) are applicable in this case. Everyone in a CKGP-based distributed group key management system can guarantee that their contributions are completely random, making it impossible for anybody else to guess anyone else's secret key or determine the group's final key without everyone's input. Because everyone in the group has an equal say in creating the keys, CKGP is just. Among the many operations that the suggested distributed group key management can facilitate are: (I) Adding a member to the group: With a credit system and privacy-preserving attribute matching, a new autonomous vehicle can join the fleet. (II) Departure from the group: For various reasons, including malevolent actions, an autonomous vehicle may be expelled from the fleet. (III) Merging into an existing fleet: a new breed of autonomous vehicles is in the works. (IV) In certain cases, a subgroup is separated from the fleet through group partitioning. Organisational structure is based on the Skinny TRee (STR). Fig. 7 shows an autonomous platoon with distributed group key management in action, with Vi-j standing for the ith group's jth vehicle.



(a) Group member joining

(b) Group member leaving

(c) Group merging (an example: two autonomous vehicles join the platoon simultaneously)

(d) Group partition (an example: three autonomous vehicles leave the platoon simultaneously)

Fig. 7. Group key management in a distributed system: a) adding members; b) removing members; c) merging groups; and d) partitioning groups [61]

D. Authentication for Collaborative Messages

Each autonomous car updates neighbouring vehicles on its status and road conditions for safety. Reliable autonomous platoon services require message authentication. Authentication methods are computationally and communicationally expensive [75]. Fixed trustworthy member and dynamic untrusted member cooperative message authentication for autonomous driving fleets can overcome these constraints because vehicles may belong to various groups. This is perfect for trusted relationships. A company's car fleet or comparable autonomous vehicles can collaborate. Group key agreements allow pre-sharing. MAC messages authenticate cooperatively.

Second type is better for dynamic untrusted members. Anonymous message authentication works best for broadcast vehicle position tracking. Linkable ring signatures verify cooperative messaging [76]. Ring signatures enable anonymous group messaging. Trusted third parties can identify ring signatures. Combining n signers' signatures on n messages into one unit-length signature cuts communication costs.

Because our system authenticates using the flock as a unit, rather than each vehicle broadcasting its message like most existing schemes, we are able to drastically reduce the number of messages needed for authentication. Also, within each group, members will use an authentication mechanism based on symmetric cryptography, and across groups, they will utilise authentication technology based on public key cryptography, which may effectively lower the authentication computation and transmission overhead. Fig 8a depicts the fundamental concept of cooperative message authentication within a group, whereas Fig. 8b shows the same concept between groups.

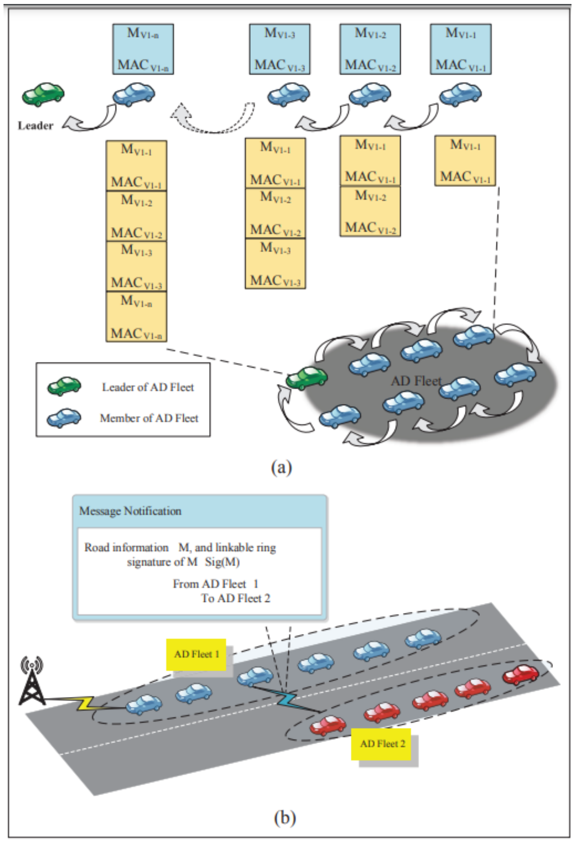


Fig. 8. The two main types of cooperative message authentication are (a) authentication within a group and (b) authentication between groups [61]

V. Taxonomy of Security in 5G-VANETs

This section briefly provides the taxonomy for security of 5G-VANET works as follows.

A. SDN enabled 5G-VANET

Duan et al. [77] proposed an SDN-enabled 5G VANET by clustering neighbouring vehicles adaptively according to real-time road conditions using SDN's global information collecting and network control capabilities to accommodate rising traffic and improve Het-Net management. With twin cluster head architecture and dynamic beamforming coverage, trunk link communication quality and vehicle cluster network robustness improve.

Kachhoria et al. [78] investigated how flexible optical networks can combine adaptive SDN with V2V communication in 5G. As the auto industry progresses towards 5G integration, commercial V2V (C-V2V) technology could revolutionise wireless infrastructure by eliminating the requirement for short-range contact methods.

Saleh et al. [79] examined the deployment of 5G technologies, particularly SDN, to satisfy the ultra-low delay and reliability communication needs of level-2 autonomous vehicle delegation to the Remote-Control Centre (RCC). Our edge-deployed deep-learning-based approach detects drowsy drivers to prevent accidents and traffic congestion. Deep learning-based models outperformed conventional methods in accuracy, precision, and recall.

B. Blockchain enabled 5G-VANET

The benefits of blockchain for 5G-based IoV are examined by Karim et al. [80]. BSDCE-IoV, a blockchain-based secure data exchange mechanism based on Elliptic Curve Cryptography, is proposed and evaluated. Our method eliminates various IoV vulnerabilities. Real-or-Random oracle model and Scyther tool analysis, along with informal security study, validate the scheme's security and privacy.

Dwivedi et al. [81] aimed to integrate blockchain technology into VANET and create a strong handover authentication protocol to address the aforesaid issues. They use the hash function and Elliptic Curve Cryptography to build blockchain-based mutual authentication and session key agreement protocols for intra-vehicular and inter-vehicular (handover case) scenarios.

C. Fog Computing Enabled 5G-VANET

Farooqi et al. [82] established a priority-based fog computing paradigm for smart urban vehicle mobility to reduce fog computing latency. To meet latency and QoS requirements, 5G localised Multi-Access Edge Computing (MEC) servers were utilised to improve the fog computing infrastructure, which greatly reduced delay and latency.

Nkenyereye et al. [83] suggested a secure and privacy-preserving 5G fog-based IoV collision avoidance system in this paper. Fog devices capture vehicle speed sensor TVR. Fog nodes aggregate numerous TVRs, authenticate their signatures, and send anonymous notifications to nearby entities. The protocol uses certificateless aggregate signcryption and pseudonymous techniques for authentication, integrity, secrecy, and privacy.

For fog resource availability to aid offloading, Maan et al. [84] proposed the Kalman filter prediction scheme to forecast the vehicle's next location. Deep Q network-based reinforcement learning selects VANET's resource-rich fog node.

D. VANET using 5G

MAT assigns dedicated nodes (with common distance from both vehicles) to monitor message forwarding and routing behaviour in information trust by Perarasi et al. [85]. The particular node drops all information after time out, making this approach beneficial for predicting an exact intruder.

Das et al. [86] presented an architecture that combines existing security requirements and 5G security standards for a safe 5G-enabled VANET paradigm. It also addresses security challenges to enable a secure and efficient 5G-VANET integration and lays out a trust management system to boost 5G-enabled VANET performance.

A fog-based DDoS detection method that uses fuzzy logic to distinguish attack traffic from regular traffic in 5G-enabled smart cities is proposed by Gaurav et al. [87]. Thier suggested technique properly identifies DDoS attack traffic with over 90% precision and true negative rate.

E. Machine Learning Enabled 5G-VANET

Tayyaba et al. [88] presented a flow-based policy framework for SDN-based vehicular networks employing two-tier virtualization. Wireless virtualization allows vehicle-to-vehicle (V2V) communication by allocating radio resources based on flow classification, such as safety-related or non-safety flows, and letting the controller manage the vehicular environment and V2X communications.

Selvakumar et al. [89] suggested a microgrid-based energy management and monitoring system. Creating an energy management microgrid is the goal. VANET monitoring data is analysed using reinforced layered adversarial neural networks.

Sharma et al. [90] proposed a 5G smart home security protocol using Sailfish-based Distributed IP Mobility Management (SbDMM). A Home Gateway communicates with IoT devices in smart homes.

F. Existing problem and solutions

The integration of 5G cellular networks with VANETs, or Vehicular Ad-hoc Networks, opens up promising avenues for the transportation of the future. Having said that, we still have a ways to go:

- Security: The increased data interchange and new types of applications in 5G networks necessitate changes to traditional VANET security.
- Localization services: Many 5G-VANET applications rely on precise location data. Still, a network of cars that are continually on the go presents unique challenges when it comes to reliable localization and effective management.
- Protocols for broadcasting: Message broadcast optimisation for reliability and delay reduction is critical as the network handles more vehicles and data.

Many potential answers to these difficulties are being considered by researchers:

- Securing 5G networks with VANETs: The development of new security protocols that take 5G-VANETs' specific features into account is of the utmost importance.
- Using traffic infrastructure as a foundation, location services: One such option could be to use the roadside infrastructure, such as traffic lights, for location management.
- Enhanced protocols for broadcasting: Creating new protocols that make use of 5G's features to decrease latency and increase message delivery dependability.

When it comes to transportation, 5G-VANETs have the ability to completely transform the industry. A future where roads are safer, more efficient, and more connected can be achieved by tackling the current difficulties through continual study.

VI. Open Challenges and Future Directions

More investors should get behind the commercialization of VANET if we want safe 5G-based VANET applications and services, and more people should use VANET services every day. Consumers will also have access to the CPS ecosystem, which comprises smart homes, healthcare, transportation, offices, and more, as 5G-based VANETs become more commonplace.

There are a number of problems that conventional VANET security standards failed to resolve, however 5G's security services for the VANET are an encouraging improvement. Nevertheless, there are new obstacles that must be overcome prior to the commercial launch of 5G-based VANETs brought about by the introduction of 5G to VANETs. This article discusses some of the impending challenges and possible solutions related to 5G and VANET security research, as shown in Fig. 9.

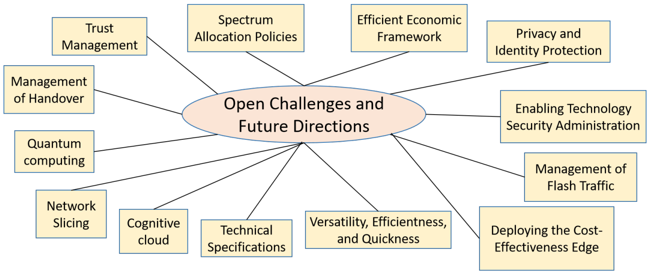

Trust Management
Spectrum Allocation Policies
Efficient Economic Framework
Privacy and Identity Protection
Management of Handover
Open Challenges and Future Directions
Enabling Technology Security Administration
Quantum computing
Management of Flash Traffic
Network Slicing
Cognitive cloud
Technical Specifications
Versatility, Efficientness, and Quickness
Deploying the Cost-Effectiveness Edge

Fig. 9. Open Challenges and Future Directions for Security of VANET using 5G

A. Efficient Economic Framework

Due to their interactions with other nodes and their environment, vehicular nodes in VANET generate a substantial volume of data. Communication over cellular networks, like 5G, will not come without cost; users may need to pay for data plans. In addition, the service providers' viewpoint should include Return on Investment (RoI). Providers of these services will also need to address the issue of hardware cost by developing a tangible, consumer-friendly business model. This matters since it has a direct impact on how popular this integration becomes and how interested people are. Payment models like pay-as-you-go, pay-per-use, pay-per-service, and others might be updated to offer consumers more options. Alternatively, service providers should think about processing and storage accordingly. Consumers must also be assured of acceptable security and privacy.

B. Management of Handover

Present VANET implementations take advantage of the dense deployment of RSUs, which allows for mobility, the apex of VANET. Given the design of 5G cellular networks, it is typical for network entities (such as Base Transceiver Stations, or BTSs) and service providers to undergo frequent handovers. To ensure authentication, secrecy, and other essential security features in VANET applications, it may be necessary to transfer cryptographic keys, identities, and certificates to the new cells. Consequently, we need devise systems for effective handoff management. One approach could be to adopt 5G's umbrella cell idea, where a single giant cell oversees multiple smaller micro-cells and covers a wide region to accommodate mobile nodes. To minimise frequent hand-overs, the connection for high-speed nodes like connected trains and trucks could be managed by the umbrella cell. Further research of the security management at the umbrella cell is still underway, nevertheless.

C. Privacy and Identity Protection

One more thing that car networks have to worry about is privacy protection. 5G wireless networks are transmitting massive amounts of sensitive data, and the open nature of these networks is causing some to worry that this data could be leaked. The majority of VANET services rely on precise user identification and location data. Users' and their locations' privacy, however, is of paramount importance to them. Currently, VANET security guidelines include using temporary identities (pseudonyms) and other cryptographic primitives for user identity, and mix-zones and silence intervals for location privacy [91], [92]. To add to that, location privacy is further enhanced using location-based encryption [93]. Cellular networks, on the other hand, use a unique hardware component called a Subscriber Identification Module (SIM) to verify the identity of each user. If we care about protecting users' identities and where they are, we need to look into hardware-based identity management more. Importantly, 5G enables identity management, meaning that several devices can be associated with a single subscriber (which is great news for the IoT and healthcare networks), but we still need to learn more about the privacy needs and how to meet them. The 5G communication paradigm could be used to modify some current technologies, such as [94] and [95], for use in VANET applications.

D. Technical Specifications

Problems arise when 5G designs incorporate network slicing. The lack of precise operational specifications is the main source of most of the worries around network slicing. For example, in order to provide a genuinely modular solution for various sliced networks, it is crucial to meticulously translate and classify the requirements of automotive applications into technical standards. This will make sure that changes made to one slice of the network are automatically reflected in the others, and that no one slice of the network affects another.

E. Spectrum Allocation Policies

The distribution of spectrum for automobiles is another obstacle with ProSe. Dynamic allocation is possible using policies that take into account the vehicle's viewpoints, such as message priority, QoS, and security. On top of that, the eNB can statically assign spectrum to cars in a static configuration. A key component of the Internet of Things (IoT) ecosystems in future 5G scenarios will be automobiles, which will play a role in auxiliary communications beyond safety [11]. What this means for the degrees of interference between vehicles using the same frequency band for both gearbox and reception is unclear.

F. Quantum Computing

The automobile industry is looking to quantum computing as the technology of the future. The quantum revolution is being facilitated in large measure by electric vehicles. In order to address a wide range of issues, car manufacturers have begun to use quantum computers. For AI in VANET to analyse and respond optimally in dynamic settings, massive amounts of data are required. A lot of processing power and speed in AI is needed to find the best route based on real-time vehicle locations [96]. Quantum computers are capable of achieving the first characteristic, which is enormous processing power. Volkswagen, a German automaker, worked with D-Wave systems to plan and implement quantum computing-based traffic routing in Beijing. Optimisation issues, such as waiting times, fleet deployment, etc., can also be solved by these systems. Additionally, Volkswagen and Google have collaborated to foresee traffic conditions in order to prevent accidents, model the operation of electrical components, and incorporate artificial intelligence into autonomous vehicles. Due to their increased exposure to the outside world, AVs can be protected from security breaches using quantum technology. To implement AV, massive computational resources are needed, for example, to improve route planning and transform transportation networks into intelligent ones. Through internal and external communication, the vehicles will acquire intelligence. To reap the benefits of processing power and computation, more advancements in the area of VANET coupled with quantum computers are anticipated.

G. Network Slicing

The categorization of user needs is another consideration for deciding whether network functions should be centralised or sliced. Network slicing is still in its early stages with vague technological requirements. Possible justifications for network segmentation in a vehicular context include service kinds offered, the needs of quality of service applications (such as infotainment and Internet access), and the resources at hand.

H. Enabling Technology Security Administration

The virtualization and softwarization of network control through 5G allows for efficient and easy network management. But it also gives hackers a chance to launch network attacks through security holes. The tried-and-true methods of addressing security vulnerabilities through hardware are still very much in use today. Consequently, network security could be compromised due to the paradigm shift towards software-based network control. Because people's lives are on the line while utilising a VANET safety application, additional research into the security of software-based network control through SDN in 5G is necessary. As a corollary, this softwarization necessitates consideration of privacy, identification, and other security concerns. From an integration perspective, VANET and 5G need more research into access control vulnerabilities, malicious applications, and distributed denial of service (DDoS) assaults because of the potential impact on VANET applications. Saturation attacks on network controllers and exploits of malicious APIs are two further types of assaults. Furthermore, VANET's auditability, security provisions, and other critical functions could be compromised due to configuration errors in SDN and NFV, which in turn could impact mobile networks. In addition, denial-of-service (DoS), side-channel, and hypervisor takeover attacks are all possible with NFV [97]. To make the 5G-driven secure VANET a reality, we need to find and fix the security flaws in the enabling technologies.

I. Deploying the Cost-Effectiveness Edge

Considering the cost-effectiveness of large-scale deployment is crucial, as the fundamental objective of MEC is to minimise latency by bringing services closer to the customer. This is especially important for vehicle networks since RSUs can contain cloud services in addition to eNB stations. Nevertheless, it is expensive to deploy RSUs and eNB stations over entire vehicle networks. The security, processing, and storage needs of specifically designed hosted services should also be carefully considered. Moreover, data that is normally kept in the cloud, like driver details, vehicle identification, destinations, and routes, cannot be maintained on eNBs/RSUs due to security considerations (e.g., confidentiality).

J. Trust Management

There is an enormous amount of data exchanged between various VANET units. Reliable data sharing is crucial to the VANET's apps and services as well as the 5G enabling technologies. Hence, it is imperative to ensure trust in both entities and material. Several methods, including cryptographic and non-cryptographic ones, are employed in conventional VANETs to create and maintain trust among various nodes in the network. Nevertheless, conventional methods of establishing trust may not be applicable when new service types like cloud, IoT, SDN, etc. are incorporated. This calls for fresh approaches to managing trust and reputation. Establishing confidence in VANET while using 5G networking becomes more challenging due to the huge quantity and heterogeneity of information sources. Several studies and proposals for cryptographic solutions have addressed the issue of secure data transfer over 5G-enabled VANET [98]–[100]. As an example, a system model for secure video transmission in 5G-enabled VANET was proposed by Eiza et al. [98]. But it's not easy to build trust across entities, and old methods like social proof, recommendations, and others may not cut it. Because various application contexts may have different security requirements, context is also crucial in establishing trust (entity trust and content trust). Consequently, 5G-enabled VANETs require efficient and adaptable trust mechanisms.

K. Versatility, Efficientness, and Quickness

The security solutions implemented for VANET applications using 5G networking need to be adaptable and efficient. The storage and computation demands of cryptographic methods are often high, which has a negative impact on VANET applications in terms of efficiency. One of the many difficulties that will arise from incorporating additional enabling technologies is the requirement for optimised security solutions in devices with limited resources [101]. Because every application and service has unique security needs, it's crucial to be able to adapt to meet those needs with ease. Vastly expanded opportunities for innovative VANET services are presented by the ultra-low latency promised by 5G. While guaranteeing promised security is important, achieving the ultra-low latency aim also requires appropriately built and optimised security solutions. In 5G, lowering the signalling overhead could be a solution [102], [103]. That is why this field need further study. While 5G is a good fit for safety-critical VANET applications because to its ultra-low latency requirements, meet those requirements with efficient and lightweight cryptographic solutions [91]. Redesigning the control plane such that it is located close to the centre of gravity could be one way to increase efficiency. Provisioning of security resources, from an agility perspective, would be application- and context-specific. So, security management systems need to be flexible to accommodate the needs of various applications and services. Further research is necessary regarding this matter.

L. Cognitive Cloud

Particularly at level 5 VANET, cognitive AI and algorithms would allow us to mimic human-level performance. To meet the requirements of the level 5 VANET—which include precise decision-making, object-detection, and localization—in unpredictable environments like heavy rain, thick fog, or complete darkness—is no easy feat. To get near human-like performance in areas like object detection and decision-making, cognitive computing improves the accuracy of the models. Cognitive computing's incorporation into VANET enhances both precision and security. With the help of the Cognitive Internet of Vehicles, autonomous vehicles can learn what, how, and where to compute in a way that mimics the human brain.

M. Management of Flash Traffic

The connectivity between vehicular nodes, other cars, and the infrastructure in their immediate vicinity causes massive volumes of data to be generated. Personal information, control information, mobility traces, and more are all part of this data set. The rapidity and volume of this data makes big data methods ideal for making VANET applications a reality. One example is the millisecond-scale intervals between cooperative awareness messages exchanged by each VANET vehicle. Consequently, nearby nodes would produce a deluge of data in the event of heavy traffic. Internet of Things (IoT), electronic health records (e-health), traffic management, and other similar applications could potentially make use of this data as well. Access control, access rights, integrity, privacy, and similar security needs must be satisfied for each user in a 5G-enabled VANET in order to manage and process such massive amounts of data efficiently. In addition, for various applications' quality of service needs to be satisfied, these mechanisms need to be efficient. To manage the massive amounts of network data created, optimised big data approaches and in-network caching could be employed. But in the future, additional studies will be required in this field.

VII. Results and Analysis

This section discusses abcomparative analysis of recent AI-based and security-enriched architectures for 5G-VANET scenarios. As illustrated in Fig. 10, we emphasize the three most important performance measures: detection accuracy, latency, and overall security robustness. The proposed mechanisms–itselfbdrawn from recent works–comprise a wide range of intelligent vehicular communication systems that combine different modalities like AI, blockchain, fog computing, SDN and machine learning.

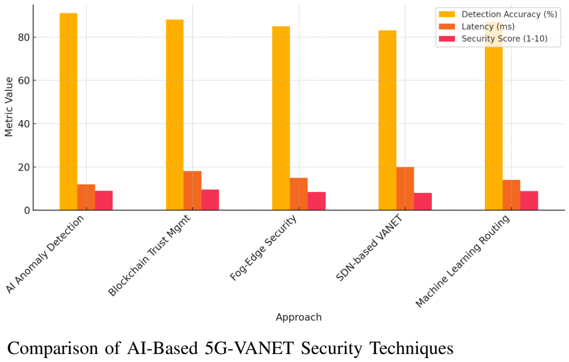


Fig. 10. Comparison of AI-Based 5G-VANET Security Techniques

In this group, AI-led anomaly detection models excel in their accuracy, with detection rates as high as 91% for threats like spoofing or intrusion attempts. These models also achieve an average low latency of 12 ms, which makes them suitable candidates for safety critical applications in VANETs such as collision avoidance and real time hazard warning. The combination of deep learning that are being infused into the network and light weight inference mechanisms for such systems will go on to react fast without sacrificing content precision especially when deployed at the edge by means of MEC.

The highest security assessment score (9.5/10) is provided for blockchain-based trust management schemes, certifying their capability to maintain data integrity, and traceability consistency, and decentralized trust with heterogeneous VANET nodes. But this performance isn't without compromise, as it also has a low response time of 18 milliseconds, which means that time critical vehicle to everything (V2X) communication could be affected. They are more appropriate for secure identity management, group authentication and electronic data provenance, where multiple parties work together.

Whereas fog-edge security implementations, leveraging the distributed nature of edge devices to perform threat detection and process vehicular information, provide a balance. With a detection accuracy of 85%, and a latency of 15 ms, and security score of 8.5, they excel in applications where centralized infrastructure connectivity is constrained or intermittent.

SDN-based VANET architectures while less accurate in detection rate and security score (83% and 8.0, respectively) offer architectural versatility. Their global control can be employed to support large-scale dynamic network orchestration, spectrum slicing, and flow-based policy enforcement- in heterogeneous network scenarios in particular.

Finally, routing algorithms derived from machine learning perform well in all parameters. They are shown to be applicable to adaptive path selection, congestion prediction and QoS-sensitive traffic steering with 87% accuracy at 14 ms latency and 8.8 security strength. Such techniques greatly benefit from data-driven reinforcement learning and optimization algorithms which are tailored to the dynamics of vehicular mobility as well as environmental conditions.

In general, no model dominated across all performance measures, highlighting the importance of a hybrid solution that integrates the predictive strengths of AI with the integrity of blockchain and the real-time capabilities of edge-based models. This evidence confirms the hypothesis of this paper: 5G-VANET security designs need to include AI-driven intelligence in order to secure our future transportation systems in a scalable, secure, and timely fashion.

VIII. Conclusion and Recommendation

The integration of Artificial Intelligence (AI) and 5G based Vehicular Ad Hoc Networks (VANETs) is a vital stepping stone for intelligent, autonomous and secure transportation systems. This paper provided a comprehensive survey on AI-based components in 5G-VANET structures, like random anomaly detection, cooperative trust-based models, DDoS and distributive key management system and real-time learning-based state decision engines. By using AI in combination with the enabling technologies such as SDN, MEC, and blockchain technologies, the proposed framework overcomes essential problems such as latency, security, and scalability in vehicular communications. Real-world applications such as autonomous platooning and collaborative message authentication shows practicability of AI-aided vehicular networks. Yet, there are still many open issues begging for solution, including the privacy-respecting, quantum safe communication, and the trust building process in a dynamic manner. In future, light and context-aware AI models and cognitive computing must be used to enable 5G-VANETs to transform into completely autonomous and trustworthy transportation systems.

Due to its many advantages over other cellular generations, it believes 5G is the best option for Vehicular Ad-hoc Networks (VANETs):

- Improvements in Communication and Data Exchange: In order to improve traffic management, encourage cooperative driving, and avoid collisions in real-time, ultra-reliable low-latency communication (URLLC) allows cars to transmit crucial safety information with minimal delays. Wide data transfer rates: Allows for the transfer of massive data sets, including as HD maps, live video streams, and sensor readings, which are essential for autonomous driving and advanced driver assistance systems (ADAS).
- Effectiveness and Expandability of the Network: The ability to connect a large number of vehicles and roadside units (RSUs) seamlessly is crucial for large-scale smart transportation system deployments, and massive machine-type communication (mMTC) provides just that. Network slicing allows for the development of specialized virtual networks for use with VANETs, which improves performance and allows for more efficient use of available resources.
- Enhancement of the User Interface: Safeguarding sensitive data shared within the network against cyberattacks and illegal access, robust authentication and encryption measures enhance security. Minimizing delays in data transfer reduces latency, which in turn improves the user experience for connected-car services and allows crucial safety applications to respond faster.
- The combination of 5G-VANET with other new technologies, such as Multi-access Edge Computing (MEC), also encourages: Processing and analyzing data in real-time: Autonomous vehicles can transfer computing activities to servers at the network's periphery, allowing for better traffic flow management and faster decision-making. Supports connected and autonomous vehicles better by laying the groundwork for real-time communication, collaboration, and data exchange between vehicles and roadside infrastructure, which in turn allows for the creation and implementation of cutting-edge automotive technology.

Acknowledgment

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. KFU251783).

References

[1] J. B. Kenney, "Dedicated Short-Range Communications (DSRC) Standards in the United States," in *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162-1182, 2011, doi: 10.1109/JPROC.2011.2132790.

[2] M. A. Al-Shareeda, M. A. Saare, and S. Manickam, "Unmanned aerial vehicle: a review and future directions," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 30, no. 2, pp. 778–786, 2023, doi: 10.11591/ijeecs.v30.i2.pp778-786.

[3] M. R. Alboalebrah and S. Al-augby, "Unveiling the causes of fatal road accidents in iraq: An association rule mining approach using the apriori algorithm," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 2, pp. 1–11, 2025, doi: 10.63180/jcsra.thestap.2025.2.1.

[4] J. Clancy *et al.*, "Wireless Access for V2X Communications: Research, Challenges and Opportunities," in *IEEE Communications Surveys & Tutorials*, vol. 26, no. 3, pp. 2082-2119, 2024, doi: 10.1109/COMST.2024.3384132.

[5] K. Herman Muraro Gularte *et al.*, "Integrating Cybersecurity in V2X: A Review of Simulation Environments," in *IEEE Access*, vol. 12, pp. 177946-177985, 2024, doi: 10.1109/ACCESS.2024.3504404.

[6] H. Zhong, L. Wang, J. Cui, J. Zhang and I. Bolodurina, "Secure Edge Computing-Assisted Video Reporting Service in 5G-Enabled Vehicular Networks," in *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 3774-3786, 2023, doi: 10.1109/TIFS.2023.3287731.

[7] M. A. Al-Shareeda, A. M. Ali, M. A. Hammoud, Z. H. M. Kazem, and M. A. Hussein, "Secure iot-based real-time water level monitoring system using esp32 for critical infrastructure," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 2, pp. 43–52, 2025, doi: 10.63180/jcsra.thestap.2025.2.4.

[8] B. N. Alhasnawi, S. M. M. Almutoki, F. F. K. Hussain, A. Harrison, B. Bazooyar, M. Zanker, and V. Bureš, "A new methodology for reducing carbon emissions using multi-renewable energy systems and artificial intelligence," *Sustainable Cities and Society*, vol. 114, 2024, doi: 10.1016/j.scs.2024.105721.

[9] B. N. Alhasnawi, M. Zanker, and V. Bureš, "A smart electricity markets for a decarbonized microgrid system," *Electrical Engineering*, pp. 1–21, 2024, doi: 10.1007/s00202-024-02699-9.

[10] O. Aljumaiah, W. Jiang, S. R. Addula, and M. A. Almaiah, "Analyzing cybersecurity risks and threats in it infrastructure based on nist framework," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 2, pp. 12–26, 2025, doi: 10.63180/jcsra.thestap.2025.2.2.

[11] S. Chen, J. Hu, Y. Shi and L. Zhao, "LTE-V: A TD-LTE-Based V2X Solution for Future Vehicular Network," in *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 997-1005, 2016, doi: 10.1109/JIOT.2016.2611605.

[12] A. Hussain, M. A. Saare, O. M. Jasim, and A. A. Mahdi, "A heuristic evaluation of iraq e-portal," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, vol. 10, no. 1-10, pp. 103–107, 2018.

[13] A. A. A. Almazroi, M. A. Alqarni, M. A. Al-Shareeda, M. H. Alkinani, A. A. Almazroey, and T. Gaber, "Fca-vbn: Fog computing-based authentication scheme for 5g-assisted vehicular blockchain network," *Internet Things*, vol. 25, 2024, doi: 10.1016/j.iot.2024.101096.

[14] M. A. AbouElaz, B. N. Alhasnawi, B. E. Sedhom, and V. Bureš, "Anfis-optimized control for resilient and efficient supply chain performance in smart manufacturing," *Results in Engineering* vol. 25, 2025, doi: 10.1016/j.rineng.2025.104262.

[15] M. Saare, A. Hussain, and W. S. Yue, "Investigating the effectiveness of mobile peer support to enhance the quality of life of older adults: A systematic literature review," *International Journal of Interactive Mobile Technologies*, vol. 13, no. 4, pp. 130–139, 2019, doi: 10.3991/ijim.v13i04.10525.

[16] S. Chen *et al.*, "Vehicle-to-Everything (v2x) Services Supported by LTE-Based Systems and 5G," in *IEEE Communications Standards Magazine*, vol. 1, no. 2, pp. 70-76, 2017, doi: 10.1109/MCOMSTD.2017.1700015.

[17] R. Almanasir, D. Al-solomon, S. Indrawes, M. A. Almaiah, U. Islam, and M. Alshar'e, "Classification of threats and countermeasures of cloud computing," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 2, pp. 27–42, 2025. doi: 10.63180/jcsra.thestap.2025.2.3.

[18] B. N. Alhasnawi and B. H. Jasim, "SCADA controlled smart home using Raspberry Pi3," *2018 International Conference on Advance of Sustainable Engineering and its Application (ICASEA)*, pp. 1-6, 2018, doi: 10.1109/ICASEA.2018.8370946.

[19] B. N. Alhasnawi, M. Zanker, and V. Bureš, "A new smart charging electric vehicle and optimal dg placement in active distribution networks with optimal operation of batteries," *Results in Engineering*, vol. 25, 2025, doi: 10.1016/j.rineng.2025.104521.

[20] S. Otoom, "Risk auditing for digital twins in cyber physical systems: A systematic review," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 22–35, 2025, doi: 10.63180/jcsra.thestap.2025.1.3.

[21] M. Shafi *et al.*, "5G: A Tutorial Overview of Standards, Trials, Challenges, Deployment, and Practice," in *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 6, pp. 1201-1221, 2017, doi: 10.1109/JSAC.2017.2692307.

[22] R. Viterbo *et al.*, "Evaluating the V2X Latency for Vehicle Positioning: A Comparison Between 5G-V2X and ITS-G5," *2024 IEEE 8th Forum on Research and Technologies for Society and Industry Innovation (RTSI)*, pp. 271-276, 2024, doi: 10.1109/RTSI61910.2024.10761733.

[23] B. N. Alhasnawi *et al.*, "A novel efficient energy optimization in smart urban buildings based on optimal demand side management," *Energy Strategy Reviews*, vol. 54, 2024, doi: 10.1016/j.esr.2024.101461.

[24] M. Jamil, M. Farhan, F. Ullah and G. Srivastava, "A Lightweight Zero Trust Framework for Secure 5G VANET Vehicular Communication," in *IEEE Wireless Communications*, vol. 31, no. 6, pp. 136-141, 2024, doi: 10.1109/MWC.015.2300418.

[25] D. Soldani and A. Manzalini, "Horizon 2020 and Beyond: On the 5G Operating System for a True Digital Society," in *IEEE Vehicular Technology Magazine*, vol. 10, no. 1, pp. 32-42, 2015, doi: 10.1109/MVT.2014.2380581.

[26] B. A. Mohammed, M. A. Al-Shareeda, Z. G. Al-Mekhlafi, J. S. Alshudukhi and K. A. Al-Dhlan, "HAFC: Handover Authentication Scheme Based on Fog Computing for 5G-Assisted Vehicular Blockchain Networks," in *IEEE Access*, vol. 12, pp. 6251-6261, 2024, doi: 10.1109/ACCESS.2024.3351278.

[27] N. H. B. Jemaludin, A. J. A. Al-Gburi, R. H. Elabd, T. Saeidi, M. F. Akbar, I. M. Ibrahim, and Z. Zakaria, "A comprehensive review on mimo antennas for 5g smartphones: mutual coupling techniques, comparative studies, sar analysis, and future directions," *Results in Engineering*, vol. 23, 2024, doi: 10.1016/j.rineng.2024.102712.

[28] T. S. Rappaport *et al.*, "Millimeter Wave Mobile Communications for 5G Cellular: It Will Work!," in *IEEE Access*, vol. 1, pp. 335-349, 2013, doi: 10.1109/ACCESS.2013.2260813.

[29] R. A. Uzcategui, A. J. De Sucre and G. Acosta-Marum, "Wave: A tutorial," in *IEEE Communications Magazine*, vol. 47, no. 5, pp. 126-133, 2009, doi: 10.1109/MCOM.2009.4939288.

[30] A. A. A. Almazroi, M. A. Alqarni, M. A. Al-Shareeda, and S. Manickam, "L-cppa: Lattice-based conditional privacy-preserving authentication scheme for fog computing with 5g-enabled vehicular system," *PLOS ONE*, vol. 18, no. 10, 2023, doi: 10.1371/journal.pone.0292690.

[31] A. Bazzi, S. Bartoletti, A. Zanella, and V. Martinez, "Performance analysis of ieee 802.11 p preamble insertion in c-v2x sidelink signals for co-channel coexistence," *Vehicular Communications*, vol. 45, 2024, doi: 10.1016/j.vehcom.2023.100710.

[32] J. Härri, F. Filali, C. Bonnet, and M. Fiore, "Vanetmobisim: generating realistic mobility patterns for vanets," in *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, pp. 96–97, 2006, doi: 10.1145/1161064.1161084.

[33] A. A. A. Almazroi, M. H. Alkinani, M. A. Al-Shareeda, and S. Manickam, "A novel ddos mitigation strategy in 5g-based vehicular networks using chebyshev polynomials," *Arabian Journal for Science and Engineering*, vol. 49, pp. 11991–12004, 2023, doi: 10.1007/s13369-023-08535-9.

[34] K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang and Y. Zhou, "Heterogeneous Vehicular Networking: A Survey on Architecture, Challenges, and Solutions," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2377-2396, 2015, doi: 10.1109/COMST.2015.2440103.

[35] Z. Ghaleb Al-Mekhlafi *et al.*, "Oblivious Transfer-Based Authentication and Privacy-Preserving Protocol for 5G-Enabled Vehicular Fog Computing," in *IEEE Access*, vol. 12, pp. 100152-100166, 2024, doi: 10.1109/ACCESS.2024.3429179.

[36] C. -K. Toh, "Future Application Scenarios for MANET-Based Intelligent Transportation Systems," *Future Generation Communication and Networking (FGCN 2007)*, pp. 414-417, 2007, doi: 10.1109/FGCN.2007.131.

[37] A. S. Akhter, M. Ahmed, A. Anwar, A. S. Shah, A.-S. K. Pathan, and A. Zengin, "Blockchain in vehicular ad hoc networks: Applications, challenges and solutions," *International Journal of Sensor Networks*, vol. 40, no. 2, pp. 94–130, 2022.

[38] M. A. Karabulut, A. F. M. Shahen Shah and H. Ilhan, "Performance Optimization by Using Artificial Neural Network Algorithms in VANETs," *2019 42nd International Conference on Telecommunications and Signal Processing (TSP)*, pp. 633-636, 2019, doi: 10.1109/TSP.2019.8768830.

[39] M. A. Al-Shareeda, T. Gaber, M. A. Alqarni, M. H. Alkinani, A. A. Almazroey and A. A. Almazroi, "Chebyshev Polynomial Based Emergency Conditions with Authentication Scheme for 5G-Assisted Vehicular Fog Computing," in *IEEE Transactions on Dependable and Secure Computing*, 2025, doi: 10.1109/TDSC.2025.3553868.

[40] M. A. Al-Shareeda, T. Gaber, M. A. Alqarni, M. H. Alkinani, A. A. Almazroey and A. A. Almazroi, "Chebyshev Polynomial Based Emergency Conditions with Authentication Scheme for 5G-Assisted Vehicular Fog Computing," in *IEEE Transactions on Dependable and Secure Computing*, 2025, doi: 10.1109/TDSC.2025.3553868.

[41] S. M. Hatim *et al.*, "Vanets and internet of things (iot): A discussion," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 12, no. 1, pp. 218–224, 2018, doi: 0.11591/ ijeecs.v12.i1.pp218-224.

[42] L. Wischhof and H. Rohling, "Congestion control in vehicular ad hoc networks," *IEEE International Conference on Vehicular Electronics and Safety*, pp. 58-63, 2005, doi: 10.1109/ICVES.2005.1563614.

[43] E. C. Eze, S.-J. Zhang, E.-J. Liu, and J. C. Eze, "Advances in vehicular ad-hoc networks (vanets): Challenges and road-map for future development," *International Journal of Automation and Computing*, vol. 13, pp. 1–18, 2016, doi: 10.1007/s11633-015-0913-y.

[44] B. A. Mohammed *et al.*, "Efficient Blockchain-Based Pseudonym Authentication Scheme Supporting Revocation for 5G-Assisted Vehicular Fog Computing," in *IEEE Access*, vol. 12, pp. 33089-33099, 2024, doi: 10.1109/ACCESS.2024.3372390.

[45] U. Mane and S. A. Kulkarni, "QoS realization for routing protocol on VANETs using combinatorial optimization," *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, pp. 1-5, 2013, doi: 10.1109/ICCCNT.2013.6726763.

[46] Z. G. Al-Mekhlafi *et al.*, "Lattice-Based Cryptography and Fog Computing Based Efficient Anonymous Authentication Scheme for 5G-Assisted Vehicular Communications," in *IEEE Access*, vol. 12, pp. 71232-71247, 2024, doi: 10.1109/ACCESS.2024.3402336.

[47] Shigang Chen and K. Nahrstedt, "Distributed quality-of-service routing in ad hoc networks," in *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, pp. 1488-1505, 1999, doi: 10.1109/49.780354.

[48] Chenxi Zhu and M. S. Corson, "QoS routing for mobile ad hoc networks," *Proceedings.Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 2, pp. 958-967, 2002, doi: 10.1109/INFCOM.2002.1019343.

[49] A. Dua, N. Kumar, and S. Bawa, "A systematic review on routing protocols for vehicular ad hoc networks," *Vehicular Communications*, vol. 1, no. 1, pp. 33–52, 2014, doi: 10.1016/j.vehcom.2014.01.001.

[50] S. Bitam, A. Mellouk and S. Zeadally, "Bio-Inspired Routing Algorithms Survey for Vehicular Ad Hoc Networks," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 843-867, 2015, doi: 10.1109/COMST.2014.2371828.

[51] S. Kaur, T. C. Aseri, and S. Rani, "Qos aware routing in vehicular ad hoc networks: A survey," *International Journal of Computer & Mathematical Sciences*, vol. 6, no. 4, pp. 1–6, 2017.

[52] M. Muhammad and G. A. Safdar, "Survey on existing authentication issues for cellular-assisted v2x communication," *Vehicular Communications*, vol. 12, pp. 50–65, 2018, doi: 10.1016/j.vehcom.2018.01.008.

[53] Z. Ghaleb Al-Mekhlafi *et al.*, "Coherent Taxonomy of Vehicular Ad Hoc Networks (VANETs) Enabled by Fog Computing: A Review," in *IEEE Sensors Journal*, vol. 24, no. 19, pp. 29575-29602, 2024, doi: 10.1109/JSEN.2024.3436612.

[54] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4g and 5g cellular networks: A survey of existing authentication and privacy-preserving schemes," *Journal of Network and Computer Applications*, vol. 101, pp. 55–82, 2018, doi: 10.1016/j.jnca.2017.10.017.

[55] D. Kombate and Wanglina, "The Internet of Vehicles Based on 5G Communications," *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 445-448, 2016, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.105.

[56] S. A. A. Shah, E. Ahmed, M. Imran and S. Zeadally, "5G for Vehicular Communications," in *IEEE Communications Magazine*, vol. 56, no. 1, pp. 111-117, 2018, doi: 10.1109/MCOM.2018.1700467.

[57] F. Jameel, Z. Hamid, F. Jabeen, S. Zeadally and M. A. Javed, "A Survey of Device-to-Device Communications: Research Issues and Challenges," in *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2133-2168, 2018, doi: 10.1109/COMST.2018.2828120.

[58] M. Gholibeigi, N. Sarrionandia, M. Karimzadeh, M. Baratchi, H. van den Berg and G. Heijenk, "Reliable vehicular broadcast using 5G device-to-device communication," *2017 10th IFIP Wireless and Mobile Networking Conference (WMNC)*, pp. 1-8, 2017, doi: 10.1109/WMNC.2017.8248846.

[59] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, *A comprehensive guide to 5G security*, 2018, doi: 10.1002/9781119293071.

[60] K. Katsaros and M. Dianati, "A conceptual 5g vehicular networking architecture," in *5G Mobile Communications*, pp. 595–623, 2017, doi: 10.1007/978-3-319-34208-5_22.

[61] C. Lai, R. Lu, D. Zheng and X. Shen, "Security and Privacy Challenges in 5G-Enabled Vehicular Networks," in *IEEE Network*, vol. 34, no. 2, pp. 37-45, 2020, doi: 10.1109/MNET.001.1900220.

[62] M. J. N. Mahi *et al.*, "A Review on VANET Research: Perspective of Recent Emerging Technologies," in *IEEE Access*, vol. 10, pp. 65760-65783, 2022, doi: 10.1109/ACCESS.2022.3183605.

[63] J. Qin, H. Zhu, Y. Zhu, L. Lu, G. Xue and M. Li, "POST: Exploiting Dynamic Sociality for Mobile Advertising in Vehicular Networks," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 6, pp. 1770-1782, 2016, doi: 10.1109/TPDS.2015.2467392.

[64] F. Lv *et al.*, "An Empirical Study on Urban IEEE 802.11p Vehicle-to-Vehicle Communication," *2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pp. 1-9, 2016, doi: 10.1109/SAHCN.2016.7732969.

[65] H. Zhou, W. Xu, J. Chen and W. Wang, "Evolutionary V2X Technologies Toward the Internet of Vehicles: Challenges and Opportunities," in *Proceedings of the IEEE*, vol. 108, no. 2, pp. 308-323, 2020, doi: 10.1109/JPROC.2019.2961937.

[66] W. Xu, H. A. Omar, W. Zhuang and X. S. Shen, "Delay Analysis of In-Vehicle Internet Access Via On-Road WiFi Access Points," in *IEEE Access*, vol. 5, pp. 2736-2746, 2017, doi: 10.1109/ACCESS.2017.2669178.

[67] N. Aung, W. Zhang, K. Sultan, S. Dhelim, and Y. Ai, "Dynamic traffic congestion pricing and electric vehicle charging management system for the internet of vehicles in smart cities," *Digital Communications and Networks*, vol. 7, no. 4, pp. 492–504, 2021, doi: 10.1016/j.dcan.2021.01.002.

[68] L. Lv, Y. Shi, and W. Shen, "Mobility-as-a-service research trends of 5g-based vehicle platooning," *Service Oriented Computing and Applications*, vol. 15, pp. 1–3, 2021, doi: 10.1007/s11761-020-00309-7.

[69] A. Balador, A. Bazzi, U. Hernandez-Jayo, I. de la Iglesia, and H. Ahmadvand, "A survey on vehicular communication for cooperative truck platooning application," *Vehicular Communications*, vol. 35, 2022, doi: 10.1016/j.vehcom.2022.100460s.

[70] K. Li, W. Ni, E. Tovar and M. Guizani, "LCD: Low Latency Command Dissemination for a Platoon of Vehicles," *2018 IEEE International Conference on Communications (ICC)*, pp. 1-6, 2018, doi: 10.1109/ICC.2018.8422933.

[71] T. H. Luan, R. Lu, X. Shen and F. Bai, "Social on the road: enabling secure and efficient social networking on highways," in *IEEE Wireless Communications*, vol. 22, no. 1, pp. 44-51, 2015, doi: 10.1109/MWC.2015.7054718.

[72] Z. Yang, K. Yang, L. Lei, K. Zheng and V. C. M. Leung, "Blockchain-Based Decentralized Trust Management in Vehicular Networks," in *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495-1505, 2019, doi: 10.1109/JIOT.2018.2836144.

[73] V. Kolesnikov, N. Matania, B. Pinkas, M. Rosulek, and N. Trieu, "Practical multi-party private set intersection from symmetric-key techniques," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1257–1272, 2017, doi: 10.1145/3133956.3134065.

[74] C. Lai, D. Zheng, Q. Zhao, and X. Jiang, "Segm: A secure group management framework in integrated vanet-cellular networks," *Vehicular Communications*, vol. 11, pp. 33–45, 2018, doi: 10.1016/j.vehcom.2018.01.004.

[75] H. J. Jo, I. S. Kim and D. H. Lee, "Reliable Cooperative Authentication for Vehicular Networks," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 4, pp. 1065-1079, 2018, doi: 10.1109/TITS.2017.2712772.

[76] E. Fujisaki, "Sub-linear size traceable ring signatures without random oracles," *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 95, no. 1, pp. 151–166, 2012.

[77] X. Duan, Y. Liu and X. Wang, "SDN Enabled 5G-VANET: Adaptive Vehicle Clustering and Beamformed Transmission for Aggregated Traffic," in *IEEE Communications Magazine*, vol. 55, no. 7, pp. 120-127, 2017, doi: 10.1109/MCOM.2017.1601160.

[78] R. Kachhoria, S. Jaiswal, R. S. Kharat, S. Pede, S. D. Kale, R. A. Mahajan, P. Sharma, and C. B. Khadse, "Adaptive sdn-based network architecture for vehicle to vehicle communication using flexible optical networks for 5g," *Optical and Quantum Electronics*, vol. 55, no. 1041, 2023, doi: 10.1007/s11082-023-05303-9.

[79] S. N. Saleh and C. Fathy, "A novel deep-learning model for remote driver monitoring in sdn-based internet of autonomous vehicles using 5g technologies," *Applied Sciences*, vol. 13, no. 2, 2023, doi: 10.3390/app13020875.

[80] S. M. Karim, A. Habbal, S. A. Chaudhry and A. Irshad, "BSDCE-IoV: Blockchain-Based Secure Data Collection and Exchange Scheme for IoV in 5G Environment," in *IEEE Access*, vol. 11, pp. 36158-36175, 2023, doi: 10.1109/ACCESS.2023.3265959.

[81] S. K. Dwivedi, R. Amin, S. Vollala and M. K. Khan, "B-HAS: Blockchain-Assisted Efficient Handover Authentication and Secure Communication Protocol in VANETs," in *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 6, pp. 3491-3504, 2023, doi: 10.1109/TNSE.2023.3264829.

[82] A. M. Farooqi, M. A. Alam, S. I. Hassan, and S. M. Idrees, "A fog computing model for vanet to reduce latency and delay using 5g network in smart city transportation," *Applied Sciences*, vol. 12, no. 4, 2022, doi: 10.3390/app12042083.

[83] L. Nkenyereye, C. H. Liu, and J. Song, "Towards secure and privacy preserving collision avoidance system in 5g fog based internet of vehicles," *Future Generation Computer Systems*, vol. 95, pp. 488–499, 2019, doi: 10.1016/j.future.2018.12.031.

[84] U. Maan and Y. Chaba, “Deep q-network based fog node offloading strategy for 5 g vehicular adhoc network,” *Ad Hoc Networks*, vol. 120, 2021, doi: 10.1016/j.adhoc.2021.102565.

[85] T. Perarasi, S. Vidhya, L. Moses M. and P. Ramya, “Malicious Vehicles Identifying and Trust Management Algorithm for Enhance the Security in 5G-VANET,” *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, pp. 269-275, 2020, doi: 10.1109/ICIRCA48905.2020.9183184.

[86] P. Das, S. Ray, D. Sadhukhan and M. C. Govil, “5G Enabled VANET Architecture Incorporating Security and Trust Management Mechanism,” *2022 IEEE 6th Conference on Information and Communication Technology (CICT)*, pp. 1-6, 2022, doi: 10.1109/CICT56698.2022.9997842.

[87] A. Gaurav, B. Gupta, F. J. G. Peñalvo, N. Nedjah, and K. Psannis, “Ddos attack detection in vehicular ad-hoc network (vanet) for 5g networks,” *Security and Privacy Preserving for IoT and 5G Networks: Techniques, Challenges, and New Directions*, pp. 263–278, 2022, doi: 10.1007/978-3-030-85428-7_11.

[88] S. Khan Tayyaba *et al*., “5G Vehicular Network Resource Management for Improving Radio Access Through Machine Learning,” in *IEEE Access*, vol. 8, pp. 6792-6800, 2020, doi: 10.1109/ACCESS.2020.2964697.

[89] A. Selvakumar, S. Ramesh, T. Manikandan, G. Michael, U. Arul, and R. Gnanajeyaraman, “Microgrid based vanet monitoring and energy management in 5g networks by reinforcement deep learning techniques,” *Computers and Electrical Engineering*, vol. 111, 2023, doi: 10.1016/j.compeleceng.2023.108933.

[90] V. K. Sharma, S. K. Mohapatra, S. Shitharth, S. Yonbawi, A. Yafoz, and S. Alahmari, “An optimization-based machine learning technique for smart home security using 5g,” *Computers and Electrical Engineering*, vol. 104, 2022, doi: 10.1016/j.compeleceng.2022.108434.

[91] A. Zhang, L. Wang, X. Ye and X. Lin, “Light-Weight and Robust Security-Aware D2D-Assist Data Transmission Protocol for Mobile-Health Systems,” in *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 3, pp. 662-675, 2017, doi: 10.1109/TIFS.2016.2631950.

[92] L. Buttyán, T. Holczer, A. Weimerskirch and W. Whyte, “SLOW: A Practical pseudonym changing scheme for location privacy in VANETs,” *2009 IEEE Vehicular Networking Conference (VNC)*, pp. 1-8, 2009, doi: 10.1109/VNC.2009.5416380.

[93] R. Hussain, Z. Rezaeifar, Y.-H. Lee, and H. Oh, “Secure and privacy-aware traffic information as a service in vanet-based clouds,” *Pervasive and Mobile Computing*, vol. 24, pp. 194–209, 2015, doi: 10.1016/j.pmcj.2015.07.007.

[94] J. Petit, F. Schaub, M. Feiri and F. Kargl, “Pseudonym Schemes in Vehicular Networks: A Survey,” in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 228-255, 2015, doi: 10.1109/COMST.2014.2345420.

[95] D. He, S. Zeadally, B. Xu and X. Huang, “An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks,” in *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681-2691, 2015, doi: 10.1109/TIFS.2015.2473820.

[96] X. Pan, X. Cai, K. Song, T. Baker, T. R. Gadekallu and X. Yuan, “Location Recommendation Based on Mobility Graph With Individual and Group Influences,” in *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 8, pp. 8409-8420, 2023, doi: 10.1109/TITS.2022.3149869.

[97] A. van Cleeff, W. Pieters and R. J. Wieringa, “Security Implications of Virtualization: A Literature Study,” *2009 International Conference on Computational Science and Engineering*, pp. 353-358, 2009, doi: 10.1109/CSE.2009.267.

[98] M. Hashem Eiza, Q. Ni and Q. Shi, “Secure and Privacy-Aware Cloud-Assisted Video Reporting Service in 5G-Enabled Vehicular Networks,” in *IEEE Transactions on Vehicular Technology*, vol. 65, no. 10, pp. 7868-7881, 2016, doi: 10.1109/TVT.2016.2541862.

[99] K. Mershad and H. Artail, “A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks,” in *IEEE Transactions on Vehicular Technology*, vol. 62, no. 2, pp. 536-551, 2013, doi: 10.1109/TVT.2012.2226613.

[100] X. Feng and L. Wang, “S2PD: A Selective Sharing Scheme for Privacy Data in Vehicular Social Networks,” in *IEEE Access*, vol. 6, pp. 55139-55148, 2018, doi: 10.1109/ACCESS.2018.2872789.

[101] K. Boakye-Boateng, E. Kuada, E. Antwi-Boasiako and E. Djaba, “Encryption Protocol for Resource-Constrained Devices in Fog-Based IoT Using One-Time Pads,” in *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3925-3933, 2019, doi: 10.1109/JIOT.2019.2893172.

[102] P. Andres-Maldonado, P. Ameigeiras, J. Prados-Garzon, J. J. Ramos-Munoz and J. M. Lopez-Soler, “Reduced M2M signaling communications in 3GPP LTE and future 5G cellular networks,” *2016 Wireless Days (WD)*, pp. 1-3, 2016, doi: 10.1109/WD.2016.7461499.

[103] R. Jin, X. Zhong and S. Zhou, “The Access Procedure Design for Low Latency in 5G Cellular Network,” *2016 IEEE Globecom Workshops (GC Wkshps)*, pp. 1-6, 2016, doi: 10.1109/GLOCOMW.2016.7849058.