University of Windsor

WIRELESS COMMUNICATION SYSTEM

SURVEY PAPER ON
"INTEGRATION OF VANET WITH 5G"

Prepared By
NARAYANAN SRINIVASAN – 105192312
MANISHCHANDAR SUNDARAVEL – 110023774
Master of Electrical and Computer Engineering
University of Windsor

Submitted To
DR. ESAM ABDEL-RAHEEM
Ed Lumley Centre for Engineering Innovation (CEI)
University of Windsor
Ontario N9B 1K3

Integration of VANET with 5G-A Survey

ABSTRACT

Network-based safety is a new trend in the field of automobiles. In recent times many automobile manufacturers are facing the huge pressure of converting ordinary vehicles into intelligent ones. Currently, Vehicular Ad Hoc Networks (VANET's) are the preferred choice for designing Intelligent Transport System (ITS). With a day to day advancements in the field of wireless communication have triggered some interest in the development of VANET. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) are the two features supported by VANET which uses wireless technologies like IEEE 802.11p [1]. With the existing standards of VANET, it is difficult for the manufactures to exploit its full potential. For that purpose, researchers are opting for the 5G technology to be integrated with it. With this integration, there can be an improvement over faster handovers, security, and safety. This paper provides a brief overview of how 5G can be integrated with VANET and explains how it can be compatible with the existing VANET.

Keywords—Ad hoc networks, VANET, Intelligent Transportation System, 5G Network, Traffic Management

1. INTRODUCTION

Technology growth in the last decade has been tremendous, especially around mobile communication techniques. This technological advancement has transformed the way of thinking of several industries by providing anytime-anywhere communication [2]. This ease of transferring seamless information between devices has now become a new paradigm among industries. This idea slowly paved the way for the devices to become intelligent to match the needs. With the population increasing at a tremendous rate there should be more preferences should be given towards safety. In the process of globalization, many people are now starting to move towards cities. Due to the hectic lifestyle of cities, the distance between the workplace and home is ever increasing.

Subsequently, there has been a sudden increase in the number of vehicles on the road than usual causing further traffic congestion and accidents. The safety of human life has become more important on the road. To address these problems and to provide accident-free transportation many cities are now opting for the Intelligent Transportation system (ITS) framework [3]. Among many solutions for this problem, the concept of the Vehicular Ad Hoc Network proved to be extremely efficient and sustainable to avail the use of security applications.

VANET works on the principles of Mobile Ad Hoc Networks (MANET). VANET forms an ad hoc network of its own with different moving vehicles and when these vehicles encounter any connecting device over a wireless medium it exchanges critical information. In this ad-hoc network, every car is considered as a node, where one information is passed to a network is received by all other nodes in that network irrespective of the distance. One vehicle communicates with other vehicles using OBU (On-Board Units) forming mobile ad hoc networks where it shares information in a completely distributed manner [4]. These nodes process this raw information to a useful one and transmit to other nodes. The network formed is an open network where a node can join or leave at any time if they are reachable inside the network. Nowadays the vehicles are equipped with all essentials making it to join an existing network at ease without any modification.

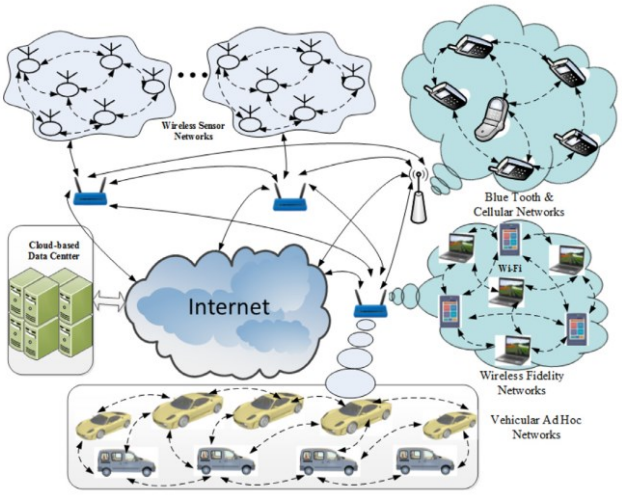

Fig 1: Heterogeneous Ad Hoc Networks [21]

Even though the VANET's are based on MANET, the routing protocols are entirely different as there is no centralized network in MANET's. Vehicular Ad hoc network (VANET) is now implemented in many vehicles because they offer several advantages such as passenger safety, comfort, enhanced traffic efficiency, and infotainment [5]. The basic exchange of information is achieved using Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure(V2I) communications. The adaptation of VANET commercially forms the basis of Intelligent Transportation System (ITS) as the VANET standards address most of the challenges faced by the wireless

vehicular network. Traditional VANET's have some technical backlogs due to flexibility, scalability, and poor connectivity.

However, next-generation VANET's will have high requirements to be satisfied requiring seamless and secure wireless solutions to be integrated with it. With the existing technologies, it will be difficult for the vehicles to withstand the upcoming years.

Now with the deployment of 5G wireless networks, users have access to ultra-high-speed (Gigabits per second), ultra-low latency with massive available bandwidth along with advanced security, reliability, and increased efficiency [6]. In this context of 5G networks, the scope for services and applications via VANET has increased tremendously. Eventually, the integration of VANET into wireless 5G networks will be imperative as it accelerates the development of secure advanced application based on VANET with new primary V2X applications such as Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P), Vehicle-to-Cloud (V2C), and more [7].

2. BACKGROUND

This part will provide a brief overview of VANET with their working methodology, application, and challenges. Moreover, this section also deals with the latest technologies whose integration with VANET's is discussed later i.e., 5G. Here only the essential details to understand 5G are only provided that are been surveyed and investigated in the later sections of this paper. The brief overview of 5G technology is out of the scope of this paper, as it is still being tested and has not launched commercially.

2.1 INTRODUCTION TO VANET

This section deals with a brief overview of VANET's architecture, its way of communication, the technology behind the wireless transmission, and VANET's application.

2.2 VANET ARCHITECTURE

VANET is a self-configuring network [8], which was evolved from the current technological advancement in network technology. There are three important parts in VANET's architecture they are On-Board Unit (OBU), Road-Side Unit (RSU), and the Application Unit (AU) OBU does the important job of interfacing with other OBU's and used for exchanging information between RSUs and OBUs. In simple it is the wireless communication device that provides routing and congestion control.

The second part i.e., RSU is a road deployed device that is fixed in dedicated locations does the job of providing internet connectivity to OBU's. The third part i.e., AU is an on-board device that does the job of communicating with networks using OBU on that vehicle.

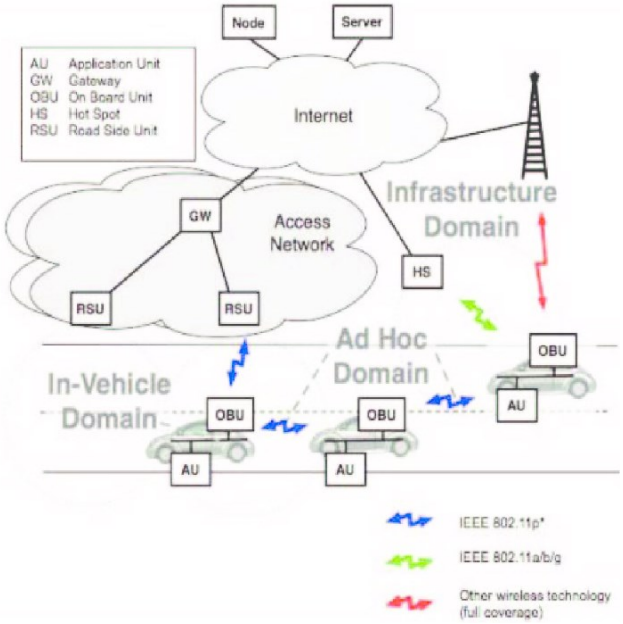

Fig 2: Architecture of VANET [20]

2.3 COMMUNICATIONS IN VANET

The communications in VANET can be classified into three types they are (i) Intra-Vehicle communication (ii) Vehicle-to-vehicle communication (V2V) (iii) Vehicle-to-Infrastructure communication (V2I). In Intra-Vehicle communication, the information is shared internally within that vehicle using available sensors and Electronic Control Units (ECU). In V2V communication, the information is exchanged with another vehicle using one-hop communication in case of direct connection and if they are not connected physically, they use routing protocols until it reaches other vehicles. With this feature, a vehicle can get services such as online gaming/infotainment.

In V2I communication, the vehicle communicates with RSU, which is deployed at the preferred location to enjoy the services such as multimedia/video streaming and location information. Apart from that Third Generation Partnership Project (3GPP) group defines a new way of communication which is Vehicle-to-X communications (V2X) that consist of V2I, V2V, and Vehicle-to-Pedestrians communications. V2X has many applications that

include remote vehicle diagnostics, vehicle traffic optimization, and in-Vehicle Internet [9].

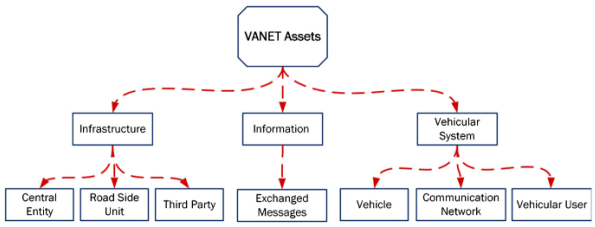

Fig 3: VANET Architecture Assets

2.4 WIRELESS TECHNOLOGY

Generally, vehicular applications are supported by wireless technology called DSRC which are mainly used for the short-range exchange of messages among the OBU's and RBU's. DSRC uses a technique called CSMA/CA contention-based Medium Access Control scheme (MAC) where they reserve a specific band which is standardized by European Telecommunication Standards Institute (ETSI).

The disadvantage with this method is that they only allow communication within a short-range area which cannot be expected for the vehicle all the time. The preferred method for wireless technology is cellular technology where it supports high network capacity and high bandwidth. The main advantage of this technology is that of DSRC is that it supports a wide cellular coverage area.

2.5 VANET APPLICATION

Some of the applications of VANET are:

(1) Safety Applications.
(2) Smart Parking.
(3) Infotainment.
(4) Lane changing applications.
(5) Intersection Collision Avoidance

3. EMERGING TECHNOLOGIES

This section describes some of the emerging technologies that are being integrated with VANET to upgrade its capabilities for the future.

3.1 5G Network

The demand for road safety is increasing at an exponential rate as the number of users starts to use their vehicles instead of common government vehicles. For the last decade, the 4G technology was in action, but this cannot be promised for upcoming generations where an essential upgrade is needed. There are some areas where 4G was lagging they are higher capacity, higher data rate, massive device connectivity, lower latency, reduced cost, and consistent QoS provisioning [10].

To address these demands, there is a need for new technology which forces us to choose the next upgraded level of cellular network which is 5G technology. 5G technology was designed in such a way that it addresses the above-mentioned problems. It includes (1) Massive Broadband (xMBB) that can deliver up to gigabytes of data when required, (2) Massive machine-type communication (mMTC) where it can connect up to millions of sensors and machines in a single network, and (3) Critical machine-type communication (uMTC) which can support immediate feedback with high reliability in cases like autonomous driving. Apart from these 5G infrastructure can provide tailored network solutions in areas like energy, agriculture, and automotive.

3.2 FEATURES OF 5G NETWORK

There are three important features of 5G enabled communications they are described in this section.

3.2.1 Proximity Service (ProSe):

The main purpose of the ProSe is to discover devices and services around them with location information. With ProSe, there is more chance of spontaneous interactions up to certain distances. This feature of 5G uses an hoc location discovery technique instead of the standard location discovery technique. Due to that, it has high data rate transmission without latency since they are traversing through the core and it also has high efficiency in resource utilization.

3.2.2 Mobile Edge Computing (MEC):

The most important requirement of 5G technology is to give low latency services. To achieve these low latencies, there is a need for moving some of the core functionalities to the edge i.e., Consumer. That is where MEC comes into play by providing a platform for the services to suitable network locations which is a mobile vehicle on roads. Apart from that mobile edge platform also supports services such as discovery, access, and advertisement of mobile edge computing services. Lastly, network integration offers uninterrupted access to MEC during commuting.

3.2.3 Network Slicing:

5G is expected to support about 1 million users in a small network. With this many users in a network, it

will be difficult for the network to keep track of each user and provide services. To address these problems 5G technology has a technique called network slicing where it does the job of managing the network. To manage a network, it uses a simple technique of separating the networks logically. By separating them as network slice, it allocates certain high priority services like safety. Another network slice can contain infotainment to satisfy QOS needs. Whatever services require special attention will be considered as network slice and treated specially.

4. INTELLIGENT TRANSPORTATION SYSTEM (ITS)

We discuss the topic of Intelligent Transportation System because the design of ITS is based on a reliable framework of Vehicular Ad-hoc Networks (VANET) [13]. In other words, the ITS is achieved through Vehicular Ad-hoc networks where vehicles communicate with each other and the infrastructure [14]. The future commercial adaptation of VANET's heavily dependent on the realization of ITS to achieve the goal of designing end-user, consumer-based applications, and services [14].

The rise of cities, expansion of suburbs, and the increase in population have given way to a huge increase in traffic both passenger and cargo. This increase in traffic will cause significant problems in terms of traffic, efficiency, safety, comfort, and reliability of travel if left without appropriate monitoring and control. The detection, recognition, tracking, and control of traffic systems are crucial in the modern-day as numerous traffic issues can be prevented, delays can be reduced, and violations can be identified [12].

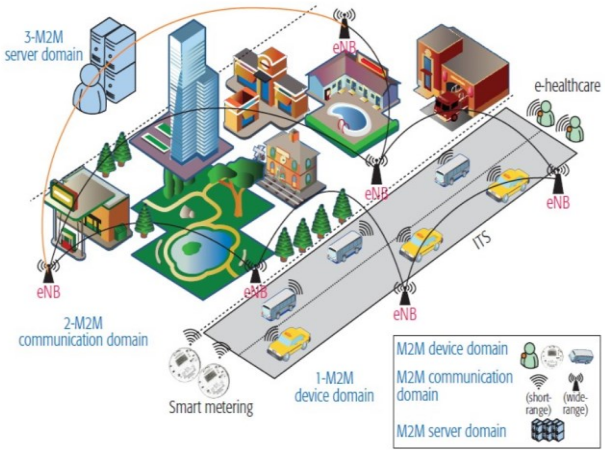

Fig 4: Massive Machine Type Communication in 5G

The concept of an Intelligent Transportation System is integration between advanced 5G communication technology categories such as Massive Machine Type Communication (mMTC) and Ultra-Reliable Machine Type Communication (URMTC). The integration of 5G technology into VANET offers greater flexibility to VANET by opening various new possibilities and use cases. Such flexibility in VANET supports the design of advanced systems such as intelligent transportation systems. ITS is used in the transportation, logistics, and traffic management systems to enhance the efficiency, connectivity, safety factor, and sustainability of the logistics.

In terms of operation, the ITS system depends upon various platforms such as VANET, sensors, control units, data, signal, and information processing systems. The dependence of ITS on various platforms has created the need to communicate faster, more securely, and effectively. Hence the 5G networks form a cornerstone in the design of ITS system where it plays a critical role in connecting the sensors, data processing, and their control units. Here, ITS is an extension of VANET where the system is data-driven instead of just a network of devices connected. The ITS operates based on the data obtained from the systems by processing it into functional information that can be used to implement new functions and services for the transportation systems [12].

As seen in the above background of VANET, these ITS systems offer several advantages to improve transportation by optimizing the existing resources available. Some of the fundamental components in ITS also known as ITS services are listed below:

- Advanced transportation management systems
- Advanced Traveler Information systems
- Advanced vehicle control systems
- Business vehicle management
- Advanced public transportation systems
- Advanced urban transportation systems

These multiple components of the ITS are fundamentally connected and operated via VANET. Furthermore, VANET forms the structural basis of the ITS system by supporting ITS Services on its ad-hoc networks.

Now, we have seen a brief introduction about the ITS and its fundamentals. We will analyze the different inter-vehicular and intra-vehicular communications using VANET connections after integrating the 5G network as the primary medium. Due to ultra-high reliability, low latency, and large data capacity, the 5G networks in VANET offers a platform for different applications. There are different

(V2X) applications that are developed based on these connections given below.

The use of such VANET to share information among vehicles, infrastructure, pedestrians, and cloud-enable number of applications for safety, comfort, vehicle design, infotainment, and much more [13]. These emerging vehicular networks are seen to be widely available in the future with the advent of 5G and advanced vehicle designs which place importance on safety, comfort, and efficiency [13]. The advancements in mobile communications, 5G networks, and current trends in the ad-hoc network have allowed for the deployment of several architectures for vehicular networks especially in urban, rural, and highway environments [17].

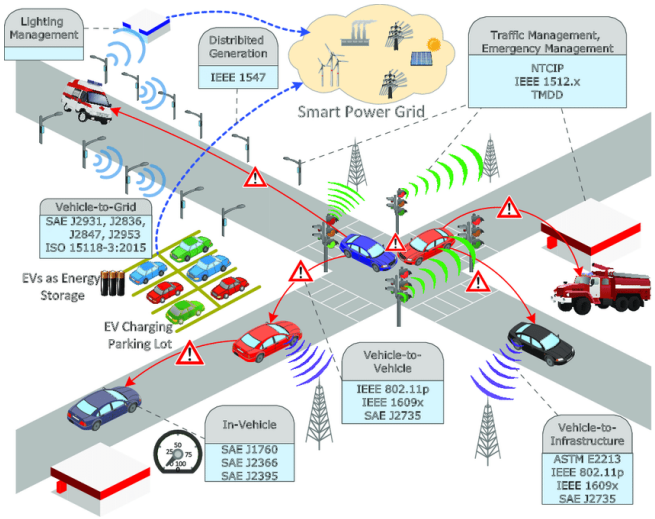

Fig 5: Intelligent Transportation System Architecture [19]

4.1 Vehicle-to-Vehicle (V2V)

The V2V ad-hoc network allows direct vehicular communication without depending on infrastructure support. These ad-hoc networks can be primarily used for directing alert messages, safety, security, and other applications [17].

In a V2V connection, each vehicle utilizes the VANET to multi-cast and communicate with other vehicles in the network. The data transmitted may hop several nodes to multiple recipients. The data transferred from V2V may be traffic-related, emergency data regarding an accident, or dynamic route planning [13]. These data are constantly transferred to the vehicle user without distracting the driver. Furthermore, there are two types of data transfer in V2V, they are unique and intelligent communication.

4.2 Vehicle-to-Infrastructure (V2I)

The V2I ad-hoc network allows the vehicle to communicate with the roadside infrastructures such as signal and traffic systems, light poles, etc., for transferring information and data gathering applications [17]. In this ad-hoc network, the Roadside Unit (RSU) sends messages to every adjacent vehicle. In this arrangement of communication, the data transfer rate is of high speed and offers a large data capacity connection between the vehicle and RSU. In practical applications, these RSU's can be set up to transfer data or information at high speeds where the data transferred is based on traffic conditions, information on speed breaking points, slow-down points, and speed limit transmissions.

4.3 Vehicle-to-Pedestrian (V2P)

The V2P ad-hoc network allows the vehicle to communicate with pedestrians on the road. The information transferred in this type of ad-hoc network is based upon the type of devices held by the pedestrian such as smartphones connected to 5G. The data transmission can include traffic information, assistance messages, safety data and offers scope for advert display of nearby businesses.

4.4 Vehicle-to-Cloud (V2C)

With the development of Cloud computing and edge computing technologies, the computational facilities that were previously in the cloud have come closer to the edge devices where they are processed. By leveraging the advantages offered by the cloud computing technologies the vehicular nodes can be designed in unique ways to interact with the cloud node, wireless access points, software-defined networks, and IoT gateways.

Furthermore, the connection between vehicle-to-cloud (V2C) will greatly enhance the processing power and revolutionize the way data is computed, stored, and transferred from the end devices to the cloud-based processing services. The integration of cloud to vehicle networks will increase the capabilities of the ITS by offering a platform for numerous use-cases, consumer applications, and improve the quality of services offered by the VANET system [18].

5. APPLICATIONS OF VANET WITH 5G INTEGRATION

The introduction of 5G telecom networks has offered numerous functionalities to consumers than ever before emerging as a preferred choice for the deployment of VANET and ITS services. With the deployment of 5G wireless networks, users have

access to ultra-high speed (Gigabits per second), ultra-low latency with massive available bandwidth along with advanced security, reliability, and increased efficiency [15]. In this context of 5G networks, the scope for services and applications via VANET has increased tremendously.

Eventually, the integration of VANET into wireless 5G networks will be imperative as it accelerates the development of secure advanced application based on VANET with new primary V2X applications such as Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P), Vehicle-to-Cloud (V2C), and more [16].

- Predictable mobility
- Lane change assistance
- Navigation
- Co-operative collision avoidance
- Large-scale network
- High computational ability
- Mobility applications
- Safety applications
- Road Traffic Management
- Pedestrian warning systems
- Speed Limit enforcement
- Interactive Entertainment
- Urban Sensing
- Message Dissemination
- Network Clustering
- Post-crash notifications
- Collision avoidance
- Road Hazard Control Notification
- Cooperative Collision Warning
- Geographic Forwarding
- Trajectory Forwarding
- Opportunistic Forwarding
- Mobile e-commerce
- Infotainment Systems
- City information systems
- Emergency Vehicle Signalling
- Dynamic Air Quality Monitoring
- Vehicle Accident Detection
- Heterogeneous Network Support
- Emergency Routing and Traffic Prioritization
- Intersection Collision Avoidance
- Smart grid Applications
- Platooning Vehicle Applications
- Road Condition Warning
- Virtualization of Wireless Network

6. CHALLENGES IN INTEGRATING 5G TO VANET

Even though the integration of 5G brings seamless, advanced, and more secure wireless network technology to the VANET. There are some challenges and risks associated with it in terms of security, connectivity loss, and a host of other issues that need to be addressed to make the VANET 5G integration more robust. Some of the challenges of VANET 5G integrations are [13]:

- Standardization of protocols in a highly heterogeneous vehicular network
- Creating Software-Defined hardware
- Interaction, cooperation, and inter-operability with other networks
- Data storage and management
- Accurate and Reliable Localization systems
- Data security and privacy
- Forgery (Vulnerabilities, Jamming)
- Vehicular cloud computing (Architecture, security, privacy, and authentication) [13].

7. SECURITY CHALLENGES IN VANET

In the perspective of the vehicular network, traffic, and safety the security of VANET plays a significant role [13]. Numerous threats intimidate the secured VANET integrated with 5G network, due to the rapid developments and increasing complexity of the vehicular networks [13]. The security challenges in Vehicular ad-hoc networks, ITS and 5G network platform are based on different layers which need to be addressed especially according to its type.

1. Security of Vehicular Networks
2. Data Privacy
3. Security of VANET Structure
4. 5G network Security

8. TYPES OF SECURITY ATTACKS EXPECTED IN VANET

The security attacks in VANET are classified into different types of attacks based on the type of security concern that is caused by the attack. Some security concerns are more complex than the others due to the scalability, high mobility, and a variety of other applications that follow the primary attack. The attacks on Vehicular ad-hoc networks are classified based on the attack on the availability of information, authentication and identification, confidentiality, integrity and data trust, and accountability of data [18].

8.1 Intra-Vehicle Attacks

These attacks are primarily carried out on Individual target or a set of vehicles based on the attacker's objective. The inter-vehicle attacks are focused on disruption of information channel, dissemination of indiscriminate information, injecting malicious code attack on the vehicle's CAN bus, accessing the vehicle to infect virus on vehicle applications [14].

8.2 Jamming Attacks

Jamming Attacks on the Vehicular ad-hoc networks will primarily affect the availability of the V2V platform to transfer data, disrupt the utilization of resources in the system, and affect multiple ITS applications based on the ad-hoc network. Commonly, the jamming attack is focused on the V2V, V2I, and V2P ad-hoc networks [14].

8.3 Distributed Denial of Service Attack (DDoS)

Denial of Service (DoS) attacks is a common way of disrupting the communication between the user and the service provider by overloading the communication channel with requests more than it can handle. DDoS attacks drain the resources on the vehicles and service providers, adversely affects the service availability, reduces the Quality of Service (QoS), and hijacks the ad-hoc network for malicious purposes. During the DDoS attack, the system cannot handle critical warning messages as the network and the nodes are overloaded with unnecessary malicious information thereby rendering the systems practically defunct.

8.4 Bogus Information Attack

The bogus information attacks are carried out to inject false information into the system which creates adverse effects on the applications using the data [14].

8.5 Sybil Attack

The Sybil attack on an ad-hoc network is based on the ability of the attacker to disrupt the existing network by creating an illusion through non-existent nodes, creating fake nodes, launching coordinated attacks via compromised nodes, and adversely affect other decision-based applications in the ITS system [14].

8.6 GPS Spoofing/ False Position Information

The GPS Spoofing is carried out by the attacker to maliciously control the user data by tampering with the GPS module by either compromising the hardware or by spoofing the GPS data. Spoofing the GPS or the navigation data can have several consequences to the vehicle. The systems and applications in the vehicle or ITS that depend on the GPS data are adversely affected due to this falsified data that is modified externally.

8.7 Replay Attack/ Impersonation Attack

The replay attacks are performed by an attacker impersonating the user data, injection of malicious information that can be dangerous to the safety steals user identity and can further coordinate the launch of Sybil attacks on the vehicle network also obtain cryptographic keys of the victim nodes [14].

8.8 Message Tempering

These attacks are carried out in V2I and in-car networks by having physical access to the hardware. During message tempering, the attacker can take control of the vehicle to launch physical attacks, steal cryptographic materials, and inject malware into the vehicle network causing irreversible permanent damage to the hardware [14].

8.9 Hardware Tampering

These attacks are unique as the attacker has direct access to the hardware of the vehicle or ITS infrastructure's hardware such as RSU, sensors, etc. The attacker tampers the hardware in the vehicle such as OBU's, nodes, and other hardware to modify the data transferred from these systems.

8.10 Malware Attack

Malware attacks are carried out normally after compromising the system integrity in the first place. The integrity of the primary layer of system security is destroyed and used as a staging platform for carrying out malware attacks. These malware attacks can be focused on destroying, disabling, or compromising the system's ability to operate normally. Depending on the type of malware attack the damage may be carried out by spreading malicious information, spamming the data nodes, disrupting, or rerouting communications, or launch other malicious codes focused on affecting specific applications [14].

8.11 Integrated Attacks

In addition to the above carried out attacks, the VANET on a 5G network is attacked in multiple ways or a combination of the above-mentioned attacks. Even though 5G networks are more secure than the existing standards some loopholes and vulnerabilities are yet to

be addressed. In integrated attacks, the IoT networks along with other vulnerabilities in cloud platforms, vehicle nodes, software-defined networks, API's, ad-hoc network infrastructures, and software bugs are leveraged by the attacker to deliver a devastating attack on the VANET or the ITS system as a whole.

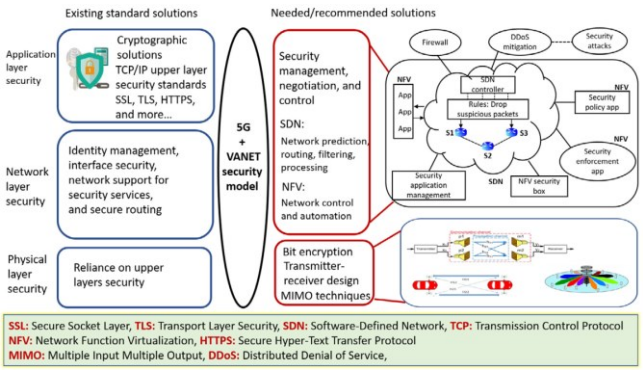

Fig 6: High Level security architecture of 5G enabled networks [14]

9. FUTURE SCOPE

Achieving the integration of 5G and VANET based applications/services is a massive task that is carried out by various stakeholders such as researchers, vehicle manufacturers, Original Equipment Manufacturers, telecom companies, and numerous governmental organizations.

However complicated of a task this may seem, the 5G VANET integration paves way for numerous applications that can address the needs of consumers and investors alike [14]. The future scope of the 5G integration into VANET is promising as it can leverage and utilize the ecosystem created by other systems such as transportation, cloud computing, and the Internet of Things (IoT). The realization of such systems will deliver critical as well as essential applications to the vehicle users in a way that has never been conceptualized before.

10. CONCLUSION

This paper gives a brief overview of the need for 5G and how 5G technology can cope up with vehicular communication in upcoming years. From the survey, it is understood that there were several areas where IEEE 802.11p lagging badly with current needs. The primary concern is the present vehicular communication standards are low latency, lack of spectrum, and highly reliable transmission of periodic communication. On the other hand, the 5G network can support low latency, high bandwidth, and higher capacity. Apart from that, 5G has some features like ProSe, MEC, and network slicing to handle autonomous vehicle attacks, reduce latency, and can give dedicated applications based on use case requirements.

However, 5G have competent issues with lower-level technologies like 4G LTE, 3G, 2G, Bluetooth, and ZIGBEE which makes it quite tough for the 5G to coexist with existing VANET. 5G also has data security issues since it has more vectors where it can be attacked. With these points in mind, it will be interesting to see how researchers are going to integrate 5G into vehicular communication. When these issues are taken care of then 5G can be a sustainable solution for vehicular communication in the coming days.

11. REFERENCES

[1] Ieeexplore.ieee.org. 2020. Vehicular Ad Hoc Networks (Vanets): Current State, Challenges, Potentials and Way Forward - IEEE Conference Publication. [online] Available at: <https://ieeexplore.ieee.org/document/6935482> [Accessed 23 November 2020].

[2] Hal.archives-ouvertes.fr. 2020. [online] Available at: <https://hal.archives-ouvertes.fr/hal-01496806/document> [Accessed 23 November 2020].

[3] Ieeexplore.ieee.org. 2020. A Survey on Vehicular Ad-Hoc Network [VANET's] Protocols for Improving Safety In Urban Cities - IEEE Conference Publication. [online] Available at: [Accessed 23 November 2020].

[4] Shrestha, R., Bajracharya, R., and Nam, S., 2020. Challenges of Future VANET And Cloud-Based Approaches.

[5] Ieeexplore.ieee.org. 2020. A Survey on Recent Advances in Vehicular Network Security, Trust, And Privacy - IEEE Journals & Magazine. [online] Available at: [Accessed 24 November 2020].

[6] ttps://www.qualcomm.com/invention/5g/what-is-5g. [Accessed 24 November 2020].

[7] Hussain, R. et al. "Integration of VANET and 5G Security: A review of design and implementation issues." Future Gener. Comput. Syst. 101 (2019): 843-864. [Accessed 24 November 2020].

[8] K. Liu, J. K. Y. Ng, V. C. S. Lee, S. H. Son, and I. Stojmenovic, "Cooperative data scheduling in hybrid vehicular ad hoc networks: Vanet as a software-defined network," IEEE/ACM Transactions on Networking, vol. 24, no. 3, pp. 1759–1773, 2016.

[9] 3gpp.org. 2020. 3GPP. [online] Available at: <https://www.3gpp.org/.> [Accessed 23 November 2020].

[10] Locard.eu. 2020. [online] Available at: <https://locard.eu/attachments/article/81/Security%20and%20Design%20Requirements%20for%20Software-Defined%20VANETs.pdf> [Accessed 23 November 2020].

[11] 2020. [online] Available at: <https://www.researchgate.net/publication/320933770_5G_for_Vehicular_Communications> [Accessed 23 November 2020].

[12] IEEE Transactions on Intelligent Transportation Systems, Vol. 12, No. 4, December 2011. [Accessed 24th November 2020].

[13] Felipe Cunha, Leandro Villas, Azzedine Boukerche, Guilherme Maia, Aline Viana, Raquel A.F. Mini, Antonio A.F. Loureiro. Data communication in VANETs: Survey, applications, and challenges, Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.02.017 [Accessed 23 November 2020].

[14] R. Hussain, F. Hussain and S. Zeadally / Future Generation Computer Systems 101 (2019) 843–864. "Integration of VANET and 5G Security: A review of design and implementation issues." [Accessed 11th November 2020].

[15] https://www.qualcomm.com/invention/5g/what-is-5g [Accessed 24th November 2020].

[16] M. Arif, Guojun Wang, Bhuiyan et al./Vehicular Communications 19 (2019) 100179. A Survey on Security Attacks in VANETs: Communication, Applications and Challenges. https://doi.org/10.1016/j.vehcom.2019.100179 [Accessed 24th November 2020].

[17] Asim Rasheed, Saira Gillani, Sana Ajmal and Amir Qayyum. "Vehicular Ad Hoc Network (VANET): A Survey, Challenges, and Applications". DOI 10.1007/978-981-10-3503-6_4. [Accessed 9th November 2020]

[18] Security and design requirements for Software-Defined VANETs. W. Ben Jaballah, M. Conti, and C. Lal / Computer Networks 169 (2020) 107099. [Accessed 24th November 2020].

[19] Turner, Stephen & Uludag, Suleyman. (2015). Towards Smart Cities: Interaction and Synergy of the Smart Grid and Intelligent Transportation Systems. [Accessed 26th November 2020].

[20] Singh, Satpal & Singh, Jaspreet. (2015). Vehicular Adhoc Network – A Review. Journal of Today's Ideas Tomorrow's Technologies. 3. 171-179. 10.15415/jotitt.2015.32012. [Accessed 26th November 2020].

[21] Tie Qiu, Ning Chen, Keqiu Li, Daji Qiao, Zhangjie Fu, Heterogeneous ad hoc networks: Architectures, advances and challenges, Ad Hoc Networks, Volume 55,2017, Pages 143-152,ISSN 1570-8705, https://doi.org/10.1016/j.adhoc.2016.11.00 [Accessed 26th November 2020].