Volume: 5, Issue: 6
Page: 148-162
2021

International Journal of
Science and Business
Journal homepage: ijsab.com/ijsb

IJSAB International

SDN Based 5G VANET: A Review

Shavan Askar, Glena Aziz Qadir, Tarik A. Rashid

Abstract

After 1G, 2G, 3G, and 4G technologies, 5G is a modern wireless system. 5G provides for the development of a modern form of network which connects virtually everyone and everything including computers, items, vehicles, and smartphones. VANETs marked as a critical infrastructure which can offer a wide range of facilities, including traffic control, accident prevention, and travel ease and comfort. VANETs are now being suggested as a primary enabler of the future fifth generation system, when combined with SDN. Using SDN-Based 5G VANETs Provide low latency, high bandwidth, Longer connectivity without failure, and support a greater number of users. In this paper we will describe how generations are developed and what are the differences between them. The main characteristics of using SDN based 5G VANET are discussed. Also, we describe four main attacks of SDN- VANET on security and security services that provided by SDN based 5G VANET. In addition, challenges and needs of SDN based 5G VANETS will be discussed. Then we will review some literatures then summarize their results. Finally, we will conclude the paper.

Keywords: *5G, SDN-VANET, performance, security, smartphone.*

IJSB
Literature review
Accepted 29 May 2021
Published 19 August 2021
DOI: 10.5281/zenodo.5221874

About Author (s)

Shavan Askar (Corresponding Author), Assistant Professor, CEO of Arcella Telecom, College of Engineering, Erbil Polytechnic University, Erbil, Iraq.
Email: shavan.askar@epu.edu.iq

Glena Aziz Qadir, Information System Engineering, Erbil Polytechnic University, Erbil, Iraq.
Email: glena.mei20@epu.edu.iq.

Tarik A. Rashid, Professor, Computer Science and Engineering, University of Kurdistan Hawler, Erbil, Iraq.

1. Introduction

5G is more powerful and unified than other generations. It has been enhanced to accommodate next-generation client interfaces, new implementation frameworks, and service delivery (Abraham, Guo, & Liu, 2006). VANETs (vehicular ad hoc networks) improve transportation safety (Englund, Chen, Vinel, & Lin, 2015). However, security issues developed from common ad hoc networks significant difficulties to their wider adoption (Sulaiman & Askar, 2015; Fares & Askar, 2016). In a traditional VANET framework, vehicles are connected with one another in an ad hoc manner via vehicle-to-vehicle connection, as well as vehicle-to-infrastructure connection with roadside units and cellular base stations (Qadir & Askar, 2021). Because of the advancement of 5G technologies and the importance of Software Defined Networking (SDN) in 5G, it was decided to improve VANETs by integrating them with 5G. 5G-SDN can provide VANETs with greater stability, scalability, and maintenance (Askar, 2017; Fizi & Askar, 2016; Askar, 2016; Luo et al., 2018). The new SDN controller relies on separating the control and data planes. The ONF has structured OpenFlow is the default SDN communication protocol as a wireless communications channel for guideline injection and message sharing between the controller and switch. The data plane, just from the other side, is the channel for routing packets among SDN Switches (Prados-Garzon et al., 2016). VANETs is mostly suggested to control vehicles to reduce road congestion as well as collisions. VANETs, on the other hand, are vulnerable to hacking that would interrupt networks or result in significant period, resources, and even life losses (Qadir et al., 2021; Tanuja, Sushma, Bharathi, & Arun, 2015). On VANETs, imitation and fake information assaults like sybil and fake information are now more popular (Iwendi et al., 2018). The SDN controller is the brain of the system. It is responsible for the overall management of the infrastructure resources efficiently (Keti & Askar, 2015; Qadir & Askar, 2021). Using SDN controller, the overall system performance is improved and optimized. It offers several advantages including efficient path selection, avoiding congestion control, and providing with fast and reliable communication. The data plane in SDN is only can route the packets. The forwarding devices includes switches, routers, access points (AP) and Road Side Unit (RSU). The connection between these devices is either wired connection or wireless connection. The SDN controller and the forwarding systems coordinate with each other occurs by OpenFlow protocol (Arif, Wang, et al., 2020). As a result, SDN-based 5G VANET support for real-time applications is available; Security alerts can have a low latency; Provide with high bandwidth for comfort messages like video streaming; Frequent automatic updates for applications like 3d maps and navigation; Longer connectivity without failure (Soua & Tohme, 2018). The key aim of this article is to introduce an SDN based 5G VANET characteristics, challenges and show recent works and suggested systems on them. The following is how the remainder of the article is laid out: in the next section we discuss background of 5G technology. Third Section, SDN enabled 5G VANETS. Fourth section, some papers are reviewed then summarized and discussed in section five. Finally, in section six we conclude and summarize the study.

2. Background of 5G networks

In Finland, the 2G service was established in 1991, enabling mobile devices to enter the digital area. Calling and message encoding, as well as SMS, image messaging, and MMS, is all possible with 2G. The top 2G speed was around 50kbps. In 1998, the first 3G system with more details, video calls, and smartphone internet was introduced. Before 4G arrived, what we now recognize a "slow" system was the height of connectivity in several major cities. 3G networks can provide 2 megabits per second to stationary or non-moving users and 384 megabits per second to devices in moving cars. 4G is a wireless communication protocol that was introduced in the late 2000s and is 500 times faster than 3G. It can handle high-definition cell TV, video conferencing (Askar et al., 2011; Al Majeed et al, 2014). It could be in the hundreds of megabits

per second. The top capacity of the 20MHz bandwidth market is 400Mbps (Dahlman, Parkvall, & Skold, 2013). Even so, because users share usable system capacity with others, users' measurable speed encounters are usually in the tens to hundreds of megabits per second, in 5G networks. The fifth generation of broadband technology is known as 5G, and it was created to improve the speed of telecommunications networks. 5G infrastructure may accommodate millions of network traffic per second, because it is 10 times faster than 4G, allowing you to download videos and media files in seconds. 5G is the backbone of IoT (Internet of Things) (Ahmed & Askar, 2021; Mohammed & Askar, 2021; Ali & Askar, 2021; Hamad & Askar, 2021). The fifth-generation infrastructure has several features that serve a wide range of individuals, including students, practitioners (doctors, architects, professors, governmental bodies, regulatory bodies, and so on), and the 5G network would benefit not only businessmen but also the general public. There will be many new techniques that will arise alongside the 5G network, making it more reliable and effective (Agiwal, Roy, Saxena, & Tutorials, 2016; Dai et al., 2015).

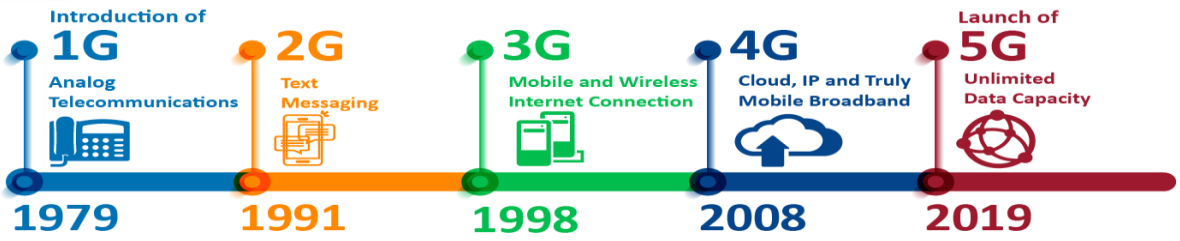

Figure1: Comparison between 3G,4G, and 5G

3. SDN Enabled 5G-VANET

3.1 SDN Enabled 5G-VANET Architecture

Many architectures have been suggested for better performance and security as described below:

Duan, Liu, and Wang suggested incorporating SDN into the 5G-VANET to provide a programmable interface for solving the problems. The suggested SDN allowed adaptive vehicle clustering and dual cluster head system greatly reduces the signaling overhead of a VANET while also improving communication performance. Cluster customers would have seamless access to the operators' facilities thanks to the planned cluster head collection. An adaptive trunk link transmission scheme and cooperative connectivity of mobile gateway members were suggested for the aggregated V2I (Vehicle to Infrastructure) traffic delivery in this interconnected network to better handle varying traffic over the trunk link and minimize latency through traffic delivery. The results of their simulations demonstrate that SDN coordinated vehicle clustering and beamformed transmission are capable of supporting fast-changing traffic environments with a wide dynamic range. The suggested scenario described in figure2 (Duan, Liu, & Wang, 2017). Also, by combining the ideas of SDN, C-RAN, and fog computing, Khan, Abolhasan, and Wei Ni presented a modern hierarchical 5G Next generation VANET framework. Furthermore, at the network's edge, a new Fog Computing architecture is designed (Husain & Askar, 2021; Samann et al, 2021). The fog computing framework's distributed support provides delay-sensitive, location-aware, and mobility-based real-time services that are suitable for future ITS scenarios. The suggested architecture, which uses SDN and C-RAN technology, offers stability, programmability, and efficient resource allocation using a control plane and centralized global information, resulting in substantial reductions in operator operating costs. Their test findings show increased throughput, decreased transmission latency, and decreased controller overhead. The scenario showed in figure 3 (Khan, 2018)

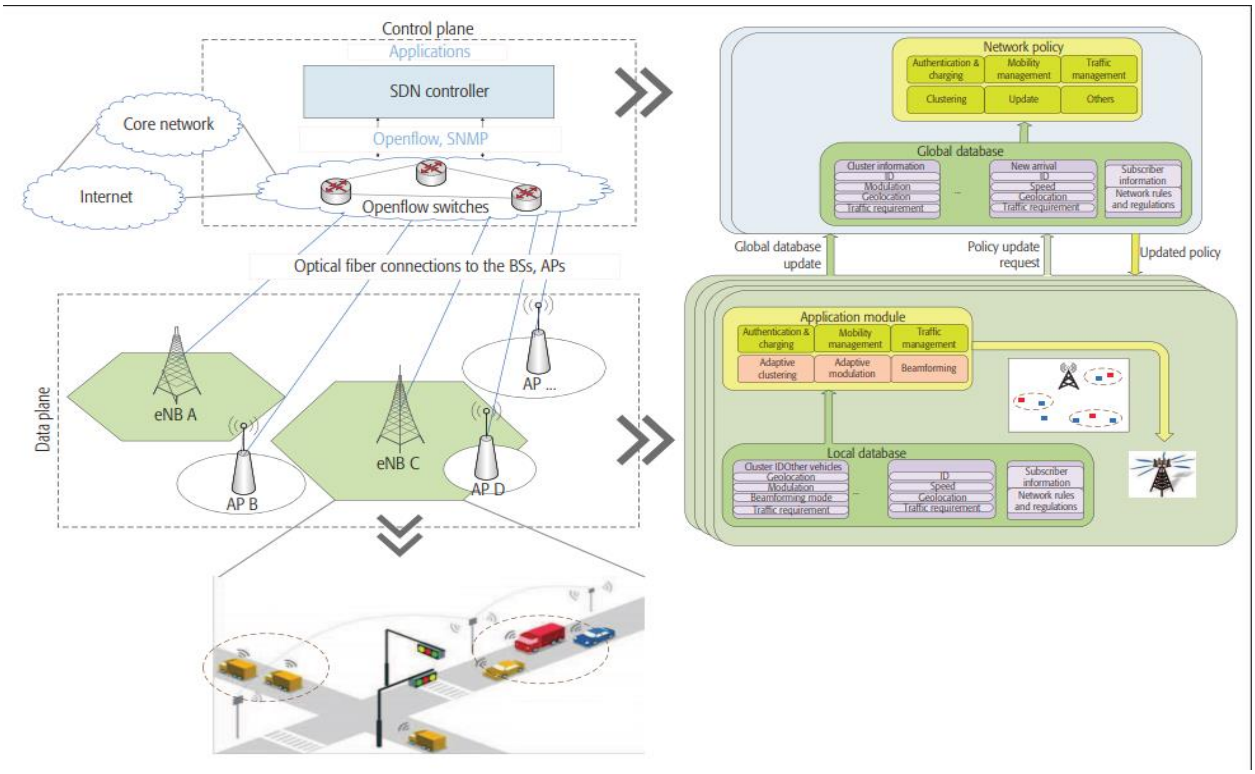

Figure2: SDN based 5G-VANET

.

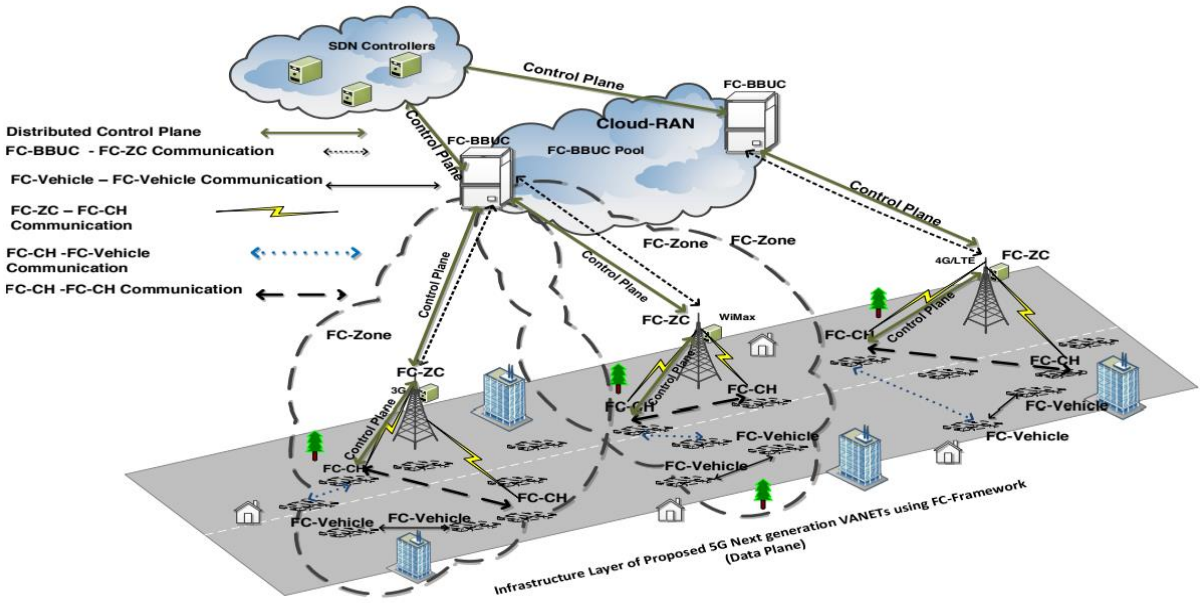

Figure3: SDN and Fog Computing (FC) System of 5G VANETs

Hussein and Chehab suggested a mechanism for integrating security services in a VANET system based on SDN incorporation in a 5G system without overloading the controller or creating data or control plane delays. They have demonstrated how this system can overcome the major security problems that standard VANETs have. A new defense plane was used to introduce an attack identification and avoidance system. To show the feasibility of the idea, a prototype of the above system and procedures was applied and evaluated in various scenarios (A. Hussein, I. Elhajj, A. Chehab, & A. Kayssi, 2017a).

3.2 Characteristic of SDN Based 5G VANETS

The fifth-generation wireless technology, that is known as 5G, is the most recent wireless communication system to be developed. It was created with the aim of achieving high data rates (up to 20 Gbps). Since the technology provides other new innovations such as vehicle-to-vehicle (V2V) communications and SDN, it guarantees a latency of 1 ms for real-time applications. 5G will produce better bandwidth, low latency, large device connectivity, higher data rate, and reliable Quality of Experience (QoE) provision with these technological advancements. Network optimization can be another major component of 5G infrastructure, in addition to improved bandwidth and lower latency (Ferrag et al., 2018).

Furthermore, 5G solves the issue of accommodating a huge number of nodes, which is a concern in VANET. Moreover, the processes and technologies of cellular networks are much too intertwined to be dealt with individually. As a result, it's critical to concentrate on a connectivity model that complements and incorporates existing technologies while still meeting a variety of application needs in a flexible, reliable, and heterogeneous manner. 5G is an interesting choice for diverse situations in this case. VANET is no exception, because it makes use of it. In VANETs or the so-called Internet of Vehicles, it can accommodate a wide number of simultaneous connection links (Shah, Ahmed, Imran, & Zeadally, 2018). From a security point of view, 5G has potentially flexible security advantages. SDN control and 5G based versatile security are two popular innovations that play a key role. As a result, 5G facilitates data protection through the user plane, allowing security parameters to be adjusted. Furthermore, by splitting the network control layer with the data routing layer, SDN allows for improved network management (Fang, Qian, & Hu, 2017). As a consequence, SDN offers complex and need-based protection by exploiting underlying system characteristics. To this end, 5G has a better possibility for the corporatization of VANET due to SDN's specific capability of managing a vast range of heterogeneous networks, diverse network environments, improved security, and network stability (Chen, Hu, Shi, & Zhao, 2016).

3.3 Security Attacks on SDN-5G VANET

Insiders and outsiders are the two broad types of attackers. Outsiders are groups who are not authenticated and may not have legitimate permissions, while insiders are harmless and authenticated VANET participants. Insider attackers, in general, face a greater challenge because they have legal access to the majority of network infrastructure. The nature of the attackers is also a critical factor to recognize in VANET. The assault may be motivated by a variety of factors, including financial gain, enjoyment, or other malicious purpose. Moreover, the reach and strategy of the attackers varies. The scale of the project can be local or international (Azam, Yadav, Priyadarshi, Padmanaban, & Bansal, 2021) Table 1 shows Security attacks. We will describe some of the security attacks in SDN- 5G VANET in this section:

1. DDoS: Attackers conduct a distributed denial-of-service (DDoS) attack by overwhelming the system with a vast amount of useless data. This form of attack may be carried out by the hackers alone or with collaboration of users. The primary goal of DDoS is to make the SDN-VANET inaccessible. Critical alarm signals will not enter the nodes in the event of an attack, potentially resulting in fatal effects for the benign nodes (Feinstein, Schnackenberg, Balupari, & Kindred, 2003; Thilak & Amuthan, 2018).
2. Replay attacks: In the SDN-VANET, data freshness is important. The hacker reuses the past data at a later point in time in active attacks. This attack has a similar impact to the spread of false facts (Sakiz & Sen, 2017).
3. Profilation: is a hack of SDN-VANET users' personal information in which a spatiotemporal data exchanged by benign SDN-VANET users is used for building a movement profiles against

the consumers. The attackers' goals are to violate clients' privacy, spy on them for commercial gain, and target them with relevant ads (Hussain, Kim, & Oh, 2009).
4. Tampering with hardware: different from all other threats, the attackers use hardware components to gain access to OBU or RSU. Tampering attacks are available in SDN-VANET by advanced attackers; however, tamper resistant device may be utilized to prevent these threats. Sensors and other vehicle systems, in addition to RSU and OBU, are vulnerable to these attacks (Vanitha & Padmavathi, 2017).

Table1: Security attacks in SDN-5G VANET

Type of attack	Aims of attack	Target of the attack
DDoS	Vehicle and service provider services are drained, service availability is impacted, VANET system QoS is disrupted, and money is lost.	V2V and V2I.
Replay attacks	Insert incorrect data, and steal the user's identification	V2P (Vehicle-to-Pedestrian), V2V, and V2I.
Profilation	Abuse users' privacy, spying on targeted users for financial purposes, and bombard users with relevant advertising.	V2V.
Tampering with hardware	Physical access to hardware, physical assaults, stealing cryptographic data, and malware injection	V2I.

3.4 SDN-5G VANET Security Services

In the SDN-VANET, security is a critical parameter (Trivedi, Tanwar, & Thakkar, 2018). 5G provides security services in two levels: via the architecture and via enabling technologies such as SDN. 5G provides authentication, anonymity, data privacy, and accessibility via its core infrastructure (Basin et al., 2018). User Equipment and 5G technology organizations like Mobility Management Entity (MME) as well as other telecom companies utilize authentication service. The key distinction between standard wireless networks (3G and 4G) and 5G is this (Fang et al., 2017). 5G also ensures data confidentiality and security. The target of 5G is on the lower networking levels, which are vulnerable to well-known threats and must be secure. 5G inherits the data integrity service from the upper layers and does not include it as a separate service. The 5G system, on the other side, protects data confidentiality information at the lower layers. Via Direct-Sequence Spread Spectrum (DSSS) and Frequency-Hopping Spread Spectrum (FHSS) , 5G mitigates attacks such as DoS and jamming at the lower transmission layers (Joshi, Renuka, & Medikonda, 2018). To meet the needs of the new generation an architecture is suggested that described below:

For a resilient VANET system security model, (A. Hussein, I. H. Elhajj, A. Chehab, & A. Kayssi, 2017b) suggested a three-way combination of VANETs, SDN, and 5G. They demonstrated how a strategy would protect VANETs from various forms of attacks, such as DDoS attacks that hit either the controllers or the cars in the system, as well as how to track down the attack's source. Their design was based on the idea that security research necessarily requires the use of a computing engine as well as additional tools. They added a third plane in SDN VANET systems in relation to the data and control planes, taking advantage of what SDN has to provide in the field of information networking. The Security Plane is responsible for establishing a connect between the vehicles and the Road Side Controllers (RSCs). Figure 4 illustrates the main components of the suggested framework.

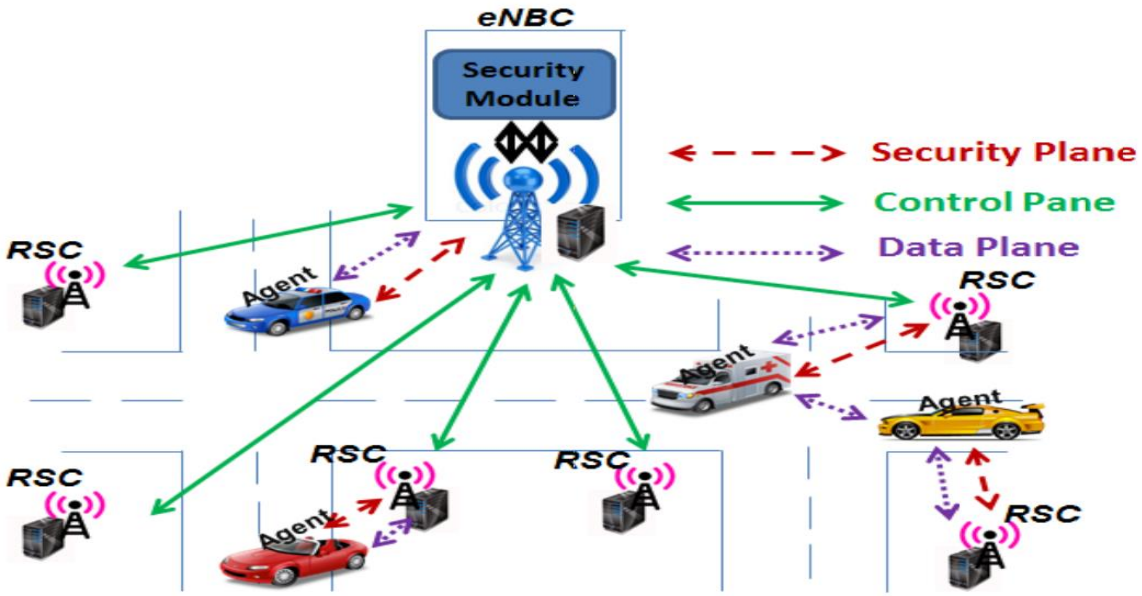

Figure 4: the proposed VANET Security Architecture based on SDN

3.5 Challenges and Needs of SDN Based 5G VANETS

VANETs enable the intelligent transport system which is efficient, safe and reliable. VANETs have emerged to make the drive safe and convenient. To provide with higher security, the critical events should be informed quickly and reliably. Efficiency can be improved by reduction of traffic jams. The connection of VANETs to the internet makes the journey more entertaining by providing files and social sites access (Qadir et al., 2021). VANETs messages are classified into two types: beacon messages and safety messages. Beacon messages are used to continuously update the vehicle position information regarding place, velocity and neighboring vehicles. Safety messages are the emergency messages in case of road accidents. They intend to avoid further accidents or traffic jam (Hasrouny, Samhat, Bassil, & Laouiti, 2017). VANETs send the message to neighboring vehicle, which is then forwarded to next. OBU are installed in the vehicle which are able to send messages to neighboring vehicles. VANETs information is stored in conventical clouds. Customers are able to purchase the cloud resources based on their budget. To connect with the cloud services while the vehicle is moving, RSU are used. They behave like gateway (Ku et al., 2014). in spite of using cloud services, VANETs are facing some fundamental challenges discussed below:

The high mobility of vehicles leads to the connectivity problem between control and management of network. The packet loss is also higher in case of higher vehicle mobility. The major requirement of future VANETs is the higher mobility and location awareness. The vehicles in the VANET communication must be traced properly. Due to emerging of lot of technologies, there will be different types of vehicles. It will be a challenge to have communication between these heterogenous vehicles. The user data and the location must be safe and secure. The user should be able to decide which data to be kept as private and which is not. Examination of the sensitive data should be done locally. It should not be shared over cloud. And future VANETs must be intelligent to perform wide number of heterogeneous information from vehicles (Yousefi, Mousavi, & Fathy, 2006).
Form the challenges listed above, we can summarize the requirements of 5G VANETs as; Provide low latency for safety messages; Support for real time applications; Provide with high bandwidth for comfort messages like video streaming; Frequent automatic updates for applications like 3d maps and navigation; Longer connectivity without failure. the integration of SDN in VANETs offers several benefits as listed below:

SDN can be used for optimal path selection. It can be extended to support for the status update of vehicle including position, speed etc. SDN controller provides the intelligence to the VANETs by centrally managing all vehicles in the network. And the SDN-VANET can be adapted for wireless environment including DSRC, WiFi, LTE, etc.(Offor, 2012).

4. Literature Review

In last few years different research works have been carried out in the field of SDN 5G VANETs. In this section we will describe the studies carried out in the area of VANETs, SDN and 5G technologies. Due to high mobility and frequent disconnection, the data recovery in VANETs is more complicated. Zhao and Cao in (2008) solves this issue by adopting the technique of carry and forward. In this technique the packet is carried out by the moving vehicle until it is able to forward it to the next moving vehicle in nearby area. this work the vehicle mobility is predicted using road layout. With minimal delay, the protocols send the packet to the nearest lane. In the mean of packet transmission ratio, latency, and overhead, the proposed models outperform others (Zhao & Cao, 2008). In addition, Hu and Grechnikov in (2010) suggested a one-dimensional VANET with a permitted region for communication. The research is still unable to determine how much of an impact the transmission range has on the system (Hu & Grechnikov). Raw and Lobiyal in (2012) suggested a throughput and delay evaluation of the next-hop forwarding process. For non-linear networks, the next-hop routing approach limits the routing range. However, due to the possibly more erratic distribution of vehicles, forced stability, and challenging scalability, position-based forwarding in city scenarios poses many difficulties (Raw & Lobiyal, 2012). Also, Sung, Shum et al. in (2012) examined the capacity of one-dimensional vehicular ad hoc networks. This research looked at a one-dimensional VANET that could be utilized to simulate a transportation scenario. The relationship between coding, latency, and throughput is shown by the performance evaluation. The analysis, on the other hand, assumes that vehicles arrive at the road through a Poisson method and that each one runs at a constant speed. As a result, constant speed does not adequately represent real-world highway scenarios (Sung, Shum, Yuen, & Communications, 2012). Sharma et al. in (2013) showed that using the SDN specification exactly as defined allows reaching Wide commercial networks have carrier-grade recovery times incredibly difficult. The authors suggested a security scheme based on a switch-based bidirectional forwarding detection (BFD) daemon (Sharma, Staessens, Colle, Pickavet, & Demeester, 2013). Jin and Papadimitratos in (2015) suggested an expansion of the standard V2V message authentication system. The intention was to add brief markers of previously validated messages into each message. While message authentication is an useful aspect in VANET security, it does not guarantee a safe atmosphere for all travelers (Jin & Papadimitratos, 2015). In addition Giotis, Androulidakis, and Maglaris in (2016), examined the VSPT authentication method, VANET authentication with Fingerprints, and TESLA prediction-based authentication to minimize processing time and overhead (Giotis, Androulidakis, Maglaris, & Networks, 2016). While Colazzo et al. (2016) presented the 5G Novel Radio Multiservice Adaptive Network Architecture, a modern architecture concept. They suggested a cloud-based architecture (Colazzo, Ferrari, & Lambiase, 2016).

VANETs offer the vehicle communication. But they suffer from connectivity issues, scalability and flexibility issue and intelligence. The communication between controller and devices occurs using openflow protocol. But *Thun and Saivichit* in (2017) have proposed the application of SDN in VANETs. The efficiency is increased with the increased capabilities of VANETs. Routing is performed using pox controller. Performance is evaluated using delay, throughput and pdr (Thun, Saivichit, & Engineering, 2017). For faster processing and reduced delay requirement fog computing has been incorporated. Hussein et al. in (2017) proposed the hybrid approach between fully centralized network and fully distributed network. Different

attacks considered here are DDOS attack with making the controller or vehicle as target and also finding the source of the attack (Hussein et al., 2017b). Moreover, Ge et al. in (2017) suggested the 5G-SDVN, a modern vehicular design that combines 5G networking technology. Fog cells are created at the edge of the system, which use multi-hop relay networks to minimize the number of handovers between the road side unit and the cars (Ge, Li, & Li, 2017). Traditional VANETS suffer from flexibility, scalability and connectivity issues. These needs can be fulfilled using cloud computing. But high mobility of vehicles, low latency requirement is not fulfilled by conventional cloud. Shrestha, Bajracharya, and Nam in (2018) discussed about the fog computing with VANETs. Also, integration of SDN in fog computing can improve the performance(Shrestha, Bajracharya, & Nam, 2018). Moreover, Nasrallah et al. in (2018) included a comprehensive survey and in-depth study of ULL network strategies as well as ongoing studies. They debated the relevance of low latency in future 5G networks. They clarified how they integrate into ULL's growth in two fields: backhaul communication and fronthaul communication (Nasrallah et al., 2018).

The combination of SDN in VANETs offers the key to enable the 5G technology in VANET. Ben Jaballah, Conti, and Lal in (2019) have focused on the advantages of integrating SDN with VANETs. Different sd-VANETs are compared based on their architecture, functions and challenges. The sd-VANET architectures are studied for security threats including availability, confidentiality, authentication, and data integrity. Different solutions suggested to solve these problems (Jaballah, Conti, & Lal, 2019). And Benalia, Bitam, and Mellouk in (2020) suggested a new generalized 5G-oriented IoV strategy called IoVs focused on 5G networks to increase data dissemination. such as 5G technology properties, SDN, and cloud fog computing. In contrast to conventional architectures, the proposed scheme assists in overcoming low latency, high reliability and security, high performance, and versatility challenges (Benalia, Bitam, & Mellouk, 2020). In 2020, Arif et al. suggested a paradigm for VANET management that combined 5G and Blockchain. The need to ensure safe and accurate information sharing between vehicles drove this decision. Low latency connectivity provided by 5G improves all V2V and V2I communications, enhancing their trustworthiness significantly. BlockChain, provides a public network that improves data storage and reliability (Abdulkahleq & Askar, 2021; Khalid & Askar, 2021). These inventions, when combined with the VANETs mechanism, will open plenty of new possibilities and applications, such as automating braking systems. They proposed a subject focused on the convergence of certain technology with the VANETs environment in order to achieve a more stable system and, as a result, safer traffic management (Arif, Balzano, et al., 2020). In addition, Adbeb, Di, and Ibrar proposed heuristic algorithms called Congestion-Free Path (CFP) and Optimize CFP (OCFP) in (2020). The suggested algorithms fix road congestion while still providing a feasible path for a car in a VANET (lower end-to-end delay). They utilized the NS-3 module to test the suggested architectures' performance as well as the SUMO module to generate a realistic VANET traffic scenario. The findings reveal that, as compared to existing methods, the implemented algorithms significantly reduce road traffic congestion (Adbeb, Di, Ibrar, & Applications, 2020). Bhavani and Valarmathi in (2020) provided a method for determining the best route for each area's source and destination. GPS, GIS, VANET, and Cloud Computing systems among others, are used to do this. Which would provide end users with the best routing scheme as well as information on traffic jams, collisions, and other issues along a certain path. This will undoubtedly assist end users in evaluating area traffic routes in real time. The percentage of accuracy has increased from 75 to 90 percent as compared to other methods (Bhavani, Valarmathi, & Computing, 2020). Maan and Chaba suggested a two-level method for detecting Primary Users in the network in their paper (2021). The received signal's power is measured, and the Primary Client is identified; this determination is then used as a threshold for the final Primary User

choosing. In comparison to state-of-the-art systems, the suggested proposal demonstrated higher performance. (Maan & Chaba, 2021). Then, in 2021, Aboud, Touati, and Hnich proposed a new handover (HO) optimization approach for the 5G mobile network. To determine when and where the handover will happen in the system, a mobility detection algorithm was combined with existing handover event logs. They intended to reduce the number of handover incidents while maintaining performance of the network in the presented design. To assess the feasibility of the suggested solutions, a simulation-based efficiency analysis was performed, and the findings were compared to the 3GPP traditional handover approach. Their suggested approach was found to decrease the number of HO incidents while maintaining system consistency (Aboud, Touati, & Hnich, 2021).

5. Discussion

VANETs are recognized as a critical technique capable of achieving a wide range of services, including traffic control, passenger safety, and travel convenience and comfort. VANETs are now being suggested as a primary enabler of 5G as part of the emerging 5G combined with SDN. In this article, various papers are reviewed and summarized based on the issues that they wanted to solve, the aim of the paper, and the results they have achieved. Table 2. Illustrates the summarization of the reviewed related works.

Table2: Summarization of the Reviewed Studies

Author(s)	Problem(s)	Objective(s)	Results summery
(Zhao & Cao, 2008)	Due to high mobility and frequent disconnection, the data recovery in VANETs is more complicated.	VADD protocols use vehicle-assisted data delivery to redirect the packet to the right path with the shortest data delivery delay.	The performance of the proposed VADD protocols is best terms of packet delivery ratio, delay and overhead.
(Hu & Grechnikov)	the transmission range of node affects the connectivity.	Connectivity in One-Dimensional VANETs	They discovered some generic formulas for calculating the probability that a one-dimensional VANET with a prevented zone contains exactly m clusters.
(Raw & Lobiyal, 2012)	routing performance.	For non-linear vehicular ad hoc networks, throughput and latency analysis of the Next-hop forwarding system.	For a fixed communication distance, network performance was optimized for the highest number of nodes.
(Sung et al., 2012)	highly dynamic topology.	Analysis of throughput in one-dimensional VANETs.	The relationship between coding, delay, and throughput is revealed by the performance analysis.
(Sharma et al., 2013)	fault tolerance of OpenFlow	If the SDN specification is used exactly as defined, large commercial networks can achieve carrier-grade recovery times.	A security scheme based on the switch's bidirectional forwarding detection (BFD) daemon is proposed.
(Jin & Papadimitratos, 2015)	Security of VANET systems.	Cooperative message authentication is used to scale VANET security.	While message authentication is an important technique in VANET security, it does not provide a safe environment for all passengers on its own.
(Giotis et al., 2016)	delay and processing overhead.	An OpenFlow middlebox is used to build a modular anomaly detection system for legacy frameworks.	a method of authentication It is proposed to use VSPT, VANET authentication with Signatures, and TESLA based on prediction.

(Colazzo et al., 2016)	high-latency communication in current wireless networks.	In upcoming cellular networks, reaching low-latency connectivity (5G).	It was announced that the 5G Novel Radio Multiservice Adaptive Network Architecture will be released.
(Thun et al., 2017)	VANETs offer the vehicle communication. But they suffer from connectivity issues, scalability and flexibility issue and intelligence	Performance Improvement of Vehicular Ad Hoc Network.	The quality of VANETs increases as their capabilities expand.
(Hussein et al., 2017b)	slow processing and delay.	To be the part of 5G technology, VANETs have been integrated with SDN	Network, accessibility, efficiency, and security features are all well-balanced.
(Ge et al., 2017)	Handover problems.	5G software defined vehicular networks.	the number of handovers between the RSU and the cars are minimized
(Shrestha et al., 2018)	flexibility, scalability and connectivity issues.	the fog computing with VANETs	integration of SDN in fog computing can improve the performance.
(Nasrallah et al., 2018)	the connection and network layer ULL mechanisms' efficiency and limitations.	ULL help in 5G networks, with backhaul, and network management being the key groups.	ULL systems provide a lot of coverage in 5G wireless systems.
(Jaballah et al., 2019)	security and privacy	enabling 5G technologies in a VANET based on SDN	Secure filtering in V2X messaging, secure mobile edge computing, convergence connectivity, and knowledge-centric networking are all subjects that have sparked discussion.
(Benalia et al., 2020)	high reliability, low latency, and security, high performance, and mobility.	A taxonomy of data distribution protocols.	It is proposed that a modern generalized 5G-oriented IoV architecture.
(Arif, Balzano, et al., 2020)	vehicular ad-hoc network management	guaranteeing secure and reliable information exchange between vehicles.	They suggested a new approach to achieve a very robust system, and hence a safer traffic control.
(Adbeb et al., 2020)	the traffic congestion issue	SDN based VANET Architecture (Mitigation of Traffic Congestion)	When compared to existing methods, the suggested architectures significantly reduce traffic congestion.
(Bhavani et al., 2020)	determining the most efficient route for each area's source and destination	Using GIS and the VANET system, smart city routing is possible.	the percentage of accuracy has been improved.
(Maan & Chaba, 2021)	Primary User identification in the system	In 5G VANET, a accurate cluster head selection technique for Software Defined Networks	As contrast to state-of-the-art systems, it has a greater degree of cluster head collection stability, and primary users are found with a zero percent chance of false detection.
(Aboud et al., 2021)	the support of efficient mobility management and handover problems.	reduce the number of handovers when maintaining network performance	The suggested approach decreases the number of handovers while maintaining network quality.

6. Conclusion

The term 5G refers to the next generation of telecommunications, which will eventually replace the existing 4G scheme. 4G was the successor to 3G, which was followed by 2G, and so forth. 5G is supposed to connect vehicles as well. As a result, we can use 5G technologies in VANET

networks that are based on SDN. Any new technology resulted in significant speed increases and a significant increase in network bandwidth. More of the same is promised by the latest SDN - 5G VANET system. It is anticipated that more users will be able to do more tasks at a quicker time. Vehicles connecting to 5G VANETS could have higher efficiency due to faster broadband speeds and greater network bandwidth. A summary of recent research studies on SDN-VANET based 5G, and suggested architectures, characteristics, security services, and challenges of SDN-5G VANETs are included in this article.

References

Abdulkhaleq, I. S., Askar, S. (2021). Evaluating the Impact of Network Latency on the Safety of Blockchain Transactions. International Journal of Science and Business, 5(3), 71-82.

Aboud, A., Touati, H., & Hnich, B. (2021). Handover Optimization for VANET in 5G Networks. Paper presented at the 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC).

Abraham, A., Guo, H., & Liu, H. (2006). Swarm intelligence: foundations, perspectives and applications. In Swarm intelligent systems (pp. 3-25): Springer.

Adbeb, T., Di, W., Ibrar, M., & Applications. (2020). Software-Defined Networking (SDN) based VANET Architecture: Mitigation of Traffic Congestion. International Journal of Advanced Computer Science, 11(3).

Agiwal, M., Roy, A., Saxena, N. J. I. C. S., & Tutorials. (2016). Next generation 5G wireless networks: A comprehensive survey. 18(3), 1617-1655.

Ahmed, K. D., Askar, S. (2021). Deep Learning Models for Cyber Security in IoT Networks: A Review. International Journal of Science and Business, 5(3), 61-70

Al Majeed, S., Askar, S., Fleury, M. (2014). H.265 Codec over 4G Networks for Telemedicine System Application. UKSim-AMSS 16th International Conference on Computer Modelling and Simulation (UK), Cambridge (pp. 292-297), doi: 10.1109/UKSim.2014.59.

Ali, K., Askar, S. (2021). Security Issues and Vulnerabilities of IoT Devices. International Journal of Science and Business, 5(3), 101-115.

Arif, M., Balzano, W., Fontanella, A., Stranieri, S., Wang, G., & Xing, X. (2020). Integration of 5G, VANETs and Blockchain Technology. Paper presented at the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom).

Arif, M., Wang, G., Geman, O., Balas, V. E., Tao, P., Brezulianu, A., & Chen, J. J. A. S. (2020). Sdn-based vanets, security attacks, applications, and challenges. 10(9), 3217.

Askar S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Evaluation of Classified Cloning Scheme with self-similar traffic. 3rd Computer Science and Electronic Engineering Conference (CEEC), Colchester, 2011, pp. 23-28, doi: 10.1109/CEEC.2011.5995819.

Askar, S. (2016). Adaptive Load Balancing Scheme For Data Center Networks Using Software Defined Network. Journal of University of Zakho, Vol. 4(A), No.2, Pp 275-286,

Askar, S. (2017). SDN-Based Load Balancing Scheme for Fat-Tree Data Center Networks. Al-Nahrain Journal for Engineering Sciences (NJES), Vol.20, No.5, pp.1047-1056

Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Service differentiation for video applications over OBS networks. 16th European Conference on Networks and Optical Communications, Newcastle-Upon-Tyne, pp. 200-203.

Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). A novel ingress node design for video streaming over optical burst switching networks. Optics Express, Vol. 19 (26), pp. 191-194

Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Adaptive Classified Cloning and Aggregation Technique for Delay and Loss sensitive Applications in OBS Networks. in Optical Fiber Communication Conference/National Fiber Optic Engineers Conference 2011, OSA Technical Digest (CD) (Optical Society of America, 2011), paper OThR4.

Azam, F., Yadav, S. K., Priyadarshi, N., Padmanaban, S., & Bansal, R. (2021). A Comprehensive Review of Authentication Schemes in Vehicular Ad-Hoc Network. IEEE Access, 9, 31309-31321.

Basin, D., Dreier, J., Hirschi, L., Radomirovic, S., Sasse, R., & Stettler, V. (2018). A formal analysis of 5G authentication. Paper presented at the Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security.

Benalia, E., Bitam, S., & Mellouk, A. (2020). Data dissemination for Internet of vehicle based on 5G communications: A survey. Transactions on Emerging Telecommunications Technologies, 31(5), e3881.

Bhavani, M. M., Valarmathi, A., & Computing, H. (2020). Smart city routing using GIS & VANET system. Journal of Ambient Intelligence, 1-7.

Chen, S., Hu, J., Shi, Y., & Zhao, L. (2016). LTE-V: A TD-LTE-based V2X solution for future vehicular network. IEEE Internet of Things journal, 3(6), 997-1005.

Colazzo, A., Ferrari, R., & Lambiase, R. (2016). Achieving low-latency communication in future wireless networks: the 5G NORMA approach. Paper presented at the Euro. Conf. Networks and Commun.

Dahlman, E., Parkvall, S., & Skold, J. (2013). 4G: LTE/LTE-advanced for mobile broadband: Academic press.

Dai, L., Wang, B., Yuan, Y., Han, S., Chih-Lin, I., & Wang, Z. J. I. C. M. (2015). Non-orthogonal multiple access for 5G: solutions, challenges, opportunities, and future research trends. 53(9), 74-81.

Duan, X., Liu, Y., & Wang, X. J. I. C. M. (2017). SDN enabled 5G-VANET: Adaptive vehicle clustering and beamformed transmission for aggregated traffic. 55(7), 120-127.

Englund, C., Chen, L., Vinel, A., & Lin, S. Y. (2015). Future applications of VANETs. In Vehicular ad hoc Networks (pp. 525-544): Springer.

Fang, D., Qian, Y., & Hu, R. Q. J. I. A. (2017). Security for 5G mobile wireless networks. 6, 4850-4874.

Fares, N., Askar, S. (2016). A Novel Semi-Symmetric Encryption Algorithm for Internet Applications. Journal of University of Duhok, Vol. 19, No. 1, pp. 1-9

Feinstein, L., Schnackenberg, D., Balupari, R., & Kindred, D. (2003). Statistical approaches to DDoS attack detection and response. Paper presented at the Proceedings DARPA information survivability conference and exposition.

Ferrag, M. A., Maglaras, L., Argyriou, A., Kosmanos, D., Janicke, H. J. J. o. N., & Applications, C. (2018). Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. 101, 55-82.

Fizi, F., & Askar, S. (2016). A novel load balancing algorithm for software defined network based datacenters, International Conference on Broadband Communications for Next Generation Networks and Multimedia Applications (CoBCom), Graz, 2016, pp. 1-6, doi: 10.1109/COBCOM.2016.7593506.

Ge, X., Li, Z., & Li, S. (2017). 5G software defined vehicular networks. J IEEE Communications Magazine, 55(7), 87-93.

Giotis, K., Androulidakis, G., Maglaris, V. J. S., & Networks, C. (2016). A scalable anomaly detection and mitigation architecture for legacy networks via an OpenFlow middlebox. 9(13), 1958-1970.

Hamad, Z., Askar, S. (2021). Machine Learning Powered IoT for Smart Applications. *International Journal of Science and Business, 5*(3), 92-100.

Hasrouny, H., Samhat, A. E., Bassil, C., & Laouiti, A. J. V. C. (2017). VANet security challenges and solutions: A survey. 7, 7-20.

Hu, X., & Grechnikov, E. On the Connectivity in One-Dimensional Ad Hoc Wireless Networks with a Forbidden Zone. University of Moscow.

Husain, B. H., Askar, S. (2021). Survey on Edge Computing Security. International Journal of Science and Business, 5(3), 52-60.

Hussain, R., Kim, S., & Oh, H. (2009). Towards privacy aware pseudonymless strategy for avoiding profile generation in vanet. Paper presented at the International Workshop on Information Security Applications.

Hussein, A., Elhajj, I. H., Chehab, A., & Kayssi, A. (2017b). SDN VANETs in 5G: An architecture for resilient security services. Paper presented at the 2017 Fourth International Conference on Software Defined Systems (SDS).

Hussein, A., Elhajj, I., Chehab, A., & Kayssi, A. (2017a). SDN VANETs in 5G: An architecture for resilient security services.

Iwendi, C., Uddin, M., Ansere, J. A., Nkurunziza, P., Anajemba, J. H., & Bashir, A. K. J. I. A. (2018). On detection of Sybil attack in large-scale VANETs using spider-monkey technique. 6, 47258-47267.

Jaballah, W. B., Conti, M., & Lal, C. J. a. p. a. (2019). A survey on software-defined VANETs: benefits, challenges, and future directions.

Jin, H., & Papadimitratos, P. (2015). Scaling VANET security through cooperative message verification. Paper presented at the 2015 IEEE Vehicular Networking Conference (VNC).

Joshi, J., Renuka, K., & Medikonda, P. (2018). Secured and Energy Efficient Data Transmission in SDN-VANETs. Paper presented at the 2018 22nd International Computer Science and Engineering Conference (ICSEC).

Keti, F., Askar, S. (2015). Emulation of Software Defined Networks Using Mininet in Different Simulation Environments. 6th International Conference on Intelligent Systems, Modelling and Simulation, Kuala Lumpur, 2015, pp. 205-210, doi: 10.1109/ISMS.2015.46.

Khalid, Z., Askar, S. (2021). Resistant Blockchain Cryptography to Quantum Computing Attacks. International Journal of Science and Business, 5(3), 116-125.

Khan, A. (2018). 5G Next generation VANETs using SDN and Fog Computing Framework.

Ku, I., Lu, Y., Gerla, M., Gomes, R. L., Ongaro, F., & Cerqueira, E. (2014). Towards software-defined VANET: Architecture and services. Paper presented at the 2014 13th annual Mediterranean ad hoc networking workshop (MED-HOC-NET).

Luo, G., Yuan, Q., Zhou, H., Cheng, N., Liu, Z., Yang, F., & Shen, X. S. J. C. C. (2018). Cooperative vehicular content distribution in edge computing assisted 5G-VANET. 15(7), 1-17.

Maan, U., & Chaba, Y. (2021). Accurate Cluster Head Selection Technique for Software Defined Network in 5G VANET. Wireless Personal Communications, 1-23.

Mohammed, C. M., Askar, S. (2021). Machine Learning for IoT HealthCare Applications: A Review. International Journal of Science and Business, 5(3), 42-51.

Nasrallah, A., Thyagaturu, A. S., Alharbi, Z., Wang, C., Shao, X., Reisslein, M., . . . Tutorials. (2018). Ultra-low latency (ULL) networks: The IEEE TSN and IETF DetNet standards and related 5G ULL research. 21(1), 88-145.

Offor, P. J. A. a. S. (2012). Vehicle ad hoc network (vanet): Safety benefits and security challenges.

Prados-Garzon, J., Adamuz-Hinojosa, O., Ameigeiras, P., Ramos-Munoz, J. J., Andres-Maldonado, P., & Lopez-Soler, J. M. (2016). Handover implementation in a 5G SDN-based mobile network architecture. Paper presented at the 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC).

Qadir, G. A., Askar, S. J. I. J. o. S., & Business. (2021). Software Defined Network Based VANET. 5(3), 83-91.

Raw, R. S., & Lobiyal, D. (2012). Throughput and Delay Analysis of Next-HOP Forwarding Method for Non-Linear Vehicular AD Hoc Networks. J International Journal on Ad Hoc Networking Systems, 2(2), 33-44.

Sakiz, F., & Sen, S. J. A. H. N. (2017). A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. 61, 33-50.

Samann, Fady E. F., Zeebaree, S. RM, Askar, S. IoT Provisioning QoS based on Cloud and Fog Computing, Journal of Applied Science and Technology Trends, Vol. 2, No. 1, pp. 29-40.

Shah, S. A. A., Ahmed, E., Imran, M., & Zeadally, S. J. I. C. M. (2018). 5G for vehicular communications. 56(1), 111-117.

Sharma, S., Staessens, D., Colle, D., Pickavet, M., & Demeester, P. J. C. C. (2013). OpenFlow: Meeting carrier-grade recovery requirements. 36(6), 656-665.

Shrestha, R., Bajracharya, R., & Nam, S. Y. (2018). Challenges of Future VANET and Cloud-Based Approaches. Wireless Communications and Mobile Computing, 2018, 1-15. doi:10.1155/2018/5603518

Soua, A., & Tohme, S. (2018). Multi-level SDN with vehicles as fog computing infrastructures: A new integrated architecture for 5G-VANETs. Paper presented at the 2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN).

Sulaiman, S., Askar, S. (2015). Invetigation of the Impact of DDoS Attack on Network Efficiency of the University of Zakho. Journal University of Zakho, Vol. 3(A) , No.2, Pp 275-280.

Sung, C. W., Shum, K. W., Yuen, W. H. J. I. J. o. S., Control, & Communications. (2012). Throughput analysis of one-dimensional vehicular ad hoc networks. 4(3), 150-163.

Tanuja, K., Sushma, T., Bharathi, M., & Arun, K. (2015). A survey on VANET technologies.

Thilak, K. D., & Amuthan, A. J. F. G. C. S. (2018). Cellular automata-based improved ant colony-based optimization algorithm for mitigating ddos attacks in vanets. 82, 304-314.

Thun, S., Saivichit, C. J. J. o. T., Electronic, & Engineering, C. (2017). Performance improvement of vehicular ad hoc network environment by cooperation between sdn/openflow controller and ieee 802.11 p. 9(2-6), 95-99.

Trivedi, H., Tanwar, S., & Thakkar, P. (2018). Software defined network-based vehicular adhoc networks for intelligent transportation system: Recent advances and future challenges. Paper presented at the International Conference on Futuristic Trends in Network and Communication Technologies.

Vanitha, N., & Padmavathi, G. (2017). A Study on Various Cyber-Attacks and their Classification in UAV Assisted Vehicular Ad-Hoc Networks. Paper presented at the International Conference on Computational Intelligence, Cyber Security, and Computational Models.

Yousefi, S., Mousavi, M. S., & Fathy, M. (2006). Vehicular ad hoc networks (VANETs): challenges and perspectives. Paper presented at the 2006 6th International Conference on ITS Telecommunications.

Zhao, J., & Cao, G. J. I. t. o. v. t. (2008). VADD: Vehicle-assisted data delivery in vehicular ad hoc networks. 57(3), 1910-1922.

Cite this article:

Shavan Askar, Glena Aziz Qadir, Tarik A. Rashid (2021). SDN Based 5G VANET: A Review. *International Journal of Science and Business, 5*(6), 148-162. doi: https://doi.org/10.5281/zenodo.5221874

Retrieved from http://ijsab.com/wp-content/uploads/752.pdf

Published by

IJSAB International