Vehicle-to-Everything: Cybersecurity and Quality of Service Challenges

Valentina Timčenko
Institute Mihajlo Pupin
University of Belgrade
Belgrade, Serbia
valentina.timcenko@pupin.rs

Slavica Boštjančič Rakas
Institute Mihajlo Pupin
University of Belgrade
Belgrade, Serbia
slavica.bostjancic@pupin.rs

Abstract—**This paper is focused to the emerging technological development in the area of the advanced vehicular communication systems. It considers the most up to date Vehicular to Everything technologies and discusses typical scenarios related to the communication between vehicles, between vehicles and infrastructure, vehicles and pedestrians and communication between vehicles and network environment. Paper also considers arising issues and countermeasures related to the security, privacy and quality of service (QoS) aspects.**

Keywords – Vehicle-to-Everything, Quality of Service, Cybersecurity, Internet of Vehicles.

I. INTRODUCTION

Vehicle-to-anything (V2X) communication technology encompasses techniques for enabling safe and efficient operation of cooperative intelligent transportation system (ITS) applications. It enables real-time wireless communication between vehicles (V2V), vehicles and infrastructure (V2I), and vehicles and pedestrians (V2P), paving the way towards full driving automation and advanced driver-assisted systems. There are numerous already implemented V2X-enabled services, covering mostly the scenarios that rely on the need for efficient, real-time and secure traffic management (smart roads, smart cities). In this context, vehicles have to react to changes in the driving environment, by exploiting complete environmental awareness obtained through V2X communication, with low latency and high reliability. Thus, privacy and security are keys for V2X scenarios.

The continuous technological development towards, IoV (Internet of Vehicles), 5G and beyond to 6G, relies in the strong incorporation of the AI (Artificial Intelligence) and ML (Machine Learning) supported, self-learning intelligent network, which brings additional features, but also higher complexity of networks. In the context of the vehicular networks, and mostly the increasingly popular Unmanned Aerial Vehicles (UAV), the efficiency, fast response times and high level of security concerns are imposed as the essentials. The stronger security goal relies on the efficient and smart deployment of sophisticated surveillance, monitoring, data analysis, data storage, vehicle tracking and recognition systems, where the ultimate goal is to provide accurate, real-time attack prevention, predictive analytics and defense from attacks. For instance, to meet the expectations for IoV, the available V2X links should comply with very rigorous requirements, such as ultra-high reliability (≈99.999 %), ultra low end-to-end latency (< 5 ms), extremely high velocities (around 150 km/h), high network density (≈500 vehicles/km2 for highway and 1000 vehicles/km2 for suburban environments), a maximum packet loss of 10−5, (application layer), etc. Still, it requires the continuous support of a number of a V2X services, and accurate positioning (accuracy of at least 30 cm, and 10 cm for and vulnerable road vehicles). There is an increased need of collaborative use of different technologies, such as the cloud and edge computing, virtualization, AI/ML security-based systems, real-time data processing, etc. This approach can provide additional savings in the bandwidth, higher level of security and privacy protection, lower latencies in order to respond to the needs of delay-sensitive applications, thus allowing the use of certain IoV features such as real-time traffic analysis, vehicle identification, and various sophisticated security features.

In this paper, section II provides some basic information related to the Vehicle to Everything paradigm. Then in the section III we focus to the Internet of Vehicles characteristics. The section IV is related to the cybersecurity and most important issues related to the security and privacy. The section V explains the quality of service (QoS), considering the most important issues and countermeasures. Finally, we close the paper with the concluding remarks and tackle some ideas for future work.

II. VEHICLE TO EVERYTHING (V2X)

Vehicle to Everything (V2X) is an in-vehicle communication system that supports the transmission of information from the vehicle to other vehicles, road side units, pedestrians, power grid, etc, that can be affected by or that can affect the vehicle. It encompasses different specific types of communication, such as Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedistrian (V2P), Vehicle-to-Network (V2N), etc., in order to improve road safety, traffic efficiency, mass surveillance, and energy savings. American department of transportation estimates at least 13% of reduction in traffic accidents with implementation of such systems, which would result in 439,000 less accidents per year [1]. The communication technology used for V2X can be twofold, WLAN-based, and cellular-based. Vehicles can share

The work is funded by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia.

their position and speed with other vehicles and infrastructures, thus improving driver awareness of potential dangers along the road and avoiding possible collisions. It also enhances traffic efficiency with warnings about traffic congestions, propositions of alternative routes, a smarter transportation management, etc.

Besides increasing the safety, V2X also introduces other benefits. It provides vehicles with real-time information for the entire urban environment, including infrastructure, other vehicles, transportation management systems, navigation sources, etc. In other words, we can say that it will create a real-time map of the vehicle's immediate surroundings. This means that drivers will be informed about the position, speed and direction of movement of other nearby vehicles. They will receive information about traffic accidents or the proximity of emergency vehicles (ambulance, fire or police vehicles), frequency and proximity of vulnerable road users (cyclists or pedestrians) or road works, etc.

V2X technology also helps improve the efficiency of traffic management and reduce congestion. It informs drivers about upcoming traffic jams and offers them alternative routes. It enables communication between vehicles and traffic lights, road signs and other smart traffic systems. In addition, V2X communication ensures eco-friendly driving that leads to a reduction in fuel consumption and air pollution. As a result, there is a better control of congestion and traffic flows are normalized.

It can also improve parking management in smart cities, providing the information on free parking spaces, which makes easier to monitor parking lot occupancy for parking lot owners and operators. It also provides automatic vehicle identification and online payment for parking in order to reduce vehicle idling, reduces circulation time for a parking space, monitors air quality and congestion control, etc. The most popular locations for smart parking management are on-street parking, train stations, universities, airports and shopping malls.

A. Vehicle to Vehicle (V2V)

Vehicle-to-vehicle (V2V) represents an ad-hoc communication mode that consists of a wireless network in which vehicles send each other messages with information about their speed, location, driving direction, braking and loss of stability, thus allowing a driver to take early evasive actions, if necessary, to avoid potential accidents or ease traffic congestion. Possible alerts can be visual, tactile, and audible or their combination, allowing drivers to take appropriate action. This type of V2X communication technology helps save lives by increasing the performance of vehicle safety systems. A police report from 2019 estimates 6.8 million, resulting in 36,096 fatalities and 2.7 million people injured. Connected vehicles can provide for drivers necessary tools to anticipate potential crashes and reduce the number of lost lives [2].

Communication between vehicles is achieved through On-Board Units (OBUs), the most important part of the communication system in the vehicle, used for location determination, data exchange and voice communication. They represent electronic units with specific software for reading and storing data from the vehicle and for the control of data transmission.

V2V uses dedicated short-range communications (DSRC), a standard set by FCC (United States Federal Communications Commission) and ISO (International Organization for Standardization). DSRC is a technology based on the IEEE standard 802.11p and it allows wireless communication between vehicles in motion. DSCR enables fast communications at distances of up to 1000 meters, with the best performance achieved at distances of up to 300 meters [3]. It is based on line-of-sight communication and supports vehicle speeds of up to 160 km/h. Data transfer rates vary from 6 to 27 Mbps per RF channel, while latency is 50ms. DSCR communication or transfer of information is done completely anonymously, i.e. no information is used to identify the vehicle.

B. Vehicle to Infrastructure (V2I)

Vehicle-to-Infrastructure (V2I) represents a bi-directional wireless data (critical safety and operational data) communication between vehicles and roadway infrastructure, i.e., road side unites (RSUs), such as traffic lanes, signs and lights, to prevent or mitigate accidents and also to enable a wide range of other safety, mobility, and environmental benefits (Figure 1).

V2I communications encompasses all vehicle types and all roads, transforming infrastructure equipment into “smart infrastructure”. It allows vehicles to share and receive information with other devices on or near the road (cameras, streetlights, signage, lane markers, etc.) to improve roadway safety by delivering more information, earlier, and to the right vehicles [4].

In a secure network system, V2I technology connects vehicles, utilities, and pedestrians to provide for the information about the weather conditions, road conditions, traffic conditions, and warn drivers about collisions, jams, fast curves and speeds [4]. It relies on DSCR technology for communication just like the V2V.

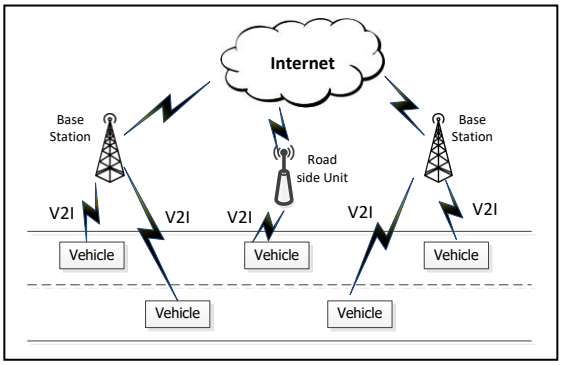

Figure 1. V2I communication

Identify applicable sponsor/s here. If no sponsors, delete this text box. (sponsors)

C. *Vehicle to Pedestrian (V2P)*

Road traffic participants, such as pedestrians, cyclists, and motorized two-wheeler operators are called Vulnerable Road Users (VRUs). There are numerous VRU fatalities every year with different rates of fatalities among different types of VRUs and different countries [5]. The V2P represents communication between vehicles and all types of VRUs, making them an active part of intelligent transportation system and improving the safety of VRUs, as well as vehicle-occupants [5]. VRUs differ in their characteristics, like speed, mobility, travel patterns and this information must developers of V2P systems have in mind when designing an effective V2P system.

V2P encompasses direct or indirect communication, as well as hybrid modes [5]. Direct mode of communication represents direct communication between vehicles and VRUs, with no intermediate entity. It is the fastest mode of communication and is best suited for safety applications due to lower latency in communication, but all entities in the communication require the same type of communication technology and the range of communication is limited. Also, devices for processing the received safety messages are needed which as a consequence require high computational power. Indirect mode of communication encompasses, besides vehicles and VRUs, an infrastructure, as an intermediate entity. Since messages are exchanged through the infrastructure, they have to be first processed in infrastructure nodes before being forwarded to other nodes. Therefore, these infrastructure nodes need to have high computation power. This type of communication can cause higher communication latency, imposing the requirement to assess latency constraints of the target V2P applications against the infrastructure latency [5].

D. *Vehicle to Network (V2N)*

V2N (Vehicle-to-Network) enables vehicles to communicate with the Internet using cellular networks. Vehicles communicate with each other and other objects (street lights, traffic signals, pedestrians etc.) via Internet. It can also enable advanced navigation based on maps. Evolution of cellular technology and the introduction of 5G, these types of networks can become a reality.

The main benefits of V2N are (1) Easy and cost-effective implementation, based on 5G, as the large part of the required physical infrastructure is already available. The technology used for Internet connections for smartphones and Internet of Things can be used for vehicles as well. Other benefit corresponds to the (2) Smooth traffic flow. This aspect relies on the use of the Cooperative Intelligent Transportation Systems (C-ITS), which allow real-time sharing of data, providing safer road traveling. In circumstances of all connected vehicular network, the simple use of the 5G mobile network will provide many advantages for easier C-ITS operation, as the information related to traffic conditions could be acquired in timely and more reliable manner. (3) Better route planning. V2N aids the autonomous vehicles to plan and optimize the routes well ahead, considering the real-time traffic information and predicted future traffic based on the planned routes of other vehicles. (4) Economies of Scale, as the V2N concept enables the use of cloud-computing concept for monitoring the collection of vehicle and traffic data. This concept is especially useful for large collections of data managing wide and heterogeneous road infrastructures. Additionally, the aforementioned techniques are enhanced with Big Data concept combined with sophisticated intelligent ML/AI operation predictive models, which can be used for further optimization, adjustment of the traffic lights length, considering the historical/experience data, but also the information of the time-of-day specific speed limits, and/or the weather conditions. (5) Faster speeds are provided base on the integration of the 5G technologies, which is crucial for providing safety in autonomous driving.

The main difference between V2N and V2I is that V2N provides services to different geographical areas, while V2I encompasses communication of vehicles in the geographical area of related RSUs [6].

III. INTERNET OF VEHICLES

Internet of Vehicles (IoV) represents a subset of a well-known Internet of Things (IoT), and it has developed from the conventional vehicle ad-hoc network (VANET). It encompasses various types of sensors that acquire data from other vehicles and road infrastructures, representing a complex vehicular network connected to the Internet **[7]**. Figure 2 present a communication architecture of the IoV.

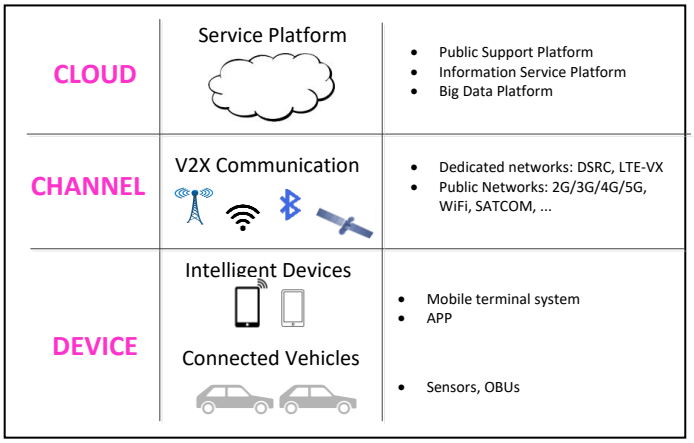

Figure 2. IoV communication architecture

The main characteristics of IoV are complex communication, dynamic topology, high scalability, localiyed communication and energy and processing capacity.

Communication in IoV is **complex** since it encompasses various types of sensors installed in the vehicles (radar, GPS, cameras, brake, temperature sensors, etc.) and uses beacon and safety messages for communication with other vehicles and network devices, while density and speed of vehicles are constantly changing (on the highway, there is fewer vehicles that move at a very high speed, while in urban area, vehicles move at lower speed but the number of vehicles is larger, which possibly causing the interferences). The topology of the IoV network is **very dynamic**, since it easily changes due to vehicles that can move at a very high speed and change their

directions often. IoV is **highly scalable**, since it can handle constantly growing number of vehicle and extend the network in large-scale environment. The communication is **localized**, since the vehicles exchange messages with neighboring vehicles within their geographical coverage. Unlike the IoT devices, vehicles in IoV have an unlimited energy due to huge battery power, high processing capacity and memory space for complex computation; therefore, have necessary **energy and processing capacity**.

IV. CYBERSECURITY ISSUES

As in every other networking environment, the wireless communications, and even more the vehicular communications seek for special countermeasures against different types of the security and privacy concerns. In that sense, there is a strong need to keep in line with CIA, the three basic security properties: confidentiality, integrity, and availability [8]. The 3GPP has identified a number of basic safety and non-safety V2X use-cases, where the release 15 [9] targets the 5G-NR (New Radio) access technology in support for advanced applications that will provide semi-automated and fully automated V2X functionalities [10].

The intensified development in the area of the VANET (Vehicular Ad hoc NETworks), and especially for the needs of providing reliable, efficient, accurate and safe autonomous vehicle (AV) and unmanned aerial vehicles (UAV) systems, gave credits to the need of developing a set of proper cybersecurity measures and attack defense systems.

In general, the attacks can be classified as either passive (eavesdroppers, mostly targeting the individual vehicles privacy) or active (intruders are actively interacting with the system), but besides their inherent nature, they can be categorized by a number of different characteristics.

The major concerns are the critical, sensitive and usually private data of the vehicles, such as the private key, certificates, or signatures which are later misused for denial-of-service (DoS), modification of transmitted data, or false data injection. That involves the presence of the eavesdroppers, and mostly corresponds to the attack on confidentiality.

In most of the V2X attack cases, the intruders are well authenticated network nodes or users, which have a permission to communicate with other users. These illegitimate users seek for necessary credentials and access in formation in order to preserve their position as the system-level access users. Due to these privileges, these nodes do follow the protocol rules, but intentionally generate and send tampered information to the target user(s).

V2X technologies allow efficient vehicles interaction and communication with other vehicles (V2V), with underlying infrastructure (V2I), with other traffic users - pedestrians (V2P), and with other networks (V2N) [11]. Inherently very complex, these communication environments are attractive field for a range of cyberattacks and safety concerns, leading sometimes to severe consequences.

Additionally, in the case of the UAV vehicles communication, the security issues mostly come with that independence from the terrain, as having the high altitude of the UAV operation, there are more security gaps and potential vulnerabilities to take care of. In that case, the V2X technologies provide communication from the edge data points, to a range of different parts of the system and RSUs, for which there is a need for multiple communication channels. Clearly, with the raise of the number of different simultaneously used communication channels, the security is reciprocally jeopardized and exposed to cyberattacks.

One of the most common V2X-communication–related attacks is the VANET, and analysis of the security issues in wireless communication from outside the vehicular system. In VANETs, with frequent leaving communication of a certain node or joining the communication by another vehicle, there is an issue of dynamical change of the network structure. For preserving the safe and uninterrupted communication, VANETs need a special set of security measures to beat their inherent vulnerability on the intentionally performed attacks resulting in damaging of network. The most common VANET V2X attacks correspond to the man-in-the-middle attacks, fake data injection attacks, location tracking, denial of service, and different forms of the replay attacks [7].

Novel tendencies in V2X field are focused to the challenging deployment issues of the new radio (NR) 5G and beyond techniques. 5G technologies provide higher transmission speeds and throughputs, multi-tenant processing, along with a high-content data communications, mobile services, along with proper Ml and AI integration, need high rang quality monitoring and security provisioning [12].

V2X systems are sensitive to a range of cyberattacks, whereas the main intruders correspond to the DoS/DDoS attack variants, injection of false data and the Sybil attacks [11]. There is also a security concern related to the non-Repudiation attack category [10].

Denial of service and distributed denial of service attacks (DoS/DDoS) can be related to different layers of communication, where the attacker(s) are sending an extremely large number of service requests in order to exhaust the server and deny the service to the legitimate users. The same activity can easily disrupt the RSUs network and established communication between RSUS and vehicles. DDoS attacks are even more severe, as in that case the attack is performed from a number of usually synchronized attackers that are targeting the victim from a number of locations, making them harder to detect. The jamming attack is one of the most specific DoS attacks (attacks against availability). It is related to the physical network layer, usually relies on the interference and has an effect of banning the users their physical access to the communication channel by limiting or denying the transmission of the incoming messages. The jamming attack on the physical level (IEEE 802.11p) or the bands close to 5.9 GHz, does not depend on the exchanged messages semantic, but is restricted only by the geographical range covered by the attackers. These attacks are not the most common for V2X but when happen their effect is mostly demonstrated through the latency increase and network reliability decrease.

At the other hand, from the network layer perspective, when considering the routing-based DoS provoked protocol

issues, the dominant security violations correspond to dropping the packets, exploiting the congestion control protocols vulnerabilities and intentionally created delays. Dropping packets can disable the possibility of propagating the warning messages related to some vehicle incident, where other vehicle would not be prevented from doing the same mistake or having the same catastrophic result. Due to high mobility characteristics of the V2X, the monitoring of this kind of the attacks would not be enough for real-time scenario. The DoS flooding attacks can be dangerous as these are directed towards the network resources unavailability for the legitimate usage. One specific characteristic of these attacks is their multi-hop communication nature.

One of the most troublesome attacks in wireless vehicular communication is the **Sybil Attack**, by which an attacker vehicle appears to have several different identities, relying on the successive or simultaneous use of different IDs. It is an attack on authenticity, and can be an initiator of the DoS attacks as well, where it will help the misuse of the network bandwidth, network operation destabilization and network reliability decrease.

In some cases, these attackers will continuously change their identities, making an impression to be a different moving vehicle producing the false road congestions, thus misleading the information system for the best routes, the existence of the obstacles, resulting in a poor decision-making operations and communication with the neighboring vehicles/RSUs. Another threat could be seen from the use of the so-called pseudo-identities that can boost the trust score, or the specific reputation factor of the malicious nodes, while reducing the scores related to the legitimate vehicles. That way, a larger number of vehicles are declared to trust the information delivered by the malicious node, versus the number declared for some of the legitimate vehicles.

Another type of the wireless vehicle communication attacks corresponds to the **injection of the false data**. It can appear as a part of other mentioned attacks, but basically relies on the generation and broadcast of the false safety or traffic information. The usual intention is to intentionally generate the collision or to interrupt the road traffic. They can be easily combined with Sybils while injecting false information at multiple locations in the network.

Having in mind that the false information can significantly contribute to the decrease of the message delivery efficiency, it is understandable the fear from the GPS spoofing cases where the false GPS coordinates can lead to the vehicle acceptance of the fake, but sometimes much stronger that the original ones, signals. In the case of the so-called replay attack, the attacker will confuse the other users by the event information which was once stored and then released when no longer valid. This way, with the retransmission of the messages the attacker is exploring the network conditions at the moment when the original messages are sent. One potential countermeasure for this attack is to use timestamps for every message, digital signatures or message sequence numbers. In V2X the replay messages are dealt also by an adequate replay protection mechanism which defines the maximum transmission delay for the single-hop messages. These values are used to be compared and evaluated by the receivers, which will have a permission to considered as not plausible every message that arrives with an out-of-date timestamp. These attacks are mostly dangerous in the case of the multi-hop communication, where the most endangered characteristic is the throughput. Eligible countermeasure would assume the use of more robust and stronger infrastructures, e.g., RSUs and base stations for C-V2X, where these can have a beneficial impact to the routing misbehavior. 4) Non-repudiation attacks relate to the need to ensure that once a vehicle broadcasts certain message, it cannot deny that if some unexpected, malicious behavior is detected [10].

V. QUALITY OF SERVICE REQUIREMENTS

In [13] we have defined the most relevant QoS issues and challenges related to a dynamic, very complex VANET-like environment. The unreliable channel represents one of the main potential security obstacles. Due to high sensitivity of the channels to interference, signal noise, and multipath fading effects the communication can be prone to information leakage by eavesdroppers, along with the considerable decrease of the bit and packet delivery ratio (PDR), which is an important QoS metric. The main QoS metrics are presented in Fig. 3.

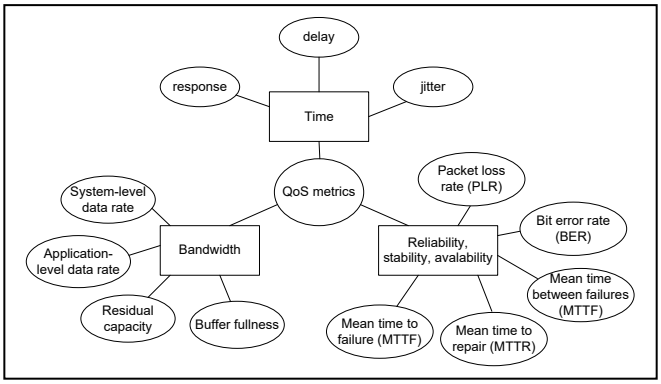

Figure 3. QoS metrics

Being dynamic networks, the V2X environments must keep in real-time the information related to their topology, and regularly update the information and provide safe delivery of the transmitted information.

In the case of the no centralized control, where the network users are continuously leaving and joining the communication, like in real-world case, it is a priority to create a kind of organized network functioning, a quasi-centralized structure responsible of quick response and decision making [13]. Another potential QoS issue is related to the limited computing and memory resources of the vehicle. The vehicular devices are highly constrained by a limited computational power, small storage spaces and a limited power supply (battery), whereas the need for a proper QoS provisioning brings some additional overhead, thus affecting the communication power consumption.

Still, one of the most challenging issues is to operate in the context of frequent channel contention circumstances. For instance, in VANETs but also in some other V2X concepts, the vehicles are using one common channel for communication

and topology discovery needs, thus the issue of potential interference and channel contention appearance seem very realistic. There are different solutions for this type of issues, whereas the most common are the TDMA-based solutions and the use of different frequency for each transmitting device. Each of these have their pros and cons, either dealing with the need for some form of the centralized control or the need for a proper channel selection and distribution of channel information. Nevertheless, one of the most demanding tasks for QoS in V2X, and especially in VANETs, is to maintain the communication paths in a highly dynamic environment, and in the case of the disconnection, the proper and efficient route reestablishment, while keeping at the minimum overhead and delays [13].

The [14] study provides an additional overview of the 5G V2X QoS demands, and relates to the advanced services in such environment, such as the self-driving autonomous car, vehicle platoon identification, exchange of the collected sensor data, maneuver changes, information related to the trajectories and their alignments, etc. These procedures are, besides direct security reasons, necessary in order to improve road safety, traffic management and data distribution.

TABLE I. QOS REQUIREMENTS FOR ADVANCED V2X SERVICES [14]

Use case class	***Max. latency (ms)***	***Packet size in (bytes)***	***Packet reliability (%)***	***Data rate (Mbps)***	***Min. range (m)***
Vehicle-platooning	10–500	50–6000	90–99.99	50–65	80–350
Advanced-driving	3–100	300–12,000	90–99.999	10–50	360–500
Extended-sensors	3–100	1600	90–99.999	10–1000	50–1000
Remote-driving	5	–	99.999	Uplink: 25 Downlink: 1	–

Table 1 summarizes the most up to date QoS requirements for advanced V2X services and applications, focusing to the latency and reliability and latency which are required to be higher than the basic safety application requirements, where usually the messages are sent on periodic basis, and typically every 100ms.

VI. CONLUSION

In this paper, we have considered the wide category of specific wireless communication technologies that correspond to Vehicle-to-Everything techniques. It is recently widely discussed in many research and industry papers, as it presents a field that is technically attractive due to its supreme applicability in many services, communication, transportation, real-time monitoring and decision-making systems.

As there are already a number of developed and implemented V2X services, the focus of this paper is on the security, availability, confidentiality, and proper functionality in different case study environments.

For the future work, we have assumed the detailed analysis of the specific attacks and vulnerabilities, providing some real-world statistics and results, which would be of use and further consideration for different case studies.

REFERENCES

[1] FMVSS No. 150 Vehicle-To-Vehicle Communication Technology For Light Vehicles, Report of Office of Regulatory Analysis and Evaluation National Center for Statistics and Analysis, U.S. Department of Transportation, 2016. [Available Online] https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/v2v_pria_12-12-16_clean.pdf

[2] M. Li, J. Gao, X. S. Shen, L. Zhao, "Intelligent Computing and Communication for the Internet of Vehicles", SpringerBriefs in Computer Science. Springer, Cham. 2023. https://doi.org/10.1007/978-3-031-22860-5_1

[3] D. Šešić, N. Stanković, J. Šišić, "Application of DSCR Wireles Technologu in Vehicle-to-Vehicle Communication in Order to Increase Trraffic Safety", Proceedings of the 4th International Conference on Traffic Safety in Local Community (Bezbjednost saobraćaja u lokalnoj zajednici), October 2015, pp. 367-372. In Bosnian.

[4] D. Kanthavel, S.K.B. Sangeetha, K.P. Keerthana, "An empirical study of vehicle to infrastructure communications - An intense learning of smart infrastructure for safety and mobility", International Journal of Intelligent Networks, vol. 2, 2021, pp. 77–82

[5] P. Sewalkar, J. Seitz, "Vehicle-to-Pedestrian Communication for Vulnerable Road Users: Survey, Design Considerations, and Challenges", Sensors, vol. 19, no. 358, 2019, pp. 1-18.

[6] I. Sotoa, M. Calderona, O. Amadorb, M. Uruenac, "A survey on road safety and traffic efficiency vehicular applications based on C-V2X technologies", Vehicular Communications, Volume 33, 2022, 100428, https://doi.org/10.1016/j.vehcom.2021.100428

[7] S. Kim, R. Shrestha, "Internet of Vehicles, Vehicular Social Networks, and Cybersecurity", In: Automotive Cyber Security. Springer, Singapore. https://doi.org/10.1007/978-981-15-8053-6_7

[8] V. H. La, A. Cavalli, "Security Attacks and Solutions in Vehicular Ad Hoc Networks: A Survey", International Journal on AdHoc Networking Systems (IJANS) Vol. 4, No. 2, April 2014, pp. 1-20.

[9] LTE. Service requirements for V2X services (3GPP TS 22.185 version 15.0.0 Release 15), Technical specification. 2018.

[10] M. Muhammad, G. Ali Safdar, "5G-based V2V broadcast Communications: A security perspective", *Array*, vol. 11, 2021, Artcile No. 100084.

[11] M. Hasan, S. Mohan, T. Shimizu, H. Lu, "Securing Vehicle-to-Everything (V2X) Communication Platforms", *IEEE Transactions on Intelligent Vehicles*, April 2020, https://doi.org/10.1109/TIV.2020.2987430

[12] B. Manale, T. Mazri, "Security of communication 5G-V2X: A proposed approach based on securing 5G-V2X based on Blockchain", ITM Web of Conferences 43, 010, ICAIE'2022, 25 (2022), https://doi.org/10.1051/itmconf/20224301025

[13] S. Boštjančič Rakas, V. Timčenko, "A Survey on Quality of Service in MANET", Proceedings of the INFOTEH-JAHORINA Vol. 15, March 2016, pp 349–352.

[14] S.A.A. Hakeem, A.A. Hady, H. Kim, "5G-V2X: standardization, architecture, use cases, network-slicing, and edge-computing", *Wireless Networks*, vol. 26, 2020, pp. 6015–6041. https://doi.org/10.1007/s11276-020-02419-8