Original research paper
UDC 004.7.056:316.774/.775
DOI 10.7251/IJEEC2302065T

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

Valentina Timčenko, Slavica Boštjančič Rakas

Institute Mihajlo Pupin, University of Belgrade, Belgrade, Serbia

E-mail address: valentina.timcenko@pupin.rs, 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 the 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 the arising issues and countermeasures related to the security, privacy and quality of service (QoS) as well as predictive 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 [1]. 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 [2]. 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. To fulfill the expectations of IoV systems, V2X connections must adhere to very stringent criteria. such as ultra-high reliability ($\approx$ 99.999 %), ultra low end-to-end latency (< 5 ms), extremely high velocities (around 150 km/h), high network density ($\approx$500 vehicles/km2 for highway and 1000 vehicles/km2 for suburban environments), a maximum packet loss of 10−5, (the application layer), etc [1]. 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 the 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 the 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, as well as predictive QoS. 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

This paper is a revised and expanded version of the paper presented at the XXII International Symposium INFOTEH-JAHORINA 2023

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 [1]. 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 [3]. Vehicles can share 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. Vehicles are provided with a real-time map of the vehicle's surroundings, i.e. the information about vehicle's urban environment (infrastructure, other vehicles, transportation management systems, navigation sources, and more). 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. Drivers are notified about traffic congestions ahead of them and presented with alternative routes. Vehicles can communicate with different parts of traffic system, such as traffic lights, road signs, etc. Moreover, its communication promotes environmentally friendly driving resulting in decreased fuel consumption and reduced 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, 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. The most complete categorization of different V2X types is as follows:

- Vehicle-to-Vehicle (V2V).
- Vehicle-to-Infrastructure (V2I).
- Vehicle-to-Pedestrian (V2P).
- Vehicle-to-Network (V2N).
- Vehicle-to-Grid (V2G).
- Vehicle-to-Cloud (V2C).
- Vehicle-to-Device (V2D) - Bluetooth / WiFi-Direct, e.g. Apple's CarPlay and Google's Android Auto.

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. The utilization of this V2X communication technology enhances the effectiveness of vehicle safety systems, contributing to the preservation of lives. A police report from 2019 estimates 6.8 million, resulting in 36,096 fatalities and 2.7 million people injured Connected vehicles can equip drivers with essential tools to foresee potential collisions, thereby diminishing the loss of lives [4].

The 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 the 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) [1]. 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 [5]. 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. The 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) denotes a two-way wireless data exchange involving critical safety and operational information between vehicles and the infrastructure of roadways, such as roadside units (RSUs), encompassing traffic lanes, signs, and lights. Its purpose is to prevent or alleviate accidents while facilitating various safety, mobility, and environmental advantages (Figure 1).

V2I communication spans all vehicle categories and road types, effectively converting infrastructure components into "smart infrastructure." This technology enables vehicles to share and receive information with nearby devices on or near the road, including cameras, streetlights, signage, and lane markers, enhancing roadway safety by delivering more information promptly to the appropriate vehicles [6].

Moreover, V2I plays a crucial role in optimizing the management of emergency vehicle traffic lights, contributing to the efficiency of ambulance, fire brigade, or police automobile traffic control.

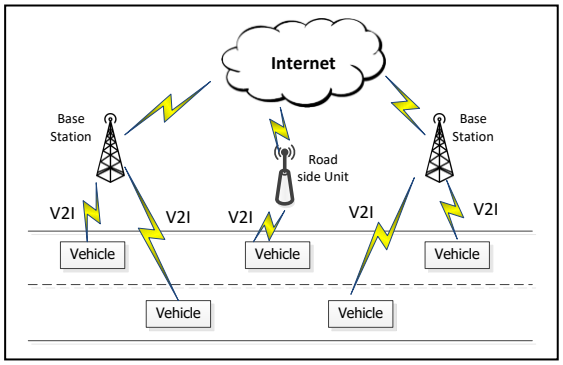

Figure 1. V2I communication

V2I technology serves the purpose of alerting drivers about potential collisions, traffic congestion, fast curves, and speeds [6]. Similar to V2V, this technology relies on DSCR technology for communication.

C. Vehicle to Pedestrian (V2P)

Vulnerable Road Users (VRUs) are traffic participants, such as pedestrians, cyclists, and two-wheeler drivers. There are numerous VRU fatalities every year with different rates of fatalities among different types of VRUs and different countries [7]. The V2P represents the 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. [7] VRUs manifest in different characteristics, like speed, mobility, travel pattern, therefore developers of such systems need to design an effective V2P system taking into account this information.

V2P encompasses direct or indirect communication, as well as hybrid modes [7]. Direct mode of communication represents direct communication between vehicles and VRUs, with no intermediate entity. It is the fastest way of communication, but the range of limited. It is best suited for safety applications due to lower delay, but the underlying communication technology needs to be the same for all entities in the communication [7]. 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 the 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 [7].

D. Vehicle to Network (V2N)

V2N (Vehicle-to-Network) facilitates communication between the vehicles and between vehicles and different smart traffic objects (street lights, traffic signals, pedestrians etc.) via Internet using cellular networks. Additionally, it has the potential to support advanced navigation systems based on maps. Such networks can become a reality with the introduction of 5G and evolution of cellular technology.

The main benefits of the 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 the 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 [8].

E. Vehicle to Grid (V2G)

The concept of Vehicle to Grid (V2G) provides th-information exchange between the vehicles and smart grids, with the goal to efficiently balance the loads. It includes the two specific subcategories: Vehicle-to-Building/Home (V2B/V2H) and Vehicle-to-Load (V2L).

It mostly uses as the battery powering backbone for the electrical vehicles (EV), as it sees them as the “battery-on-wheels”. Conceptually, it provides the possibility of the bidirectional charging, allowing the vehicle the battery charging during the low demand hours, and is dependent on the exorbitance of the supply. Otherwise, during the peak hours, extra energy can be released back into the grid.

That way, the consumers take an active part in V2G utilities and system functioning and grid stabilization by providing a possibility to efficiently manage the demand-response balance and obtain stronger flexibility. This is evident when considering the raise of the number and types of the used renewable sources. As digitally evolving concept, which is highly related to the energy transmission and distribution systems, there is a need to raise a red flag for the related cybersecurity awareness. V2G cybersecurity guidelines encompass all the communication elements, starting from the vehicle, its charging infrastructure, the communication networks and used technologies between the vehicle and finally the assets or the grid to which it is connected. This path covers a number of different vulnerability points, which can intentionally or un intentionally, open to malicious activities.

F. Vehicle to Cloud (V2C)

Vehicle to cloud (V2C) communication practically controls and manages the V2N access to broadband cellular mobile networks, with a goal to provide the data exchange with the cloud infrastructure. Some applications of this technology include: Over the air (OTA) updates vehicles' software and remote vehicle diagnostics (DoIP, Diagnostics over Internet Protocol) tools.

As being a very complex system, the modern vehicular communication demands for a specific driving APIs (Application Programming Interfaces). The security of these APIs is of the most important importance, as these should be protected from any malware or vulnerability. The vital role in this concern is given to the Cloud API gateways being a barrier and control point for communication, managing the traffic between applications and their services, handling the authentication and authorization for the users or services access.

G. Vehicle to Device (V2D)

Vehicle-to-Device (V2D) represent a type of the V2X communication where it is referred to the exchange of information between a vehicle and a number of different user (driver) devices such as Bluetooth ear device, Wi-Fi direct, smartphone, tablet, geolocation devices (Google's Android Auto) and other. Although bringing an additional comfort to the driver, these devices do suffer from specific security issues. Thus there is a need to connect secure ICT (Information and Communication Technology) terminals, PKI (Public Key Infrastructure), and ISFs (Information security firewall) that are designed with an aim to provide higher level of security and safety. The terminals will allow smooth V2D communication, relying on the proper functioning and integrity of the devices (phones, tablets…). The PKIs provide the application of the digital certificates and encryption/decryption mechanism in order to authenticate the identity of the communicating devices.

The ISFs represents a particular network security device dedicated to the filtering and monitoring of the communication traffic in search for the unauthorized access and potential threats.

III. INTERNEET 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 [9]. Figure 2 present a communication architecture of the IoV.

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

The 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 the density and speed of vehicles is 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.

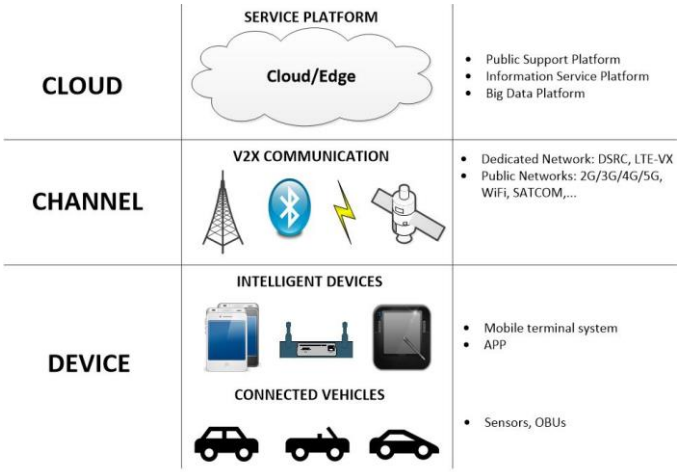

Figure 2. IoV communication architecture

IV. CYBERSECURITY ISSUES

The V2X concept is by its nature highly constrained environment with limited power and computational resources, usually working in real-time, and often adhering to very strict performance requirements. Thus, the implementation of the robust, accurate and time efficient security solution, along with the implementation of the advanced encryption/decryption mechanisms and complex authentication protocols, can be an extremely intensive computational and resource management task. Instead, when considering the in-vehicle communication between the components situated behind the gateway, this communication can be weak in privacy, authentication, and integrity methods application.

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 [10]. The 3GPP has identified a number of basic safety and non-safety V2X use-cases, where the release 15 [11] targets the 5G-NR (New Radio) access technology in support for advanced applications that will provide semi-automated and fully automated V2X functionalities [12].

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 (the 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) [13]. 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 [9].

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 [14].

The 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 [13]. There is also a security concern related to the non-Repudiation attack category [12].

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 [12].

V. QUALITY OF SERVICE REQUIREMENTS

In [15] 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.

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 [15]. 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.

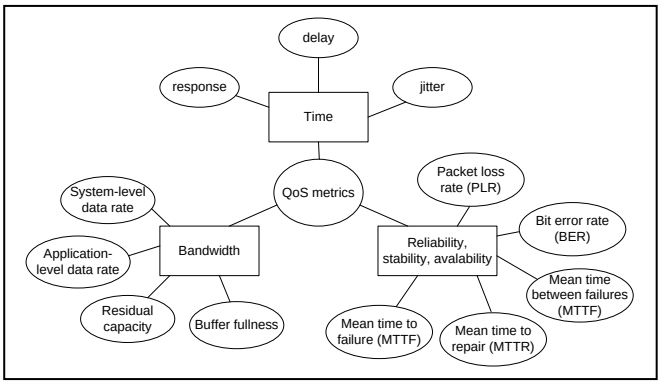

Figure 3. QoS metrics

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 the overhead and delays [15].

TABLE I. QOS REQUIREMENTS FOR ADVANCED V2X SERVICES [16]

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	–

The [16] 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.

The 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 the periodic basis, and typically every 100ms.

A. Predictive QoS

V2X applications depend on mobile network connectivity and rely on a stringent QoS requirements. But this can be challenging due to fluctuating network conditions, therefore it is of vital importance for the vehicle to receive notifications regarding anticipated changes of the available QoS in advance. Also, it is of vital importance for V2X services to prevent the abruption of session interruptions due to QoS deterioration. This creates the necessity for prediction of the QoS parameters change and provisioning of early notifications to the vehicles about the expected change (decrease or increase) of QoS. These notifications can help V2X applications to adapt, before the QoS change and not having to adjust after the change has already made an impact on the V2X services [17]. This can be provided by the Predictive QoS (PQoS), an innovative mechanism for delivering advance QoS notifications from the network to the V2X application. This allows vehicle to respond accordingly, adjusting or halting applications that may pose safety concerns under the predicted QoS conditions [18].

While functional safety mandates the shutdown of the system in the event of a system fault, PQoS should incorporate mechanisms to smoothly transition the operational mode. This ensures that V2X applications adhere to stringent latency and reliability constraints. Table II depicts certain use cases, where PQoS could be beneficial [18].

TABLE II. V2X APPLICATIONS AND PQOS [18]

		V2X applications		
		HD map collecting and sharing	**Teleoperated driving**	**High-density platooning**
QoS	**Delay**	≤ 100 ms	≤ 50 ms	10–25 ms
	Reliability	99%	99% (uplink) 99.999% (downlink)	90–99.99%
	Data Rate	up to 500 Mbps	30/50 Mbps	30/50 Mbps
PQoS	**Role of predictions**	ensure reliable services	guarantee a minimum safety level at all times	ensure continuous operation (even without connectivity)
	Prediction window	minutes/hours	seconds/minutes	seconds/minutes

VI. CONCLUSION

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.

ACKNOWLEDGMENT

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

REFERENCES

[1] D. .P. M. Osorio, I. Ahmad, J. D. V. Sánchez, A. Gurtov, J. Scholliers, M. Kutila, P. Porambage, “Towards 6G-Enabled Internet of Vehicles: Security and Privacy”, *IEEE Open Journal of the Communications Society*, vol. 3, January 2022, pp. 82-105.

[2] Z, Ali, S. Lagén, L. Giupponi, R. Rouil, “3GPP NR V2X Mode 2: Overview, Models and System-Level Evaluation”, IEEE Access, Vol. 0, June 2021, pp. 89554 – 89579.

[3] 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

[4] 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

[5] 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 saobra?aja u lokalnoj zajednici), October 2015, pp. 367-372. In Bosnian.

[6] 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

[7] 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.

[8] 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

[9] 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

[10] 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.

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

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

[13] 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

[14] 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

[15] 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.

[16] 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

[17] Predictive QoS and V2X Service Adaptation. 5GAA Automotive Association Technical Report, January 2023.

[18] M. Boban, M. Giordani, M. Zorzi, "Predictive Quality of Service: The Next Frontier for Fully Autonomous Systems", *IEEE Network*, Vol. 35, No. 6, November/December 2021, DOI: 10.1109/MNET.001.2100237.

Valentina Timčenko received her Dipl. Eng., M.S. and PhD degree in electrical engineering from the School of Electrical Engineering, University of Belgrade, in 2004, 2010, and 2022 respectively. She works as a Research Associate at the University of Belgrade, Institute Mihajlo Pupin, Belgrade, Serbia. She has participated in several research projects and studies concerning NGN design and network management systems. Author and coauthor in more than 120 papers in journals, national and international conferences and books. Her scientific and professional commitment includes research, design, and implementation of solutions for telecommunication networks, especially in the area of network and data security, machine learning, and virtualization. She is an IEEE member for 21 years.

Slavica Boštjančič Rakas received her B.Sc. (2004) and M.Sc. (2007) degrees in traffic engineering and her Ph.D. degree (2011) in technical sciences, all from the University of Belgrade, Serbia. Dr. Boštjančič Rakas joined Mihailo Pupin Institute in Belgrade in 2005, where she is currently research fellow in the area of telecommunication networks. She has participated in national and international research projects and studies concerning design of next generation networks, quality of service, network management systems as well as cyber security of industrial control systems, such as SCADA and dynamic line rating. As author or coauthor, she published more than 60 papers at national and international journals, books and conferences. She was co-editor of the book on ICS cyber security in the Future Internet environment. Her research interests include quality of service architectures, network management in the future Internet, and security issues in industrial control systems.